

Transparent Ready

Guide utilisateur

10/2009

Le présent document comprend des descriptions générales et/ou des caractéristiques techniques générales sur la performance des produits auxquels il se réfère. Le présent document ne peut être utilisé pour déterminer l'aptitude ou la fiabilité de ces produits pour des applications utilisateur spécifiques et n'est pas destiné à se substituer à cette détermination. Il appartient à chaque utilisateur ou intégrateur de réaliser, sous sa propre responsabilité, l'analyse de risques complète et appropriée, et d'évaluer et de tester les produits dans le contexte de leur application ou utilisation spécifique. Ni la société Schneider Electric, ni aucune de ses filiales ou sociétés dans lesquelles elle détient une participation, ne peut être tenue pour responsable de la mauvaise utilisation des informations contenues dans le présent document. Si vous avez des suggestions, des améliorations ou des corrections à apporter à cette publication, veuillez nous en informer.

Aucune partie de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique ou photocopie, sans l'autorisation écrite expresse de Schneider Electric.

Toutes les réglementations locales, régionales et nationales en matière de sécurité doivent être respectées lors de l'installation et de l'utilisation de ce produit. Pour des raisons de sécurité et afin de garantir la conformité aux données système documentées, seul le fabricant est habilité à effectuer des réparations sur les composants.

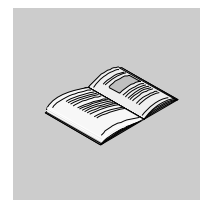
Lorsque des équipements sont utilisés pour des applications présentant des exigences de sécurité techniques, suivez les instructions appropriées.

La non-utilisation du logiciel Schneider Electric ou d'un logiciel approuvé avec nos produits peut entraîner des blessures, des dommages ou un fonctionnement incorrect.

Le non-respect de cette consigne peut entraîner des lésions corporelles ou des dommages matériels.

© 2009 Schneider Electric. Tous droits réservés.

Table des matières



	Consignes de sécurité	11
	A propos de ce manuel	13
Chapitre 1	Transparent Ready	17
	Transparent Ready	18
	Classes de services Transparent Ready offerts	22
	Utilisateurs de ce guide	26
	Organisation de ce guide	27
Chapitre 2	Planification physique, conception et installation d'un réseau Ethernet industriel Transparent Ready	29
2.1	Normes requises	30
	Vers une normalisation de l'Ethernet industriel	31
	Normes de planification et d'installation requises	34
2.2	Configuration et planification physiques	36
	Planification de câblage Ethernet industriel	37
	Normes de câblage structuré	38
	Câblage dans un système Ethernet industriel Transparent Ready	42
	Présentation de la structure de base d'un réseau	47
	Développement d'architecture réseau pour les réseaux Ethernet industriel	54
	Topologie en anneau redondant	59
	Technologies LAN et conception réseau	61
	Matériel LAN	66
	Autres considérations LAN	69
	Technologies WAN et conception réseau	70
	Matériel WAN	73
2.3	Exigences liées à l'environnement	76
	Résumé des normes environnementales	77
	Exigences liées à la mécanique	78
	Exigences liées à la protection climatique	80
	Exigence de protection contre la pénétration de corps étrangers	82
	Emission électromagnétique et exigences d'immunité	85

2.4	Choix des composants Ethernet industriel	86
	Câbles cuivre Ethernet	87
	Câbles à fibre optique	91
	Spécifications de la couche physique 10/100BaseF	95
	Connecteurs Ethernet pour les réseaux en cuivre	96
	Connecteurs pour fibre optique	99
	Équipements d'infrastructure recommandés pour Ethernet industriel	101
2.5	Installation	102
	Règles d'installation CEM pour les réseaux Ethernet	103
	Liaison équipotentielle	105
	Liaison équipotentielle de votre bâtiment	106
	Liaison équipotentielle locale des équipements et des machines	108
	Câblage de réseau Ethernet compatible avec CME et les chemins de câbles	109
	Types de câbles cuivre Ethernet	115
	Outils pour câbles cuivre Ethernet	118
	Comment fabriquer un câble Ethernet	119
	Administration du câblage	121
	Documentation de câblage	123
2.6	Vérification d'un réseau Ethernet industriel Transparent Ready	125
	Recommandations de vérification de réseaux Ethernet industriel Transparent Ready	126
	Liaisons permanentes	127
	Voies	129
	Test d'une installation en cuivre	131
2.7	Considérations supplémentaires pour la conception d'un réseau Ethernet industriel Transparent Ready	132
	Internet et technologies IP dans un environnement d'automatisation	133
	Modèle Open System Interconnection (ou modèle pour l'interconnexion de systèmes ouverts)	135
	Modèle TCP/IP	137
	Modèle Transparent Ready	139
	Adresses IP et classes	142
	Remarques concernant la multidiffusion	147
	Filtrage de multidiffusion	149
	Gestion du réseau	151
	Routage	153
	Présentation de l'accès à distance	155
	Types d'accès distant	157
	Méthodes d'accès au réseau	159
	Automate connecté à Internet	162
	Problèmes de sécurité	164

Chapitre 3	Vue d'ensemble des services	169
3.1	Evaluation de la configuration du système	170
	Services communs à chaque niveau de l'usine	171
	Communication au niveau de l'entreprise	172
	Niveau inter-automates	173
	Communications au niveau du terrain	174
	Sélection du service de communication	175
	Services et protocoles de prise en charge de Transparent Ready	178
3.2	Service I/O Scanning	183
	Description du service I/O Scanning	184
	Fonctionnement du scrutateur d'E/S	187
	Périodes de répétition	192
	Etats défectueux courants	194
	Temps de réponse	195
3.3	Messagerie Modbus	197
	Description du service de messagerie Modbus	198
	Equipements prenant en charge les services Ethernet Modbus	203
	Fonctionnement du client Modbus dans les systèmes Quantum	204
	Fonctionnement du client Modbus dans les systèmes Premium	206
	Fonctionnement du client Modbus dans les systèmes Momentum	208
	Fonctionnement du serveur Modbus dans les systèmes Quantum	209
	Fonctionnement du serveur Modbus dans les systèmes Premium	212
	Fonctionnement du serveur Modbus dans les systèmes Momentum	214
	Serveurs Modbus et limites des sockets	215
	Nombre de tentatives et délais d'attente de la messagerie Modbus	216
3.4	Service Global Data	217
	Service Global Data	218
	Considérations relatives à Global Data	222
3.5	Remplacement d'équipements défectueux	225
	Service FDR	
	(Faulty Device Replacement, Remplacement d'équipements défectueux)	226
	Equipements prenant en charge les services FDR	229
3.6	Synchronisation horaire	230
	Service de synchronisation horaire	231
	Fonctionnement du service de synchronisation horaire	233
	Applications de synchronisation horaire	234
	Equipements Schneider -	
	mise en œuvre du service de synchronisation horaire	238
3.7	Service de notification par message électronique	239
	Service de notification par message électronique	240
	Fonctionnement du service de notification par message électronique	242
	Equipements prenant en charge la notification par message électronique	244

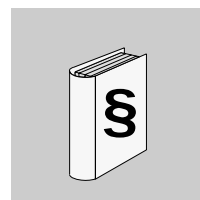
3.8	Serveur Web standard	245
	Services du serveur Web	246
	Fonctionnement du serveur Web	248
	Equipements prenant en charge les services de serveur Web standard	252
3.9	Serveur Web FactoryCast	253
	Serveur Web FactoryCast	254
	Fonctionnement du serveur Web FactoryCast	256
	Equipements prenant en charge les services de serveur Web FactoryCast	258
3.10	Serveur Web FactoryCast HMI	259
	Services Web FactoryCast HMI	260
	Equipements prenant en charge le service Web HMI FactoryCast	265
3.11	Autres services	266
	Service FTP	267
	Service SNMP	269
	Service TFTP	271
	Service Telnet	272
	Autres services pris en charge par les équipements Quantum	274
	Autres services pris en charge par les équipements Premium	275
	Autres services pris en charge par les équipements TSX Micro	277
	Autres services pris en charge par les équipements Momentum	277
	Autres services pris en charge par les équipements Advantys STB	278
	Autres services pris en charge par les passerelles/ponts Power Logic	278
	Autres services pris en charge par les systèmes de câblage ConneXium	279
3.12	OPC Factory Server	280
	OPC Factory Server	281
	Services OFS	285
	Performances OFS	288
	Architecture d'exécution pour Unity/OFS/SCADA : un exemple simple	292
	Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA non fréquemment modifiés	294
	Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA nécessitant des modifications fréquentes	296
	Architecture Build-time/Runtime pour système avec multiples connexions SCADA	298
3.13	SCADA/IHM	300
	SCADA/IHM	301
	Communications entre un serveur d'E/S et un équipement terrain	303
	Communications SCADA vers des équipements terrain : Utilisation des sockets et des requêtes	308
	Communications client entre un serveur d'E/S et un affichage	312
	Détails sur la mise en œuvre des produits Schneider	313

3.14	Redondance	314
	Redondance réseau et services de communication	315
	Redondance dans un système SCADA	319
	SCADA dans un système de redondance d'UC Quantum	323
	Permutation de redondance d'UC et services Ethernet	333
3.15	Systèmes de passerelle/pont	335
	Vue d'ensemble des passerelles et des ponts	336
	Fonctionnement des passerelles et des ponts	340
3.16	Services pris en charge par équipement.	344
	Services Ethernet et équipements	
	Transparent Ready qui les prennent en charge	344
3.17	Evaluation des performances système	352
	Communications système	353
	Temps de réponse de la messagerie Modbus	353
	Temps de réponse du serveur Modbus	354
	Temps de réponse du client de messagerie Modbus	359
	Scruteurs d'E/S	363
	Charge totale sur les équipements	365
	Solutions pour les performances système	366
	Temps de réponse de la passerelle	372
Chapitre 4	Dépannage	375
4.1	A propos du dépannage	376
	Introduction au dépannage	377
	Identification générale des problèmes.	378
4.2	Dépannage réseau	380
	Introduction au dépannage réseau	381
	Dépannage des connexions	383
	Dépannage en cas de connexions intermittentes	385
	Dépannage en cas de connexions lentes	386
	Dépannage de l'accès distant	387
4.3	Dépannage des services.	389
	Dépannage des services.	390
	Dépannage de la messagerie Modbus et du scrutateur d'E/S	391
	Dépannage SNMP	394
	Dépannage Telnet et FTP	395
	Dépannage pour remplacement d'équipements défectueux/BootP	396
	Dépannage SMTP	398
	Tableau de dépannage de synchronisation horaire (NTP)	399
	Tableau de dépannage Web	400
4.4	Dépannage en cas de lenteur de réponse d'un système SCADA/HMI	401
	Dépannage en cas de lenteur de réponse (SCADA/HMI)	401
4.5	Dépannage du pont.	403
	Dépannage du pont.	403

4.6	Dépannage en cas de perte de paquets	404
	Dépannage en cas de perte de paquets	405
	Utilisation d'un outil de capture de paquet	406
	Dépannage de capture de paquet	408
Annexes		411
Annexe A	Temps de réponse de la scrutation d'E/S	413
A.1	Temps de réponse du scrutateur d'E/S des automates Premium	414
	Temps de réponse du scrutateur d'E/S Premium :	
	Entrée distante vers sortie distante	415
	Temps de réponse du scrutateur d'E/S Premium :	
	Entrée distante vers sortie locale	419
	Temps de réponse du scrutateur d'E/S Premium :	
	Mémoire de l'automate vers sortie distante	423
A.2	Temps de réponse du scrutateur d'E/S des automates Quantum	427
	Temps de réponse du scrutateur d'E/S Quantum :	
	entrée distante vers sortie distante	428
	Temps de réponse du scrutateur d'E/S Quantum :	
	Entrée distante vers sortie locale	432
	Temps de réponse du scrutateur d'E/S Quantum :	
	Entrée locale vers sortie distante	436
Annexe B	Débit de serveurs Modbus	441
	Débit des serveurs Modbus Quantum : Unity v2.0	442
	Débit des serveurs Modbus Premium : Unity v2.0	444
Annexe C	Temps de réponse des clients Modbus	447
	Temps de réponse du client Modbus : Premium TSXP575634M	448
	Temps de réponse du client Modbus : Premium TSXP57304M	454
	Temps de réponse du client Modbus :	
	Quantum 140 CPU65150 avec port Ethernet intégré	461
	Temps de réponse du client Modbus : Quantum 140 CPU65150	
	avec module de communication Ethernet 140 NOE77101	467
	Temps de réponse du client Modbus : Quantum 140 CPU65150	
	avec module de communication Ethernet 140 NOE77111	473
	Temps de réponse du client Modbus : Quantum 140 CPU43412A	
	avec module de communication Ethernet 140 NOE77101	479
	Temps de réponse du client Modbus : Quantum 140 CPU43412A	
	avec module de communication Ethernet 140 NOE77111	485
Annexe D	Mesures du timeout et	
	du temps de réponse de la passerelle	491
D.1	Mesures du timeout et du temps de réponse	
	du serveur série de passerelles EGX200	492
	Temps de réponse du serveur série EGX200	493
	Mesures des réponses du serveur série	
	EGX200 avec timeout de la requête	498

D.2	Mesures du timeout et du temps de réponse	
	du serveur série de passerelles EGX400	503
	Temps de réponse du serveur série de passerelles EGX400	504
	Mesures des réponses du serveur série	
	EGX400 avec timeout de la requête	509
D.3	Mesures du timeout et du temps de réponse	
	du serveur série de passerelles 174CEV30020	514
	Temps de réponse du serveur série de passerelles 174CEV30020	515
	Mesures des réponses du serveur série	
	174CEV30020 avec timeout de la requête	520
Annexe E	Normes et autres considérations	
	relatives aux réseaux Ethernet industriel.	525
	Normes et organisations	526
	Compatibilité électromagnétique	536
	Activités de normalisation des connecteurs en cuivre	541
	Conformité aux normes	542
	Conformité du réseau Ethernet industriel Transparent Ready	544
Annexe F	Procédures de mise à la terre (masse).	547
	Connexions de mise à la terre (masse) adéquates	548
	Réalisation d'une connexion de terre	549
	Options de connexion des blindages de câble	555
	Procédures de test des réseaux Ethernet en cuivre	557
	Paramètres de performance	558
	Définition des paramètres de performance	560
Glossaire		565
Index		603

Consignes de sécurité



Informations importantes

AVIS

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.



L'apposition de ce symbole à un panneau de sécurité Danger ou Avertissement signale un risque électrique pouvant entraîner des lésions corporelles en cas de non-respect des consignes.



Ceci est le symbole d'une alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.



DANGER

DANGER indique une situation immédiatement dangereuse qui, si elle n'est pas évitée, **entraînera** la mort ou des blessures graves.



AVERTISSEMENT

L'indication **AVERTISSEMENT** signale une situation potentiellement dangereuse et susceptible **d'entraîner la mort** ou des blessures graves.

ATTENTION

L'indication **ATTENTION** signale une situation potentiellement dangereuse et susceptible **d'entraîner des** blessures d'ampleur mineure à modérée.

ATTENTION

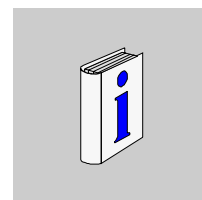
L'indication **ATTENTION**, utilisée sans le symbole d'alerte de sécurité, signale une situation potentiellement dangereuse et susceptible **d'entraîner des** dommages aux équipements.

REMARQUE IMPORTANTE

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de cet appareil.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction et du fonctionnement des équipements électriques et installations et ayant bénéficié d'une formation de sécurité afin de reconnaître et d'éviter les risques encourus.

A propos de ce manuel



Présentation

Objectif du document

Ce guide utilisateur concerne le vaste sujet de l'Ethernet industriel, qui constitue un élément clé dans la stratégie *Transparent Ready* de Schneider Electric. Son objectif est double :

- décrire l'impact de l'Ethernet industriel sur la conception de nouveaux systèmes de contrôle ;
- fournir les informations nécessaires pour mettre en œuvre et prendre en charge une solution Transparent Ready qui réponde au mieux à vos besoins applicatifs.

Le guide décrit quatre tâches essentielles pour réussir la mise en œuvre d'un système :

- Planification d'un système en vue d'optimiser les performances
- Sélection des services et des équipements Ethernet adaptés à votre application
- Choix appropriés lors de la conception du système et de son installation
- Résolution efficace des problèmes liés au système

Le guide s'adresse :

- aux concepteurs, intégrateurs de système et techniciens de maintenance qui connaissent les systèmes de contrôle industriels et leurs exigences, mais qui ne sont pas nécessairement familiarisés avec les produits et services Ethernet ;
- au personnel informatique des usines qui connaissent les principes de conception et d'installation d'un système Ethernet, mais qui ne sont peut-être pas familiarisés avec les environnements et les exigences du contrôle industriel.

Bien implantée dans les univers commerciaux et professionnels, la technologie Ethernet est relativement nouvelle dans l'industrie de l'automatisme. Du fait qu'il s'agit d'une technologie ouverte, Ethernet offre une large gamme de produits et de services commercialisés par de nombreux fournisseurs. Les avantages d'une approche ouverte sont évidents : votre système ne dépend plus des contraintes de communication, des coûts et des programmes de développement d'un fournisseur propriétaire.

Toutefois, certains composants Ethernet peuvent ne pas fonctionner de manière optimale en milieu industriel et les équipements Ethernet ne prennent pas tous en charge l'ensemble des services dont vous souhaiteriez disposer. Pour réussir la conception et la mise au point d'un système Ethernet industriel, vous devez associer des éléments informatiques Ethernet et les connaissances en matière d'automatisme classique. Le présent guide est destiné précisément à combler le fossé entre ces deux disciplines.

Le guide doit être utilisé en complément des manuels utilisateur Transparent Ready spécifiques aux différents produits. Pour en savoir plus sur les produits Transparent Ready commercialisés, reportez-vous au dernier catalogue Transparent Ready ou consultez le site www.telemecanique.com.

Document à consulter

Vous pouvez télécharger ces publications et d'autres informations techniques depuis notre site Web à l'adresse suivante : www.telemecanique.com.

Titre de documentation	Référence
Guide de référence rapide du commutateur Ethernet ConneXium 499NES25100 à 5 ports, 10/100 Base-TX	31005153
Guide de référence rapide du commutateur Ethernet ConneXium 499NES18100 à 8 ports, 10/100 Base-TX	31005416
Manuel de gestion des commutateurs - Système de câblage Ethernet ConneXium	31005844 (Anglais), 31005845 (Français), 31005846 (Allemand), 31005847 (Espagnol)
Guide de référence rapide du système de câblage Ethernet ConneXium (Commutateur électrique 10/100 Mbit/s 7TX 499NES17100/Commutateur optique 10/100 Mbit/s 5TX/2FX 499NOS17100)	31005848 (Anglais), 31005849 (Français), 31005850 (Allemand), 31005851 (Espagnol)
Guide de référence rapide de l'émetteur-récepteur ConneXium 499NTR10100	
Modicon Quantum - Module TCP-IP Ethernet - Guide utilisateur	043511452 (Anglais), 31004578 (Français), 31004579 (Espagnol)
Modicon Quantum Ethernet Web Embedded Server User Guide	31001403 (Anglais)
Guide utilisateur des modules Ethernet Quantum 140 NOE 771 xx	31001913 (Anglais), 31003063 (Français), 31002922 (Allemand), 31003122 (Espagnol)
Guide utilisateur des modules 140NOE771xx/140NWM10000/140CPU651x0 sous Unity Pro 2.0	
FactoryCast pour Quantum, Premium et Micro - Guide utilisateur	31001229

Manuel de configuration des modules FactoryCast HMI, Premium et Quantum HMI	35007415
Guide utilisateur de l'adaptateur de communication Ethernet 170ENT11001 et 170ENT11000 Momentum	31004109 (Anglais), 31004110 (Français), 31004111 (Allemand), 31004112 (Espagnol), 31007101 (Chinois), 31007558 (Italien)
174 CEV 200 30 Modicon TSX Momentum Modbus Plus to Ethernet Bridge User Guide	31000301 (Anglais)
Guide utilisateur du pont Modbus vers Ethernet 174 CEV 300 20	31005108 (Anglais), 31005109 (Français), 31005110 (Allemand), 31005111 (Espagnol)
Coupleur Modbus Plus vers Ethernet 174 CEV 200 40 Guide utilisateur	31005104 (Anglais), 31005105 (Français), 31005106 (Allemand), 31005107 (Espagnol)
Guide d'applications de l'interface réseau Advantys STB Ethernet Modbus TCP/IP	31003688 (Anglais), 31003689 (Français), 31003690 (Allemand), 31003691 (Espagnol), 31004622 (Italien)
Guide utilisateur des modules TSX Micro TSX ETZ 410/510	35004734
Guide utilisateur des modules réseau Ethernet Premium et Atrium sous Unity Pro	35006192 (Anglais), 35006193 (Français), 35006194 (Allemand), 35006195 (Espagnol), 31007102 (Chinois), 31007214 (Italien)
Guides du module Ethernet sous Unity	20110V20F
Option de communication Ethernet Modbus TCP/IP pour Altivar 58 - Instructions	VVDED300053
Fonctions Sepam Série 80 - Introduction	
Guide d'installation EGX	63230-314-200B1
Guide utilisateur EGX	63230-208A1
Guide de référence EGX	63230-314-202A2

Vous pouvez télécharger ces publications et autres informations techniques depuis notre site web à l'adresse : www.schneider-electric.com.

Commentaires utilisateur

Envoyez vos commentaires à l'adresse e-mail techpub@schneider-electric.com

Transparent Ready



Vue d'ensemble

Ce chapitre présente Transparent Ready, un programme stratégique essentiel au déploiement des technologies au niveau des produits et des services Schneider Electric.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Transparent Ready	18
Classes de services Transparent Ready offerts	22
Utilisateurs de ce guide	26
Organisation de ce guide	27

Transparent Ready

Définition de Transparent Ready

En 1996, Schneider Electric proposait un ensemble de technologies qui ont transformé l'univers des automatismes industriels. Cette approche consistait à associer les couches de liaison physique et de données d'Ethernet, telles qu'elles sont définies dans le modèle OSI (*voir page 135*), à des solutions Ethernet industrielles TCP/IP et Modbus. Le concept, initialement connu sous le nom de Transparent Factory, a évolué pour devenir Transparent Ready.

Transparent Ready est une initiative stratégique majeure conçue pour déployer des technologies Internet au niveau des produits et des services de Schneider Electric. Tous les produits ou services Schneider Electric qui prennent en charge des technologies Internet sont des produits Transparent Ready.

Définition des technologies Internet

Les technologies Internet décrivent un ensemble d'innovations techniques qui permettent la gestion des informations à l'aide d'Internet et de matériels, logiciels, langages et protocoles associés. Elles sont utilisées pour transférer, présenter et gérer des informations. En voici quelques exemples :

- Support Ethernet (sans fil, fibre optique, cuivre ou autre) sur lequel s'effectue le transfert des informations
- Trame Ethernet, suite de protocoles Internet (TCP/IP), SOAP et autres protocoles employés pour le transfert des informations
- Langages Java, HTML, XML et autres protocoles servant à présenter des informations

Définition de l'Ethernet industriel

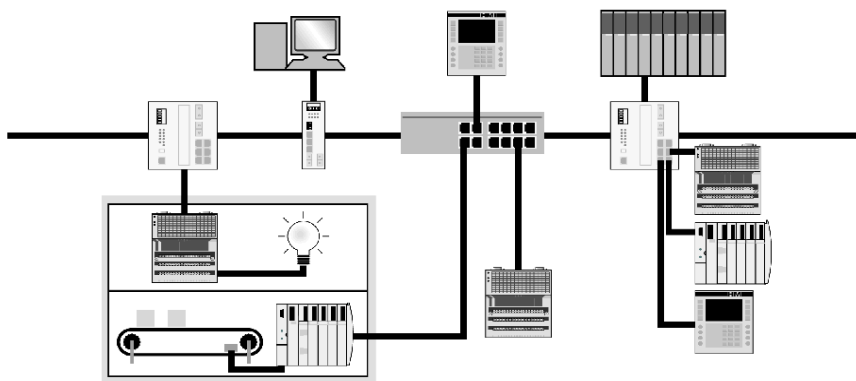
Ethernet fait référence à la manière dont les données accèdent au réseau et dont les messages sont mis en forme en vue de leur émission et de leur réception, ainsi qu'aux caractéristiques physiques du réseau : topologie, câbles, connecteurs et infrastructure.

L'Ethernet industriel est le nom commercial adopté par le segment de marché de l'automatisme industriel pour faire référence à l'utilisation d'Ethernet dans un environnement industriel. L'expression est désormais générique et englobe d'autres technologies Internet, même si Ethernet n'est pas toujours présent. Par exemple, Ethernet n'est pas utilisé dans les communications sans fil régies par la norme industrielle 802.11, mais celles-ci sont malgré tout considérées comme une application de l'Ethernet industriel.

Une analyse détaillée de l'Ethernet industriel (*voir page 29*) est présentée dans ce manuel, avec une explication des différentes caractéristiques et origines des protocoles Ethernet, TCP/IP et Modbus.

Comparaison entre l'Ethernet commercial et l'Ethernet industriel

Dans un environnement de contrôle industriel, des automates programmables industriels implantés dans l'usine jouent le rôle de serveurs pour les modules d'entrée et de sortie (E/S). Les automates peuvent être interconnectés par des bus terrain industriels de façon à permettre une distribution des tâches de gestion et de stockage des données. Un automate peut agir comme serveur pour certains équipements et comme client pour d'autres :



Le réseau industriel illustré ci-dessus est très différent des applications standard commerciales et professionnelles. En raison de la nature critique de nombreuses applications de contrôle, les équipements clients du système Ethernet industriel sont habituellement plus intelligents que les clients Ethernet commerciaux standard. Les modes de communication entre les équipements clients et serveurs sont définis par leurs services Transparent Ready.

Un réseau Ethernet commercial comprend un groupe de serveurs installés dans une salle de contrôle. Les données professionnelles sont stockées et gérées dans cette zone centrale, et envoyées depuis et vers les clients via des commutateurs et des routeurs répartis dans l'entreprise. Des pare-feux protègent l'entreprise contre les accès non autorisés.

L'Ethernet industriel est différent de l'Ethernet commercial sur trois points principaux : l'environnement, la structure et les exigences de performance.

	Ethernet commercial (bureautique)	Ethernet industriel
Environnement	Adapté à la présence et au travail de l'homme	Industrie légère et lourde
	Plage de températures standard	Environnements potentiellement difficiles
	Peu de poussière, d'humidité et de vibrations	Exposition aux interférences électromagnétiques
	Quasiment toutes les charges mécaniques ou tous les problèmes liés aux produits chimiques	Températures extrêmes, variables climatiques
	Exigences réduites en termes de compatibilité électromagnétique (CEM)	Possibilité de poussière, d'humidité et de vibrations
	Exigences minimales de traction	Risque de dommages mécaniques ou de problèmes liés aux produits chimiques Exigences de mise à la masse et de liaison pour le câblage et les équipements industriels
Structure	Espace au sol réduit dans des bâtiments en hauteur	Grandes zones de fabrication sur un seul étage
	Topologie en étoile	Possibilité d'utiliser des topologies en étoile, bus et chaînage
	Conforme aux normes de bureau	Anneau auto-régénérant et anneau auto-régénérant redondant pour optimiser la disponibilité
Performances	Haute disponibilité du réseau avec des connexions fiables	Haute disponibilité du réseau (généralement 24h/24, 7j/7 avec redondance)
	Paquets de données volumineux	Utilisation réduite de la bande passante toujours recommandée (pas plus de 40 % dans toutes les circonstances)
	Niveau acceptable de prévisibilité	Paquets de données de petite taille. La prévisibilité est essentielle.

Il existe d'autres éléments de différenciation, tels que les services Ethernet requis.

Stratégie Transparent Ready

Transparent Ready offre une stratégie en trois phases :

1 *Exposition des informations de contrôle industrielles via des normes ouvertes ou de facto*

Grâce aux produits de type serveur Web intégré et OPC, les équipements de Schneider Automation peuvent être intégrés dans différents systèmes capables d'accéder aux informations et aux données stockées sur ces équipements. La technologie serveur Web standard permet à toutes les personnes qualifiées de l'entreprise d'interagir avec le système automate.

2 *Création d'interfaces et de points d'intégration entre les systèmes automates et les applications professionnelles*

L'utilisation d'un équipement en tant que serveur de données au sein d'une architecture client/serveur permet à Schneider Alliances de développer des interfaces servant à accéder aux systèmes professionnels dans les environnements Windows ou UNIX.

3 *Développement d'une infrastructure ouverte qui gère les comportements déterministes et en temps réel*

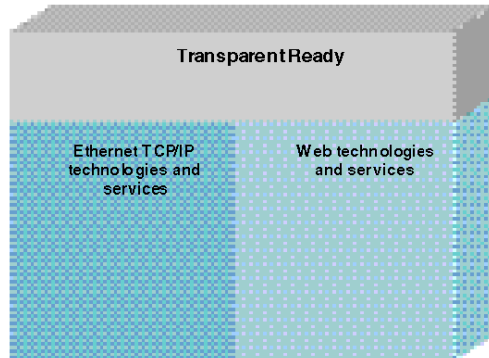
Le réseau constitue la base d'un échange efficace des informations. Ethernet, TCP/IP et Modbus sont les principales solutions choisies par Schneider pour mettre en place un réseau ouvert. Des commutateurs et des concentrateurs facilitent la construction de sous-réseaux hautement disponibles et en temps réel, ainsi que la prise en charge d'un éventail élargi d'applications.

Classes de services Transparent Ready offerts

Résumé

Les classes de services Transparent Ready permettent d'identifier les différents services fournis par chaque produit :

- Services de diagnostic, d'affichage et de contrôle via les technologies du Web
- Services de communication Ethernet



Classes de services Web

Les services Web Transparent Ready Web sont répartis en 4 classes, chacune identifiée par une lettre :

- Classe A : aucun service Web
- Classe B : services Web standard
- Classe C : services Web configurables
- Classe D : services Web actifs

Les produits Transparent Ready dotés d'un serveur Web intégré offrent 4 types de services Web :

- des services Web de maintenance ;
- des services Web de contrôle ;
- des services Web de diagnostic ;
- des services Web facultatifs, tels que la documentation ou la configuration.

Le tableau ci-dessous répertorie les services fournis par chaque classe de services Web :

Classe de serveur Web		Services Web			
		Maintenance	Surveillance et liaison informatique	Diagnostics	Facultatif
D	Serveur Web actif	Mise à jour du site Web utilisateur	Exécution autonome de services spécifiques (par ex., notification d'alarme par message électronique, échange avec les bases de données, calculs) SOAP/XML (client/serveur)	Etats définis par l'utilisateur	Documentation utilisateur
C	Serveur Web configurable		Editeur de variables d'automate Commandes déportées Pages Web utilisateur SOAP/XML (serveur)	Diagnostics des services de communication Etat des ressources internes du produit	
B	Serveur Web standard	Mise à jour du logiciel de l'équipement déporté Auto-tests distants	Description de l'équipement Afficheur de données	Diagnostics de l'équipement	Configuration des paramètres du réseau et des services de communication Ethernet Documentation de l'équipement
A	Aucun serveur Web	Aucun service Web			

Classes de services de communication Ethernet

Les services de communication Ethernet offerts par un produit sont répartis en 3 classes. Chaque classe est identifiée par un numéro :

- Classe 10 : services de communication Ethernet standard
- Classe 20 : services de gestion des communications Ethernet (niveau réseau et niveau produit)
- Classe 30 : services de communication Ethernet avancés

Les produits Transparent Ready offrent 8 types de services de communication Ethernet :

- Messagerie TCP Modbus
- Scrutation d'E/S
- Remplacement d'équipements défectueux (FDR)
- Gestion du réseau (SNMP)
- Données globales
- Gestion de la bande passante
- Synchronisation horaire (NTP)
- Notification des événements par message électronique (SMTP)

Le tableau ci-dessous répertorie les services fournis par chaque classe de services de communication Ethernet :

Classe de service	Services de communication Ethernet							
	Messagerie Modbus	Scrutation d'E/S	FDR	SNMP	Données globales	SMTP	Gestion de la bande passante	NTP
30	Lecture/écriture directe des E/S	Lecture/écriture périodique des E/S Configuration de la liste des équipements scrutés	Contrôle/mise à jour automatique de la configuration des paramètres de l'équipement	Utilisation de la bibliothèque MIB par un gestionnaire SNMP	Publication et souscription des variables du réseau	Notification des événements par message électronique	Surveillance du niveau de charge local	Synchronisation de l'horloge de l'équipement
20			Affectation automatique de l'adresse IP et des paramètres du réseau Contrôle/mise à jour de la configuration et des paramètres du produit par l'utilisateur	Détection du produit par un gestionnaire SNMP				
10	Lecture/écriture des mots de données		Affectation locale de l'adresse IP Vérification des adresses IP doubles					

Sélection des produits Transparent Ready

Les services offerts par un produit Transparent Ready sont identifiés par une lettre définissant le niveau de service Web, suivie d'un numéro définissant le niveau de service de communication Ethernet. Exemple :

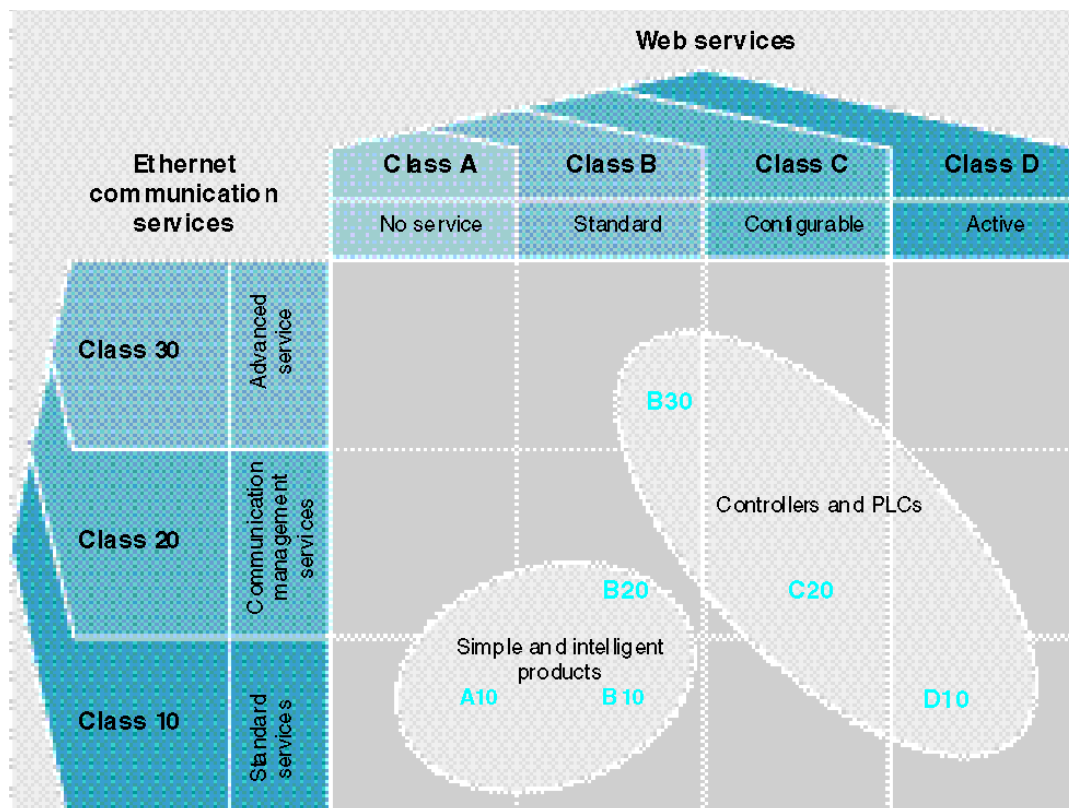
- Un produit de classe A10 n'offre aucun service Web mais fournit des services Ethernet standard.
- Un produit de classe C30 contient un serveur Web configurable et fournit des services de communication Ethernet avancés.

Les services fournis par une classe de niveau supérieur incluent tous les services des classes inférieures.

Les produits Transparent Ready sont regroupés en 4 grandes familles :

- produits de type capteurs et préactionneurs (simples ou intelligents) ;
- automates ;
- applications d'interface homme-machine (IHM) ;
- passerelles et serveurs dédiés.

Le schéma de sélection suivant peut vous aider à choisir vos produits Transparent Ready en fonction des classes de services requises.



Utilisateurs de ce guide

Récapitulatif

Pour réussir la conception et le dépannage d'un système Ethernet industriel, vous devez associer des éléments informatiques Ethernet et les connaissances en matière d'automatisme classique. Une relation de collaboration entre l'ingénieur de contrôle industriel et le responsable informatique de l'usine est la clé du succès d'un système Transparent Ready.

Analyse du public de ce guide

Ce tableau décrit les deux publics auxquels s'adresse ce guide, leurs domaines d'expertise et leurs besoins en matière d'information. Il indique également les sections de ce guide dans lesquelles se trouvent les informations nécessaires :

Public	Expertise	Connaissances requises
Responsables informatiques	● Protocole TCP/IP ● Alternatives d'architecture, telles que la commutation Ethernet ● Problèmes de sécurité du réseau ● Sélection des composants matériels ● Systèmes ouverts ● Interprétation des normes selon les fournisseurs ● Sélection des composants du réseau	● Environnement industriel et conditions de l'usine ● Blindage du réseau pour le protéger du bruit et des interférences ● Mise en œuvre physique du réseau dans une configuration industrielle ● Priorités opérationnelles : redondance, récupération rapide ● Problèmes de sécurité associés à une panne des automatismes
Professionnels du contrôle industriel	● Interaction avec l'équipement de contrôle ● Exigences liées à l'installation industrielle ● Exigences liées à la vitesse de transfert des données ● Récupération et redondance	● Exigences liées à la technologie Ethernet ● Sélection des services Transparent Ready ● Services Transparent Ready (<i>voir page 169</i>) ● Exigences liées aux environnements ouverts ● Problèmes de communication des systèmes ouverts ● Intégration de produits provenant de plusieurs fournisseurs ● Conception du système et protocoles ● Problèmes de sécurité du système

Organisation de ce guide

Récapitulatif

Un système Transparent Ready comprend deux éléments majeurs :

- le réseau Ethernet sur lequel les équipements échangent les données sur les applications ;
- les services qui permettent les transactions se produisant sur le réseau.

Les trois chapitres qui suivent contiennent des descriptions autonomes des principaux sujets à prendre en considération lorsque vous concevez un nouveau système Transparent Ready ou lorsque vous gérez un système existant. Vous pouvez lire ces chapitres dans n'importe quel ordre en fonction des sujets qui vous intéressent le plus.

Planification, conception et installation physiques

Le *Planification physique, conception et installation d'un réseau Ethernet industriel Transparent Ready*, page 29 décrit la procédure de conception, d'installation et de vérification de votre réseau Ethernet industriel Transparent Ready de sorte à répondre au mieux à vos besoins liés aux applications, en prenant en compte notamment les éléments suivants :

- les normes de conception ;
- le choix du câblage et des composants ;
- la vue d'ensemble de la technologie Internet ;
- les exigences liées à l'environnement ;
- les recommandations relatives à la mise à la terre de protection ;
- le test de votre réseau ;
- l'adressage IP ;
- le routage ;
- la sécurité.

Services Transparent Ready

Le *Vue d'ensemble des services*, page 169 décrit chaque service Transparent Ready, les choix adaptés en termes d'équipement pour chacun d'eux et les équipements Transparent Ready prenant en charge chaque service. La prise en charge des services constitue un critère de sélection d'équipement décisif. En choisissant les services appropriés, vous pouvez prendre en compte les composantes de conception du système suivantes :

- les temps de réponse des équipements appropriés ;
- l'élimination de toute surcharge d'équipement ;
- les besoins liés au débit des applications pour l'ensemble du système.

Ce chapitre explique également comment les différents services fonctionnent et quelles sont leurs performances prévues.

Dépannage

Le *Dépannage*, page 375 fournit des procédures de gestion d'un système Transparent Ready après son installation. Elles décrivent comment :

- identifier des problèmes tels que :
 - les questions liées à l'infrastructure réseau ;
 - incompatibilité entre les équipements.
 - les questions liées aux performances ;
 - l'interférence de l'environnement.
- identifier les sources par :
 - temps de requête et de réponse des équipements ;
 - incompatibilité entre les équipements.
- identifier des solutions telles que :
 - le remplacement des équipements ;
 - la re-conception du système ;
 - des procédures alternatives pour un problème insoluble.

Informations de prise en charge

Un ensemble d'annexes contenant les résultats des mesures de performances est présent à la fin de ce guide. Ces résultats comparent les temps de réponse et débits de différents équipements Transparent Ready utilisant certains des principaux services réseau. Il existe également une section détaillée sur les normes.

Planification physique, conception et installation d'un réseau Ethernet industriel Transparent Ready



Vue d'ensemble

Ce chapitre aborde les aspects relatifs à Ethernet qu'un ingénieur de contrôle ou d'automatisation doit prendre en considération lors de la planification, de l'installation et de la vérification d'un réseau Ethernet industriel de type Transparent Ready.

Lorsque vous concevez un réseau Ethernet industriel Transparent Ready adapté à vos installations, vous devez bien connaître tout ce qui concerne la configuration du réseau, les critères de choix des composants, les aspects spécifiques du processus de conception et les normes existantes applicables à la structure et aux composants des réseaux commerciaux, ainsi qu'au développement des réseaux industriels. Pour plus d'informations, vous pouvez consulter le personnel de votre département informatique ou vous reporter aux nombreuses sources écrites ou électroniques sur le sujet.

La partie Planification contient une description des topologies de réseau, une présentation des normes applicables aux bureaux et aux usines, des considérations générales de conception et des recommandations pour la sélection des composants.

La partie Installation décrit l'installation conforme aux règles CEM et la mise en place des câbles et des connecteurs.

La partie Vérification traite des méthodes applicables à votre réseau.

Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
2.1	Normes requises	30
2.2	Configuration et planification physiques	36
2.3	Exigences liées à l'environnement	76
2.4	Choix des composants Ethernet industriel	86
2.5	Installation	102
2.6	Vérification d'un réseau Ethernet industriel Transparent Ready	125
2.7	Considérations supplémentaires pour la conception d'un réseau Ethernet industriel Transparent Ready	132

2.1 Normes requises

Vue d'ensemble

Les normes Ethernet de bureau font actuellement l'objet d'une révision en vue d'être améliorées et rendues conformes aux exigences Ethernet industriel. Ces normes Ethernet sont compilées avec les normes industrielles en vigueur, afin de mieux représenter l'environnement dans lequel un réseau Ethernet industriel doit fonctionner et d'intégrer ses exigences en matière de performance et de topologie.

De nombreuses normes sont requises pour définir un Ethernet industriel. Ces normes, élaborées et gérées par différentes organisations de normalisation, couvrent les domaines suivants :

- Protocoles
- Couche physique
- Exigences liées à l'environnement
- Structures de câblage
- Caractéristiques des câbles

La plupart de ces normes ont un champ d'application régional et peuvent ne concerner que des régions ou des pays spécifiques.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

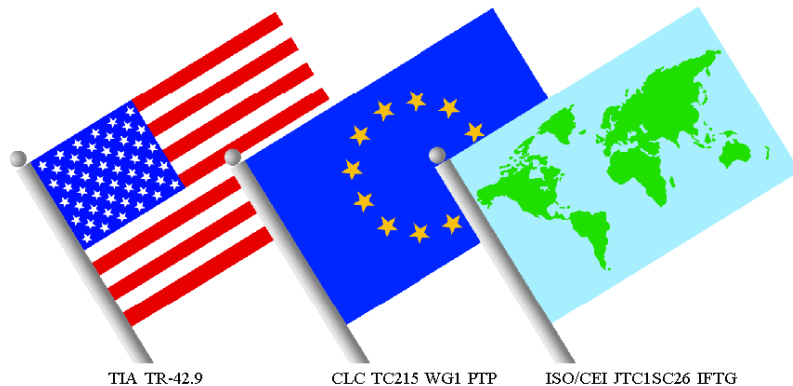
Sujet	Page
Vers une normalisation de l'Ethernet industriel	31
Normes de planification et d'installation requises	34

Vers une normalisation de l'Ethernet industriel

Introduction

Il n'existe actuellement aucune norme de planification Ethernet à laquelle se référer pour obtenir des directives et des réglementations. Néanmoins, de nombreuses recommandations, destinées à l'industrie et basées sur des normes spécifiques aux environnements de bureau (TIA/EIA-568-B, ISO/CEI-11801 et EN 50173), ont été préparées et soumises aux comités de normalisation par plusieurs organisations de réseau industriel.

L'effort de normalisation internationale le plus considérable a été mené par un groupe d'experts appartenant aux organisations CEI TC65, TIA TR-42.9 et CENELEC TC215 WG1. Leurs travaux seront publiés sous la norme ISO/CEI 24702.



Norme ISO/CEI 24702 : calendrier et définitions

La publication de la norme ISO/CEI 24702 est prévue pour l'année 2006.

La norme ISO/CEI 24702 définit le câblage générique pour les bâtiments industriels et les configurations informatiques associées. La définition du câblage équilibré et de la fibre optique est tirée de la norme ISO/CEI 11801, notamment en ce qui concerne :

- les applications ;
- les classes de transmission des liaisons et des voies ;
- les performances de transmission des composants.

Cette norme introduit également de nouveaux concepts, tels que l'environnement de classification (voir tableau MICE ci-dessous), des composants adéquats et une structure de câblage modifiée.

Indice mécanique du concept MICE

Le groupe de travail CEI TC65C a créé le concept MICE d'indice mécanique afin de définir les paramètres d'environnement et leurs exigences. Les trois classes d'environnement de MICE sont :

- Classe 1 : environnement général (non industriel/non résidentiel)
- Classe 2 : environnement industriel léger
- Classe 3 : environnement industriel lourd

Il définit également les paramètres d'environnement suivants (dont les initiales des termes anglais forment le sigle MICE) :

- mécaniques (**m**echanical) ;
- de pénétration de corps étrangers (**i**ngress) ;
- climatiques (**c**limatic) ;
- électromagnétiques (**e**lectromagnetic).

Chaque paramètre d'environnement est défini par un indice de niveau : (1) niveau faible , (2) niveau moyen et (3) niveau élevé. Celui-ci est ajouté en indice à côté de chaque lettre de paramètre, par exemple $M_2I_2C_3E$. Comme le montre cet exemple, les niveaux des paramètres peuvent être combinés et varier au sein d'une même voie.

Chaque classe d'environnement comporte un scénario du pire des cas, comme indiqué ci-après :

- $M_1I_1C_1E_1$: pour un environnement général (ISO/CEI 11801)
- $M_2I_2C_2E_2$: pour un environnement industriel léger
- $M_3I_3C_3E_3$: pour un environnement industriel lourd

Le tableau MICE est représenté ci-dessous :

		--->Gravité croissante--->		
		Classe		
Paramètres mécaniques	Chocs/à-coups	M_1	M_2	M_3
	Vibrations			
	Effort de traction			
	Ecrasement			
	Impacts			
Pénétration de corps étrangers	Particules	I_1	I_2	I_3
	Immersion			

		--->Gravité croissante--->		
		Classe		
Paramètres climatiques	Température	C ₁	C ₂	C ₃
	Air ambiant			
	Taux de variation			
	Humidité			
	Rayonnement UV			
	Rayonnement solaire			
	Pollution liquide			
	Pollution par les gaz			
Paramètres électromagnétiques	Décharges électrostatiques	E ₁	E ₂	E ₃
	Radiofréquences rayonnées			
	Radiofréquences conduites			
	Transitoires rapides			
	Surtension			
	Champ magnétique			

ISO/CEI 24702 : Unification des principaux comités de normalisation

Le groupe de travail sur le câblage des locaux du client (ISO/CEI JTC 1 SC 25 WG3) a été créé afin d'éviter les développements propriétaires. Ce groupe a ensuite créé un nouveau groupe de travail, dédié aux locaux industriels (ISO/CEI JTC 1 SC 25 WG3.IPTG). Afin d'optimiser la coopération et d'accélérer le développement d'une norme internationale, le groupe en charge des locaux industriels a travaillé directement avec les experts des principaux comités des organisation de normalisation (CEI TC65C, TIA TR42.9 et CENELEC TC215 WG1). La mission de ce nouveau groupe est de normaliser les caractéristiques des systèmes de câblage pour les sites industriels. La norme sera publiée sous le nom ISO/CEI 24702.

Le groupe de travail dédié aux locaux industriels est mené conjointement par les sous-comités ISO/CEI JTC 1/SC 25 et CEI SC 65C :

- le sous-comité JTC 1/SC 25 est en charge du câblage pour les chantiers de construction ;
- le sous-comité CEI SC 65C a la charge du câblage pour le contrôle des processus. Le sous-comité CEI SC 65C est un sous-comité du CEI TC65C, chargé de développer les normes pour les réseaux industriels.

En attendant la publication de la norme ISO/CEI 24702, Schneider Electric vous recommande de suivre les indications fournies dans ce chapitre.

Normes de planification et d'installation requises

Normes Ethernet

La norme Ethernet à prendre en compte lorsque vous planifiez un réseau Ethernet industriel est celle définie par l'IEEE et adoptée par ISO/CEI, à savoir :

Norme IEEE 802.3, Edition 2002, Partie 3 : Méthode d'accès par détection de porteuse avec accès multiples et détection de collision (CSMA/CD) et spécifications pour la couche physique.	IEEE 802.3
Technologie de l'information. Télécommunications et échange d'information entre systèmes. Partie 3 : Accès multiple par surveillance du signal et détection de collision (CSMA/CD)	ISO/CEI 8802-3

Normes de câblage informatique structuré

Les fabricants de câbles, les fournisseurs, les concepteurs de bâtiments, les architectes réseaux et les techniciens d'entretien s'appuient tous sur des normes de câblage pour définir des spécifications pour leurs projets. Ces spécifications englobent tous les aspects des phases de planification, de conception et d'installation, ainsi que la configuration, les performances, les tests de conformité et la vérification du système final.

Les trois normes internationales indiquées dans le tableau ci-dessous font référence en matière de planification du câblage, de sélection, d'installation et de performance des réseaux informatiques. Chacune de ces normes est basée sur celle qui la précède. Elles sont donc toutes très similaires.

Zone d'application et norme		Organisations de normalisation	Description
Etats-Unis	TIA/EIA-568-B	Telecommunications Industry Association	Norme de câblage des télécommunications des immeubles commerciaux – Définit comment concevoir, mettre en place et gérer un système de câblage structuré.
		Electronic Industries Association	
Internationale	ISO/CEI 11801	Organisation internationale de normalisation	Norme de câblage générique des locaux du client – Définit, à partir de la norme TIA/EIA-568, les caractéristiques générales de câblage pour les locaux du client.
		International Engineering Consortium	
Europe	CENELEC EN 50173	Comité Européen de Normalisation Electrotechnique	Définit, à partir de la norme ISO 11801, le câblage générique et les composants de câblage sur le marché européen.

Normes environnementales

Les normes environnementales ne s'appliquent pas spécifiquement au réseau Ethernet industriel, mais à tout appareil ou équipement situé dans un environnement particulier.

Schneider Electric a défini trois types d'environnements, coïncidant avec le classement MICE :

- Environnement de bureau où un réseau Ethernet standard peut être utilisé
- Environnement industriel léger
- Environnement industriel lourd

Les exigences environnementales propres au réseau Ethernet industriel sont définies par les mêmes spécifications que celles s'appliquant aux automates industriels (*voir page 76*).

2.2 Configuration et planification physiques

Vue d'ensemble

Ce sous-chapitre présente les différentes normes de câblage applicables à un réseau Ethernet industriel. Il décrit également les configurations appropriées pour un réseau industriel Transparent Ready. De plus, afin de vous aider à mieux comprendre cette structure, une synthèse des topologies de réseau de base est fournie. Enfin, il couvre les technologies LAN et les problèmes liés à un réseau Ethernet industriel, ainsi que les technologies WAN et le matériel associé.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Planification de câblage Ethernet industriel	37
Normes de câblage structuré	38
Câblage dans un système Ethernet industriel Transparent Ready	42
Présentation de la structure de base d'un réseau	47
Développement d'architecture réseau pour les réseaux Ethernet industriel	54
Topologie en anneau redondant	59
Technologies LAN et conception réseau	61
Matériel LAN	66
Autres considérations LAN	69
Technologies WAN et conception réseau	70
Matériel WAN	73

Planification de câblage Ethernet industriel

Introduction

Etant donné qu'il n'existe pas encore de normes définies pour la configuration physique d'un réseau Ethernet industriel, Schneider Electric a choisi de se conformer aux recommandations émises par les organisations de normalisation telles que Modbus-IDA, IAONA, PNO et aux travaux en cours de la CEI.

Un site de fabrication industriel est une installation physique dans laquelle se déroulent des activités de contrôle des processus ou de fabrication. Dans la plupart des cas, le site se compose de plusieurs bâtiments ou usines qui gèrent des processus interconnectés, mais distincts. La configuration physique et les variables environnementales inhérentes à chacune de ces installations peuvent entraîner des exigences de câblage différentes, propres à chaque site. Ce sous-chapitre décrit les recommandations de Schneider Electric en matière de planification des réseaux Ethernet industriel dans les environnements de contrôle des processus et de fabrication.

Planification du câblage

Un plan de site réseau définit la configuration logique et physique d'un réseau spécifique aux exigences de votre site. Ce plan constitue un élément important du processus de conception du réseau dans votre installation. Le site peut être une installation industrielle ou un site d'infrastructure. Les sites d'infrastructure sont des environnements, tels que les tunnels, les usines de traitement des eaux et les aéroports, qui présentent des exigences supplémentaires par rapport à un site industriel. Les deux types de sites incluent des variables environnementales parfois extrêmes par rapport aux environnements de bureau. Les normes existantes sur les environnements de bureau, même si elles s'avèrent utiles et valides, ont une application limitée dans ces environnements. Les performances d'application, dans des conditions environnementales strictes (conditions climatiques et protection contre la pénétration de corps étrangers comprises), sont de prime importance dans les environnements industriels.

Les rubriques suivantes fournissent des informations générales sur la planification d'un réseau Ethernet industriel pour des applications d'infrastructures et industrielles. Ces informations ne prétendent pas couvrir toutes les variantes possibles de ces deux environnements. Vous devez donc les adapter aux besoins spécifiques de votre site.

Normes de câblage structuré

Introduction

Schneider Electric recommande l'utilisation de normes de câblage structuré, comme les normes TIA/EIA 568B, ISO/CEI 11801 et CENELEC EN 50173 (*voir page 34*). Des normes de câblage sont en cours de développement par un groupe de travail composé des représentants des diverses organisations de normalisation.

Eléments d'un système de câblage

Le tableau ci-dessous répertorie les éléments d'un système de câblage défini par la norme ISO/CEI 11801. Cette norme identifie également les interfaces via lesquelles les différents composants du réseau sont connectés au système de câblage.

Eléments (par ordre hiérarchique)	Abréviation	Objectif
Répartiteur campus	CD	Répartiteur d'où émane le câble du réseau fédérateur campus
Câble du réseau fédérateur campus		Câblage entre bâtiments partageant les mêmes installations de télécommunications
Répartiteur bâtiment	BD	Répartiteur où termine le câble du réseau fédérateur bâtiment et d'où partent les connexions au câble du réseau fédérateur campus
Câble du réseau fédérateur bâtiment		Câble intermédiaire et matériel de connexion
Répartiteur sol	FD	Connexion du système de câbles horizontal aux autres sous-systèmes de câblage
Câble horizontal		Câblage entre la prise de télécommunications, incluse, et le répartiteur horizontal
Point de transition (facultatif)	TP	Point de connexion, dans le sous-système de câblage horizontal, du câble plat "sous-tapis" au câble rond
Prise de télécommunications	TO	Prise de télécommunications femelle qui se trouve dans la zone de travail

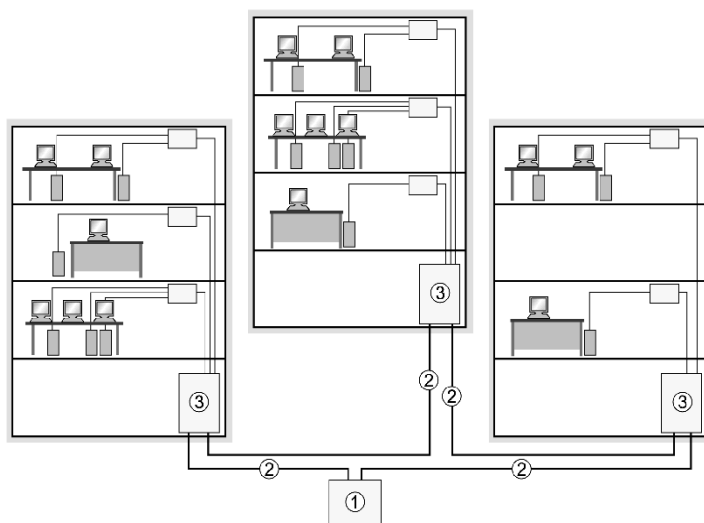
Sous-systèmes de câblage

Pour qu'une installation de câblage soit conforme à la norme ISO/CEI 11801, la configuration doit connecter les sous-systèmes suivants d'un système de câblage :

- réseau fédérateur campus : les campus utilisent des répartiteurs bâtiment ;
- réseau fédérateur bâtiment : chaque bâtiment comporte un répartiteur bâtiment ;
- câblage horizontal : chaque sol comporte un répartiteur sol.

Structure des systèmes de câblage

Le système de câblage générique défini par la norme ISO/CEI 11801 est une structure en étoile (*voir page 49*) hiérarchique. Le schéma ci-dessous illustre un répartiteur campus central et un système de câblage de réseau fédérateur campus reliant plusieurs répartiteurs bâtiment. Chaque bâtiment doit avoir au moins un répartiteur bâtiment. Chaque répartiteur bâtiment est connecté au répartiteur campus central à l'aide d'une topologie en étoile. Le répartiteur campus devient l'unité de communication centrale. Par mesure de sécurité et de secours, il est conseillé de créer des liaisons redondantes entre les bâtiments. Au sein d'un bâtiment, chaque étage dispose de son propre répartiteur sol qui dessert jusqu'à 2 000 m² de superficie de bureaux.



- 1 Répartiteur campus central
- 2 Câblage de réseau fédérateur campus
- 3 Répartiteur bâtiment

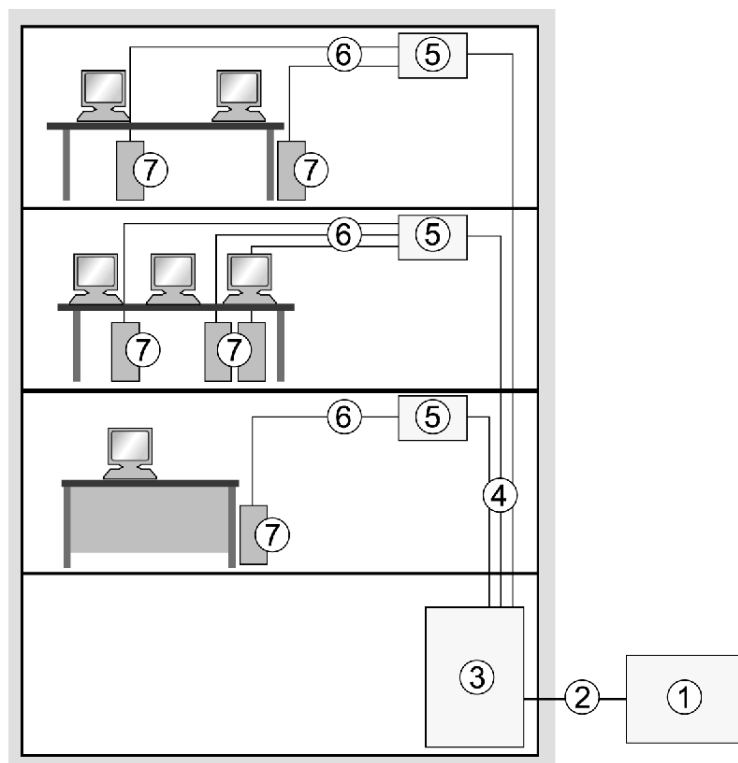
Dans un campus constitué d'un seul bâtiment, le point de répartition principal devient le répartiteur bâtiment de ce bâtiment. Cependant, lorsque le bâtiment est assez large, il peut se comporter comme un campus et disposer d'un réseau fédérateur campus avec plusieurs répartiteurs bâtiment.

Le nombre de sous-systèmes et le type d'éléments inclus dans votre implémentation dépend des facteurs suivants :

- taille du campus ou du bâtiment ;
- géographie du site ;
- objectif du système de câblage (applications et équipements) ;
- types d'utilisateur final.

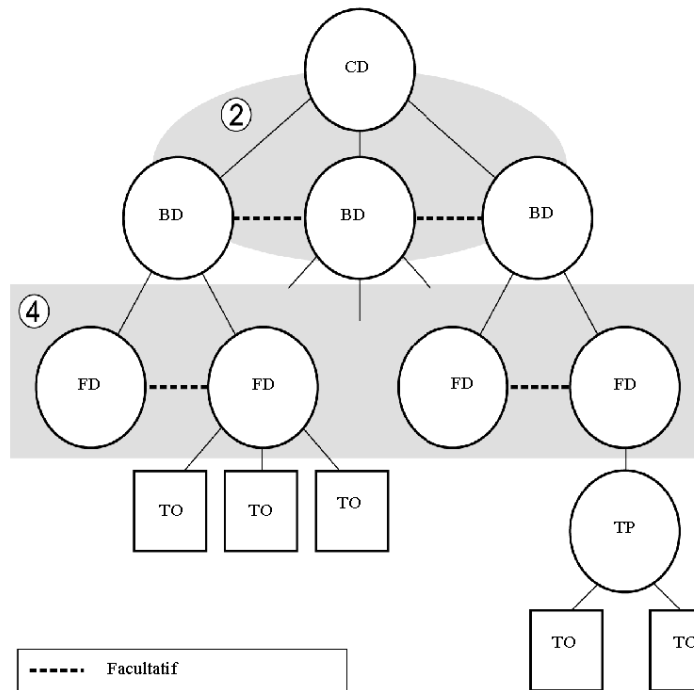
Configuration

Il est possible de configurer un système de câblage générique ciblé sur vos besoins spécifiques en réorganisant les répartiteurs selon différentes topologies (voir page 47), telles que bus, étoile et anneau. Le schéma ci-dessous illustre les connexions linéaires d'un système de câblage partant du répartiteur campus à l'équipement et à la prise de terminal.

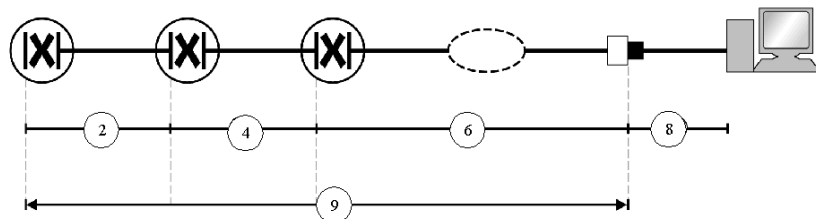


- 1 Répartiteur campus
- 2 Câblage de réseau fédérateur
- 3 Répartiteur bâtiment
- 4 Câblage secondaire
- 5 Répartiteur sol
- 6 Câblage tertiaire
- 7 Prise de télécommunications

Les deux schémas suivants montrent comment implémenter physiquement un système de câblage générique dans un seul bâtiment ou dans plusieurs bâtiments le long d'un réseau fédérateur campus.



- 2 Câblage de réseau fédérateur
4 Câblage secondaire



- 2 Câblage de réseau fédérateur
4 Câblage secondaire
6 Câblage tertiaire
8 Câble de raccordement
9 Système de câblage générique

Câblage dans un système Ethernet industriel Transparent Ready

Introduction

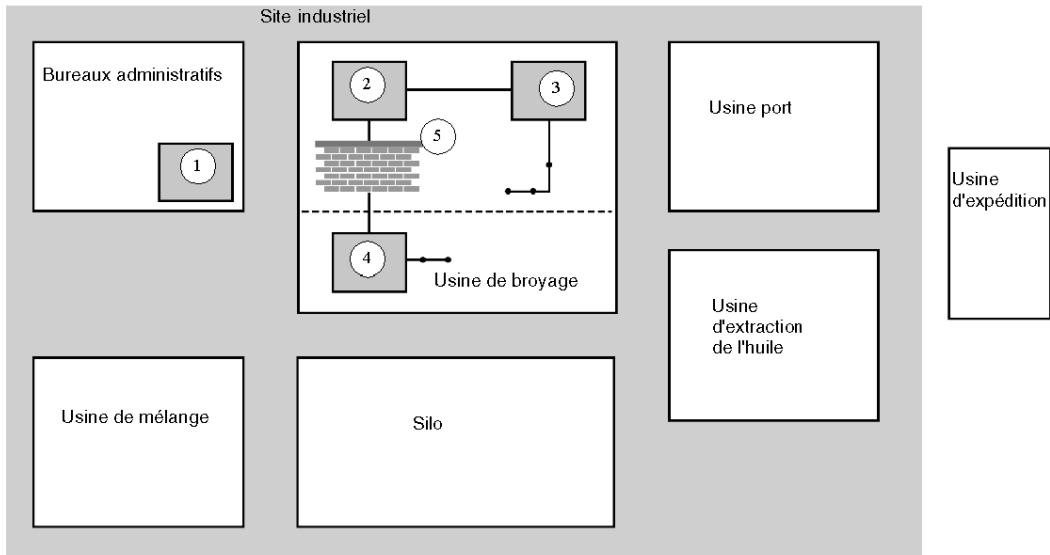
L'approche Transparent Ready de planification d'un système de câblage est similaire à celle des organisations Ethernet industriel telles que Modbus-IDA, basées sur les normes ISO/CEI 11801, EN 501731 et TIA/EIA 568B agréées.

Exemple de site multiusine

Le schéma ci-dessous présente un système de câblage avec les paramètres suivants :

- répartiteur de site industriel agissant comme unité de communication centrale à la place d'un répartiteur de campus (*voir page 38*) et connectant les répartiteurs usine sur un réseau fédérateur de site industriel ;
- répartiteurs usine connectant des répartiteurs bureau et répartiteurs sol usine sur un réseau fédérateur d'usine ;
- répartiteurs sol usine se connectant aux répartiteurs armoire (CD, également appelés répartiteurs machine ou terrain, FD) ainsi qu'aux équipements et aux prises équipement (DO) situés à l'intérieur de l'armoire ;
- répartiteurs bureau se connectant aux prises de télécommunication, elles-mêmes raccordées aux imprimantes et ordinateurs.

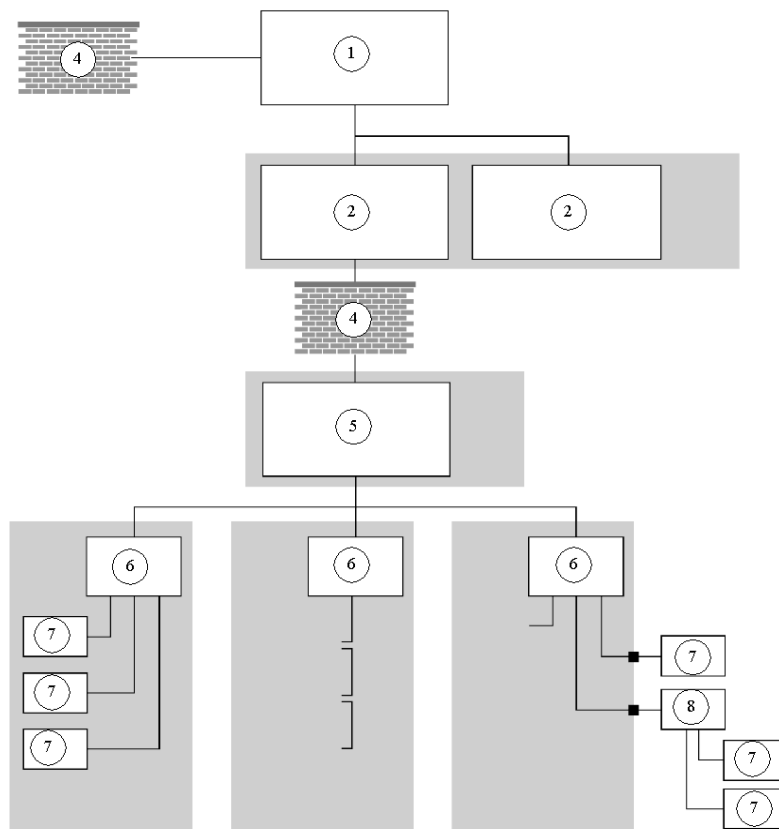
Il est important de savoir qu'un site peut englober plusieurs usines. L'exemple suivant illustre une vue d'ensemble d'un site céréalier contenant 6 usines.



- 1 SD Répartiteur site
- 2 PD Répartiteur usine
- 3 POD Répartiteur bureau
- 4 PFD Répartiteur sol usine
- 5 FW Coupe-feu

Exemple de site à une usine

L'exemple suivant illustre une vue rapprochée d'une usine au sein du site céréalier représenté ci-dessus.



- 1 SD Répartiteur site
- 2 PD Répartiteur usine
- 3 POD Répartiteur bureau
- 4 FW Coupe-feu
- 5 PFD Répartiteur sol usine
- 6 CD Répartiteur armoire
- 7 DO Prise équipement
- 8 FD Répartiteur terrain

Répartiteur de site industriel

Le répartiteur de site industriel se comporte comme un répartiteur campus pour la norme ISO/CEI 11801, correspondant au répartiteur d'où émane le câble du réseau fédérateur. Ce répartiteur est géré par le personnel informatique et peut consister en un ou plusieurs équipements (commutateurs en bâti) à ports multiples. Il est généralement situé dans un environnement bureautique et fournit à l'ensemble du site de fabrication une connexion à Internet et aux autres sites physiques de la même entreprise ou entité. Le trafic entrant et sortant du site est isolé par un routeur (*voir page 73*) et sécurisé par un coupe-feu.

Réseau fédérateur de site industriel

Le réseau fédérateur de site industriel est le système de câblage acheminé du répartiteur de site industriel vers les répartiteurs usine. En général, le site industriel est un anneau auto-régénérant (*voir page 56*) pouvant être configuré en redondance avec un double anneau auto-régénérant (*voir page 59*).

Répartiteur usine

Le répartiteur usine connecte le réseau fédérateur du site industriel à une usine. Il se comporte comme un répartiteur bâtiment. La majorité des sites industriels se compose de plusieurs usines distinctes. Chacune de ses usines peut disposer de salles de contrôle du fonctionnement général de l'usine ou de centres commande moteur où sont situés le MCC et les équipements de contrôle. Généralement, le répartiteur usine est situé dans la salle de contrôle ou dans le centre MCC. L'exigence liée à l'environnement du répartiteur usine implique soit des bureaux, soit un site industriel léger.

Répartiteur bureau et répartiteur sol usine

Comme mentionné précédemment, le répartiteur usine est généralement situé dans la salle de contrôle ou le centre MCC ; le répartiteur usine est connecté aux autres répartiteurs, comme le répartiteur bureau et le répartiteur sol usine. Le répartiteur bureau gère les prises de terminal des bureaux de l'usine. Ces terminaux sont utilisés pour raccorder les imprimantes, ordinateurs et équipements de visioconférence. Le répartiteur sol usine gère les équipements posés sur le sol de l'usine. Dans la plupart des cas, ces deux répartiteurs sont situés soit dans des bureaux, soit dans un environnement industriel léger. Le répartiteur bureau est normalement géré et maintenu par le personnel informatique. Le répartiteur sol usine est, lui, géré par le personnel responsable des répartiteurs armoire (également appelés répartiteurs machine ou terrain). Le trafic entre le répartiteur sol et le répartiteur usine est isolé au moyen d'un routeur et sécurisé par un coupe-feu.

Répartiteurs armoire, terrain et machine

En règle générale, les armoires renferment des équipements avec peu de ports ou de connexions, comme les commutateurs. Les répartiteurs armoire (également appelés répartiteurs machine ou terrain) fournissent une connectivité aux équipements situés à l'intérieur d'une armoire, dans une machine ou posés sur le sol de l'usine.

Le tableau ci-dessous indique les exigences liées à l'environnement selon l'emplacement des équipements.

Emplacement des équipements	Exigences liées à l'environnement
A l'intérieur d'une armoire	Environnement industriel léger
Dans une machine	Environnement industriel léger ou lourd
Sur le sol de l'usine	Environnement industriel lourd

La configuration à l'intérieur des armoires est en étoile ou en chaîne (en utilisant des équipements à deux ports Ethernet). La rubrique suivante (*voir page 47*) présente certaines topologies de réseau classiques et explique comment les développer dans un environnement Ethernet. Ces topologies sont généralement déployées à partir du répartiteur sol usine. Les prises équipement (DO) sont situées à l'intérieur de l'armoire. Si les équipements sont posés sur le sol de l'usine, il peut s'agir soit d'une prise équipement, soit d'un nouveau répartiteur dédié aux équipements sur le terrain (appelé dans ce cas répartiteur terrain, ou FD).

Présentation de la structure de base d'un réseau

Récapitulatif

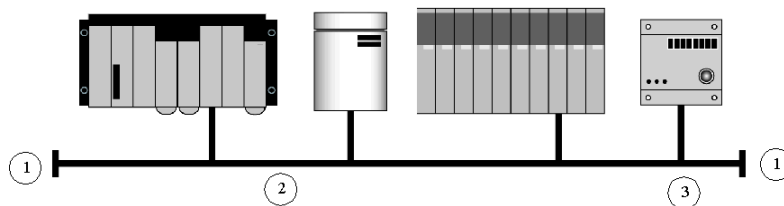
Un réseau constitué de câbles, de composants et d'équipements peut avoir plusieurs architectures ou topologies :

- Bus
- Etoile
- Chaînage
- Anneau
- Double anneau
- Maillage

Cette section fournit des illustrations de chaque type de topologie. Chacune a ses avantages et ses inconvénients, comme indiqué dans les tableaux ci-dessous. Les commutateurs et concentrateurs appropriés sont mentionnés pour chaque architecture de réseau. La topologie recommandée par Schneider Electric est également décrite.

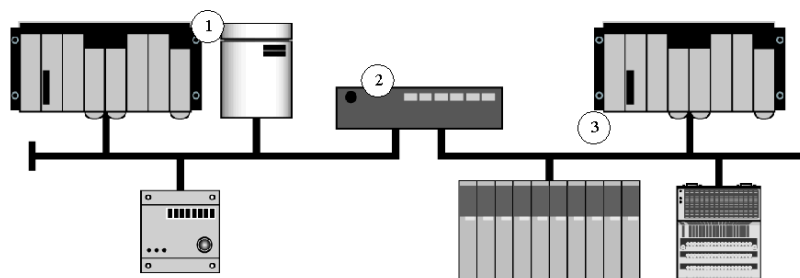
Topologie de bus

La topologie de bus présente une architecture similaire à celle d'un réseau d'automatisation plus traditionnel comme Modbus Plus. Un câble fédérateur connecte tous les équipements du réseau. Des terminaisons sont placées à chaque extrémité du réseau fédérateur pour envoyer et effacer les signaux sur le réseau. Les équipements, généralement reliés à l'aide de connecteurs en T, peuvent être installés n'importe où le long du bus.



- 1 Terminaison
- 2 Câble du réseau fédérateur
- 3 Connecteur en T

Une partie du câble fédérateur est appelée *segment*. Il est possible de connecter plusieurs segments à l'aide de ponts ou de répéteurs, comme illustré ci-dessous.



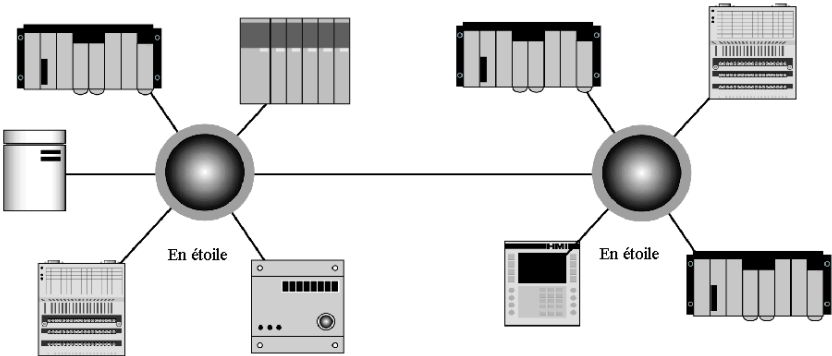
- 1 Segment 1
- 2 Répéteur
- 3 Segment 2

Seul un équipement à la fois peut envoyer ou transmettre un paquet d'informations. Le paquet transite dans l'intégralité du câble fédérateur du bus. Voilà pourquoi la topologie de bus est considérée comme un support partagé. Les terminaisons sont très importantes car une rupture du câble peut bloquer toute communication entre les équipements.

Avantages	Inconvénients
Faible coût.	L'évolutivité pose problème. Il est difficile d'adapter le réseau à mesure que vos besoins évoluent. Lorsque le trafic et le nombre d'équipements augmentent, les performances du réseau diminuent.
Simplicité d'installation. Tous les équipements du réseau sont connectés à un segment du câble. Tout ce dont vous avez besoin, c'est d'une longueur de câble suffisante pour relier vos équipements.	Les équipements sont généralement reliés au câble principal à l'aide de boîtiers. En cas de perte d'un équipement ou d'un segment, tous les équipements situés en aval deviennent indisponibles.
Le câble fédérateur suit un trajet qui couvre toute l'usine, à l'image d'un réseau d'automatisation propriétaire, ce qui en rend la conception facilement compréhensible par les concepteurs qui s'initient aux applications Ethernet utilisées dans le secteur de l'automatisation.	Comme tous les équipements partagent le même câble fédérateur, le débit est limité. Un seul équipement peut communiquer à la fois. La vitesse de tous les équipements d'un réseau de bus doit être identique.

Topologie en étoile

Dans une topologie en étoile, tous les équipements sont reliés à un équipement central. Cette topologie est très fréquente dans les environnements professionnels ainsi que dans les environnements d'automatisation récents.



Dans une topologie en étoile, les équipements utilisent des sections dédiées du réseau pour différents services.

Avantages	Inconvénients
Le débit du réseau est bien plus élevé que sur un réseau à topologie de bus.	Les topologies en étoile sont plus onéreuses car un câble dédié doit relier chaque équipement. Pour compenser cet inconvénient, les composants du réseau (commutateurs, concentrateurs, etc.) sont placés dans des armoires situées dans l'usine elle-même, ce qui permet de connecter tout un groupe d'équipements locaux. Il suffit de faire courir un câble vers un point central pour prendre en charge le groupe, évitant ainsi d'utiliser des câbles séparés pour chaque équipement.
La reconfiguration du réseau est bien plus facile.	
La centralisation des composants du réseau simplifie l'administration. De plus, la gestion centralisée et la surveillance du trafic améliorent les performances du réseau.	
Les diagnostics sont simples. En cas de défaillance d'un segment du réseau, seuls les équipements reliés directement à ce segment sont concernés.	
Les composants d'infrastructure utilisent un logiciel de surveillance et les voyants des équipements pour signaler les défaillances. La plupart du temps, les points de défaillance uniques font l'objet d'un diagnostic et d'une réparation rapides.	
Résilience. La défaillance d'un câble n'entraîne la mise hors service que de l'équipement concerné.	
Un réseau à topologie en étoile peut compter davantage d'équipements qu'un réseau à topologie de bus.	

Topologie de chaînage

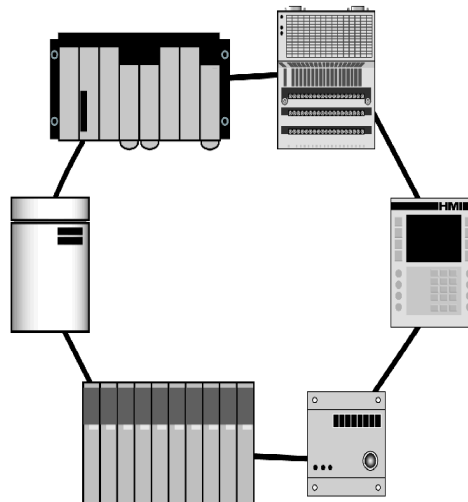
Dans une topologie de chaînage, l'équipement fait partie du câble principal, contrairement à la topologie de bus où l'équipement est relié au câble via un boîtier et n'est pas considéré comme faisant partie intégrante du câble principal. Dans une chaîne, chaque équipement a deux ports réseau et les informations circulent à travers l'équipement. Bien que la chaîne soit linéaire, il existe des équipements de dérivation qui permettent de développer des topologies plus complexes.

L'Interbus est un exemple de réseau à topologie de chaînage.

Avantages	Inconvénients
Faible coût. Les boîtiers sont inutiles.	En cas de défaillance d'un équipement dans une configuration linéaire, le réseau est coupé.
	Si la conception n'est pas adéquate, il est possible que les équipements d'une chaîne aient quelques problèmes pour gérer l'afflux des informations qui les traversent.
	Risque de surcharge du réseau. Tous les équipements partagent le même câble principal.

Topologie en anneau

Dans une topologie en anneau, tous les équipements ou composants de l'infrastructure du réseau sont reliés dans une boucle sans fin. Les paquets circulent d'un équipement à l'autre dans une seule direction au sein de l'anneau. Chaque équipement vérifie la destination du paquet qu'il reçoit et le transmet à l'équipement suivant.

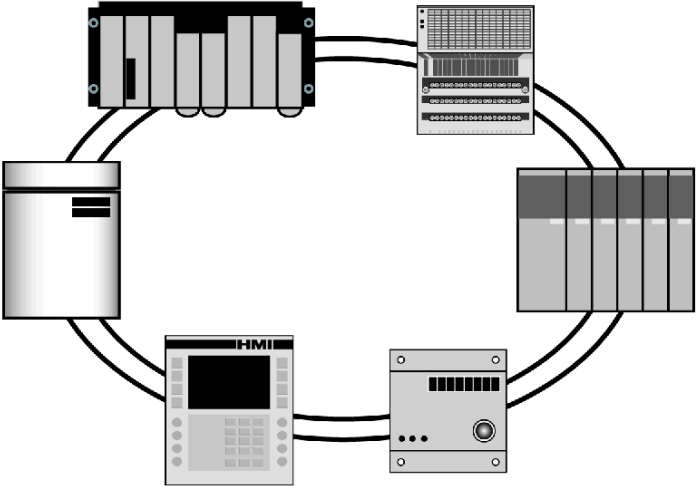


Les topologies en anneau assurent la redondance. En cas de défaillance d'une liaison, le trafic est acheminé dans la direction opposée. Un anneau fonctionne selon une rotation de jeton ou un accès aléatoire/partagé. Dans le cas d'un réseau commuté, tous les équipements ont accès au réseau en même temps à des vitesses différentes.

Avantages	Inconvénients
Redondance. La défaillance d'une liaison ou d'un composant de l'infrastructure du réseau n'affecte pas le réseau en entier.	Coût élevé. Le câblage nécessaire pour constituer l'anneau est plus important.
Une topologie en anneau utilise un logiciel pour surveiller les liaisons du réseau.	Les composants d'infrastructure du réseau ont besoin d'intelligence pour répondre aux défaillances des équipements. Ils coûtent plus chers que les composants utilisés dans les topologies de bus ou en étoile.

Topologie à double anneau

La topologie à double anneau est déployée lorsque des systèmes industriels d'automatisation sont utilisés dans des applications stratégiques où l'indisponibilité du système n'est pas envisageable.



Un double anneau possède toutes les fonctionnalités d'un anneau simple, mais offre une meilleure tolérance aux pannes. Il est constitué de composants d'infrastructure reliés entre eux par plusieurs anneaux. Chaque équipement est connecté à deux composants d'infrastructure. Chaque composant d'infrastructure est relié à un anneau séparé. Même en cas de défaillance d'une liaison ou d'un équipement d'infrastructure, les autres équipements peuvent communiquer.

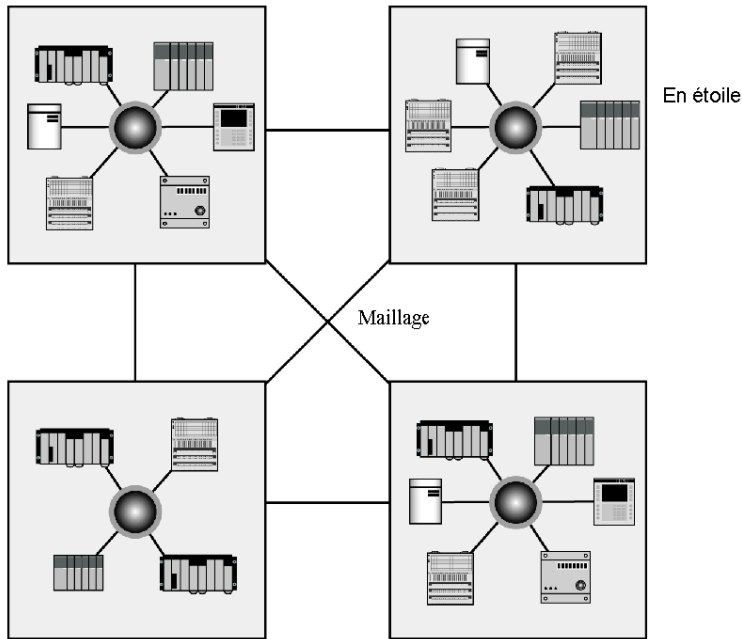
Les topologies à double anneau utilisées dans les environnements d'automatisation proposent des fonctionnalités que les environnements traditionnels de communication de données n'offrent pas toujours. Par exemple, des liaisons à redondance d'UC sont utilisées entre les anneaux. Lorsqu'une liaison connaît une défaillance, la liaison redondante prend le relais et empêche toute interruption des communications au sein du réseau. Des paquets dits " chiens de garde " sont envoyés aux connexions inactives. Ils consignent des informations dans des journaux si la connexion reste inactive. Les entrées créées par ces paquets sont contrôlées par l'administrateur du réseau.

Avantages	Inconvénients
Redondance. La défaillance de plusieurs équipements ou câbles ne bloque pas les communications au sein du réseau.	Coût. Par rapport à une topologie en anneau, le nombre d'équipements est doublé.
Chaque anneau requiert des alimentations séparées.	Les liaisons inutilisées doivent faire l'objet de contrôles réguliers pour s'assurer de leur bon fonctionnement en cas de besoin.
Plusieurs interfaces d'un équipement peuvent connecter ce dernier à différents anneaux, de sorte qu'un nombre trop important de collisions ou de trafic de diffusion dans un anneau n'entraîne pas le blocage du système.	

Topologie de maillage

La topologie de maillage est utilisée dans les réseaux très importants ou les fédérateurs de réseaux, dans lesquels chaque équipement terminal ou d'infrastructure est connecté à un ou plusieurs composants du réseau. Idéalement, chaque équipement est relié directement à tous les autres au sein du maillage.

La topologie de maillage peut également prendre la forme d'un fédérateur de réseau qui relie plusieurs structures en étoile. Cette topologie combinée garantit une tolérance aux pannes au réseau fédérateur, sans le coût élevé lié à la mise en place d'une topologie de maillage dans l'ensemble du réseau.



Les topologies de maillage sont moins fréquentes en raison de leur coût et de leur complexité.

Avantages	Inconvénients
Tolérance aux pannes. En cas de rupture d'un segment du câble du réseau, le trafic est acheminé par un autre itinéraire.	Complexité. Gestion et administration compliquées.
	Coût élevé. Les connexions redondantes requièrent un câblage et un nombre d'interfaces plus importants.

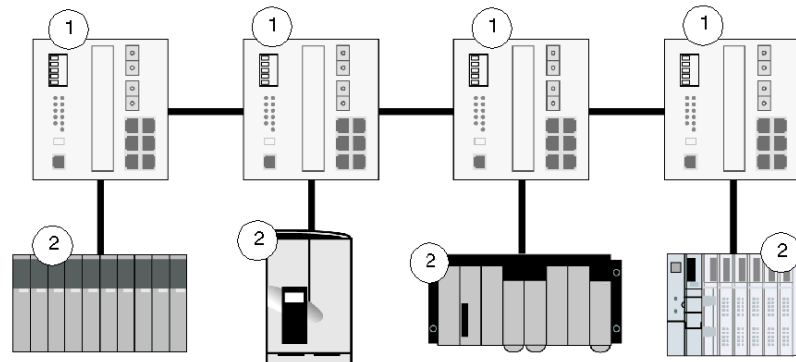
Développement d'architecture réseau pour les réseaux Ethernet industriel

Introduction

Outre des connaissances de base en architecture réseau (topologies) et en réseau Ethernet pour les environnements de bureau, d'autres aspects sont à assimiler lorsque vous déployez Ethernet dans un environnement industriel. Les diverses topologies et leur application dans une configuration d'automatisation industrielle sont décrites ci-après, avec quelques suggestions de matériel adéquat.

Topologie en bus Ethernet

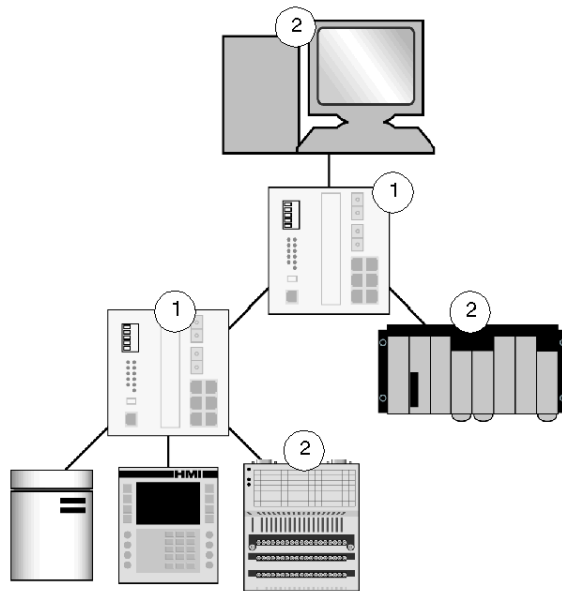
Un bus Ethernet peut être déployé en interconnectant des concentrateurs et/ou des commutateurs en ligne et en considérant chacun d'eux comme point de connexion d'un équipement. Toutefois, il n'est possible d'interconnecter qu'un nombre limité de concentrateurs, contre un nombre illimité de commutateurs.



- 1 Commutateurs Ethernet
- 2 Equipements Ethernet

Topologie en étoile Ethernet

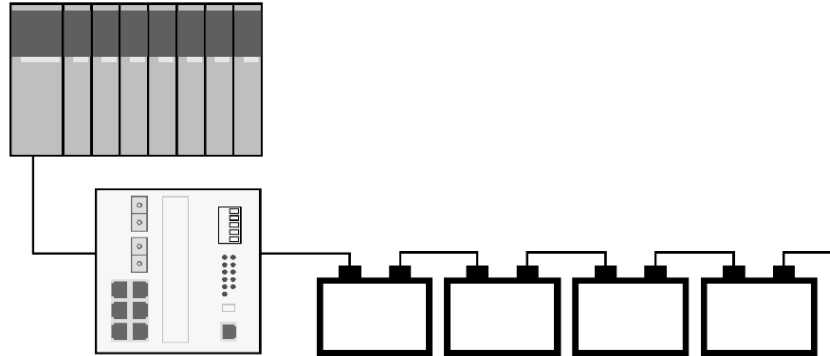
Dans une topologie Ethernet en étoile, l'équipement intermédiaire peut être soit un concentrateur, soit un commutateur. La topologie en étoile est la plus répandue dans les réseaux de bureau et a été adoptée dans la plupart des applications d'automatisation. Pour les applications Ethernet industriel, l'utilisation d'un commutateur Full Duplex comme équipement central à la place d'un concentrateur est fortement préconisée.



- 1 Commutateurs Ethernet
- 2 Equipements Ethernet

Topologie en chaînage Ethernet

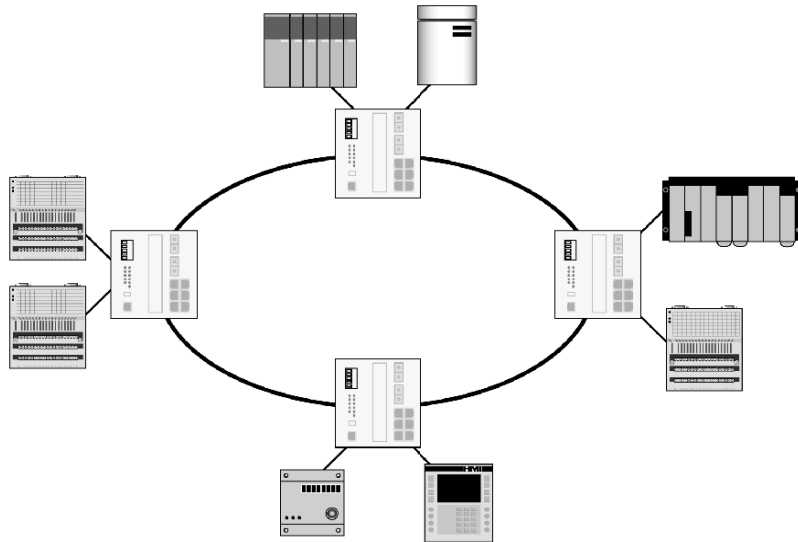
Pour déployer un réseau en chaînage Ethernet, des équipements avec doubles ports Ethernet sont requis. Schneider Electric est actuellement en train de développer des équipements Ethernet industriel dotés de cette fonctionnalité (doubles ports Ethernet pour une connectivité en chaînage).



Topologie en anneau Ethernet

Les anneaux Ethernet forment généralement le réseau fédérateur pour les applications à haute disponibilité. Deux chemins sont disponibles pour atteindre le même équipement. Si une topologie en anneau est nécessaire, des commutateurs prenant en charge soit une topologie en anneau propriétaire, soit un protocole d'arbre recouvrant (arbre recouvrant ou arbre recouvrant rapide) doivent alors être utilisés.

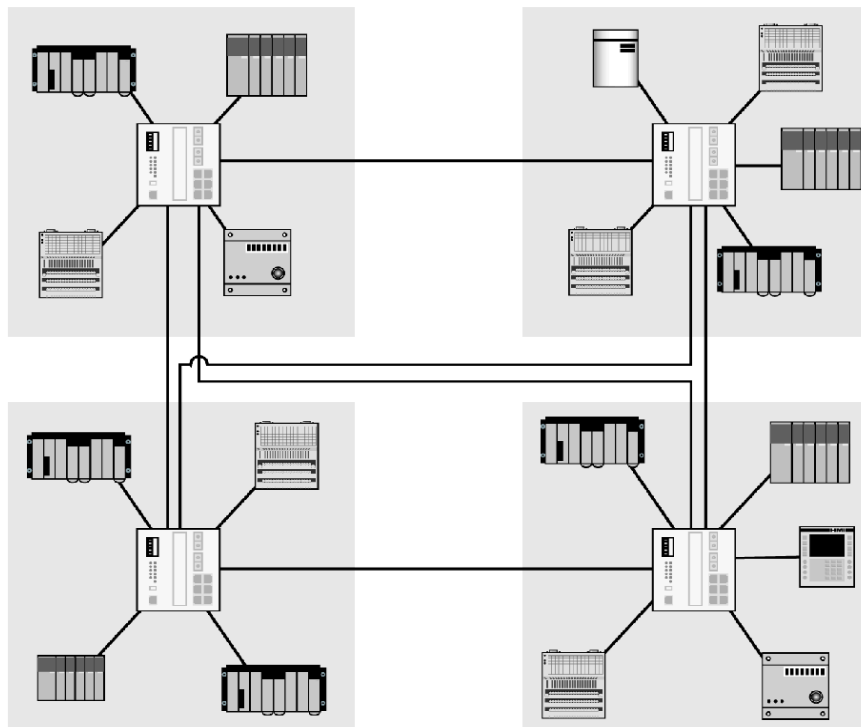
Les protocoles arbre recouvrant (STP - IEEE 802.1D) et arbre recouvrant rapide(RSTP - IEEE 802.1w) sont des protocoles qui permettent d'éviter les boucles de communication et recherchent un nouveau chemin de communication lorsque le chemin initial n'est plus disponible. Le délai de récupération (temps mis à trouver un nouveau chemin) est d'environ 30 s avec le protocole STP. Avec le protocole RSTP et une conception de réseau adéquate, le délai de récupération peut descendre à 100 ms.



Topologie maillée Ethernet

Un réseau maillé Ethernet offre davantage de redondance qu'une architecture Ethernet en anneau. Dans un anneau, deux chemins sont généralement disponibles pour atteindre le même équipement. Dans un réseau maillé, il existe davantage de chemins disponibles.

Pour développer une topologie maillée Ethernet, des commutateurs prenant en charge le protocole arbre recouvrant ou arbre recouvrant rapide doivent être utilisés.



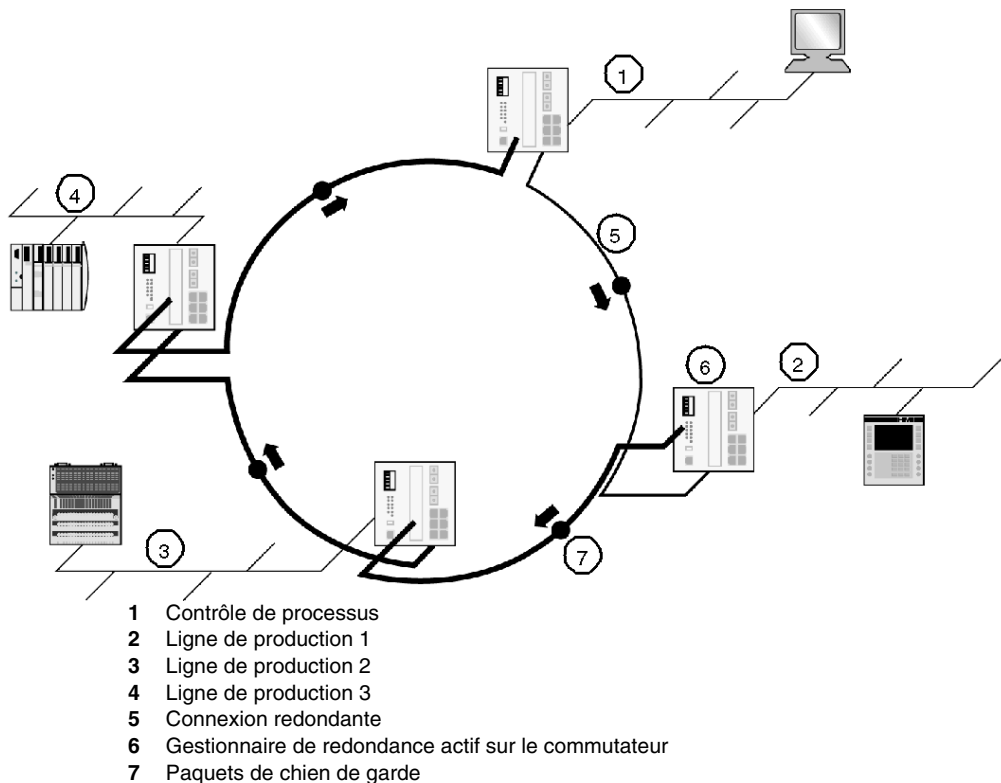
Topologie en anneau redondant

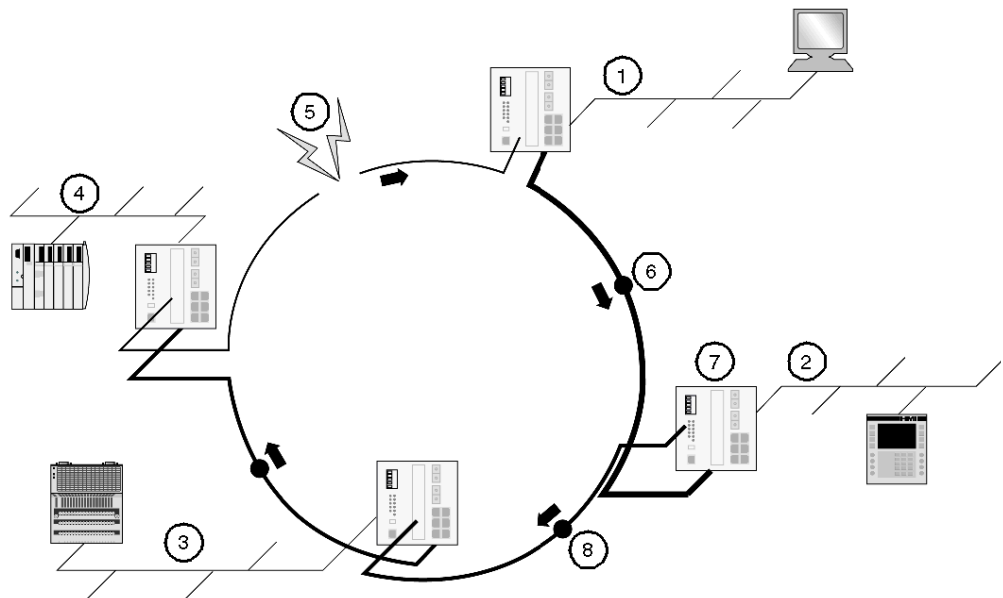
Récapitulatif

Une topologie en anneau redondant est recommandée pour les environnements d'automatisation dans lesquels il est essentiel d'avoir un réseau de tolérance de pannes. A l'inverse d'une topologie en double anneau dans laquelle il existe deux liaisons sur chaque équipement, un anneau redondant utilise la gestion logique sur le commutateur pour rediriger le trafic à travers une structure de liaison unique.

Fonctionnement auto-régénérant

Lorsqu'une liaison échoue sur un anneau redondant, une liaison redondante est activée en une fraction de seconde. Grâce au gestionnaire de redondance, le commutateur surveille l'anneau à l'aide de paquets de chien de garde. Si l'une des liaisons échoue sur l'anneau, la connexion redondante réalise une auto-régénération en activant la liaison redondante afin de prendre le relais de la transmission des paquets de données. Une fois que la liaison rompue a été réparée, la liaison d'auto-régénération est réactivée.





- 1 Contrôle de processus
- 2 Ligne de production 1
- 3 Ligne de production 2
- 4 Ligne de production 3
- 5 Panne de réseau
- 6 La connexion redondante prend le relais de la transmission des paquets de données
- 7 Gestionnaire de redondance actif sur le commutateur
- 8 Paquet de données en mesure d'atteindre tous les nœuds

Avantages	Inconvénients
Moins complexe, nécessitant une seule connexion physique.	Si deux liaisons échouent simultanément, la connectivité à des équipements stratégiques peut être perdue.
Plus rentable, une seule interface et un seul réseau sont utilisés.	
Auto-régénération automatique détectant les pannes et redirigeant les paquets de données.	

Technologies LAN et conception réseau

Récapitulatif

Éviter les perturbations au cours du transfert de données est un enjeu de première importance pour un planificateur de réseau industriel, parfois même une priorité sur le débit (vitesse de transfert des informations). Ci-dessous sont décrits les problèmes liés à la conception réseau tels que la congestion, la gestion des collisions et la diffusion qui peuvent avoir un impact sur le transfert rapide et sans heurts des informations sur le réseau. Des suggestions vous sont données pour une conception réseau appropriée capable de minimiser le risque de perturbations.

Parmi les nombreuses technologies pouvant être utilisées pour construire un réseau IP, Ethernet s'est avérée être la technologie préférée à la fois pour les environnements bureautiques et industriels.

Avantages et normes Ethernet

Ethernet est devenue la technologie LAN la plus répandue parce qu'elle offre des avantages en termes de vitesse, de coût et de facilité d'installation. Capable de prendre en charge la quasi-totalité des protocoles réseau, elle a gagné une large approbation sur le marché informatique en tant que technologie de mise en réseau adaptée à la plupart des environnements réseau.

La norme IEEE définit des règles pour la configuration d'un réseau Ethernet et la spécification du mode d'interaction entre les éléments d'un réseau Ethernet de la norme IEEE 802.3. La conformité à la norme IEEE 802.3 garantit l'efficacité des communications de votre équipement réseau et vos protocoles réseau. Reportez-vous aux informations relatives au modèle OSI (*voir page 135*).

Fast Ethernet et Gigabit Ethernet

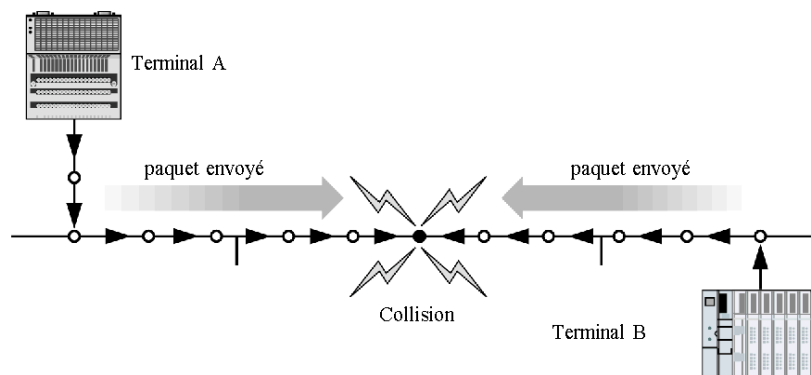
Les réseaux Ethernet nécessitant des vitesses de transmission supérieures peuvent utiliser la norme Fast Ethernet (IEEE 802.3u), qui fait passer la limite de la vitesse Ethernet de 10 à 100 Mbit/s avec seulement quelques modifications minimales à apporter au câblage. La norme Fast Ethernet 100Base-TX est devenue la plus répandue parce qu'elle est très compatible avec la norme Ethernet 10Base-T existante. Gigabit Ethernet (1000 Mbit/s) est une technologie en cours de développement (IEEE 802.3z) qui devrait permettre à la prochaine génération de réseaux de prendre en charge des vitesses de transfert encore plus élevées.

Trames/paquets Ethernet

Le réseau envoie des données dans des unités appelées *trames* (également appelées trames de données ou paquets). Chaque trame peut transporter entre 46 et 1 500 octets de données. Une trame comprend des informations de protocole pour un routage approprié.

Ethernet et collisions

Dans la mesure où Ethernet permet l'échange simultané de données par des équipements multiples, des collisions se produisent parfois lorsque deux équipements transmettent des données en même temps. Dans ce cas, les deux équipements interrompent leur transmission et utilisent un algorithme de recul aléatoire pour attendre un certain temps avant de tenter une nouvelle transmission.



Les collisions peuvent être gérées par une planification et une conception réseau minutieuses. Les facteurs de conception et de fonctionnement suivants peuvent affecter le taux de collision d'un réseau Ethernet :

- le nombre d'équipements sur le réseau ; plus il y a d'équipements, plus le risque de collision est élevé.
- la longueur du réseau ; plus il est long, plus le risque de collision est élevé.
- la longueur du paquet ou la taille MTU ; une longueur de paquet supérieure est plus longue à transmettre, augmentant de ce fait le risque de collision. Plus la taille de trame est importante, plus le risque de collision est élevé.

Réseaux commutés et domaines de collision

Les commutateurs, à condition d'être bien intégrés dans la conception de la structure réseau, constituent la clé pour éviter le ralentissement du réseau suite à une collision ou une congestion. Certains commutateurs intelligents créent moins de trafic réseau en envoyant des données uniquement au destinataire qui en a besoin. Ils peuvent également filtrer les paquets défectueux, interrompant ainsi leur progression. Les commutateurs divisent également un réseau en domaines distincts plus courts qui acheminent respectivement un trafic moins important. Les commutateurs full-duplex (*voir page 66*), qui permettent une transmission de données dans les deux sens, peuvent augmenter la bande passante et supprimer complètement les collisions sur les segments qui les utilisent. Schneider Electric recommande l'utilisation de la commutation full-duplex dans les réseaux d'automatisation.

Congestion du réseau

La performance observable sur un réseau partagé se détériore si des équipements ou des applications nécessitant plus de données viennent s'ajouter à la configuration globale. L'augmentation des collisions peut être due à l'installation d'équipements en surnombre ou d'un trafic trop important sur le réseau. Par exemple, le débit réel sur un réseau Ethernet de 10 Mbit/s de charge modérée est d'environ 35 % de capacité, ce qui représente 2,5 Mbit/s environ (après calcul du traitement des paquets, des intervalles interpaquets et des collisions). Un réseau Fast Ethernet de charge modérée partage 25 Mbit/s de données réelles dans la même situation. Les collisions augmentent sur les deux réseaux au fur et à mesure que des nœuds supplémentaires et/ou un trafic plus important sont ajoutés au domaine de collision partagé. Encore une fois, une bonne planification dans la segmentation du réseau et une utilisation des commutateurs intelligents, contribuent à réduire la congestion et à maintenir des performances convenables.

Domaines de diffusion Ethernet

Une diffusion est la transmission d'un même message à des destinataires multiples sur le réseau. Tout équipement configuré pour la diffusion réseau reçoit le message en question.

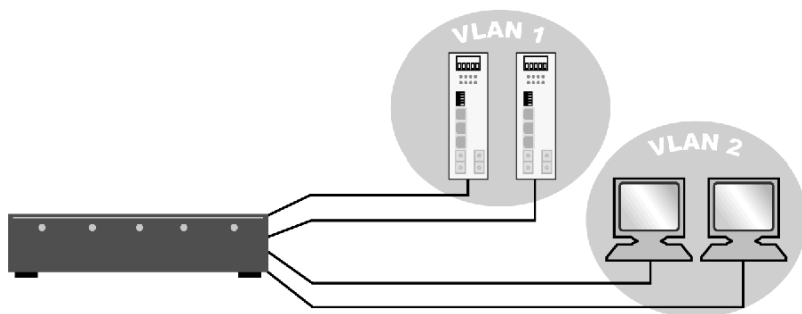
La diffusion peut être très utile. Cependant, si le domaine créé dans la conception réseau est trop volumineux, une diffusion peut créer un volume de trafic si important qu'il entraîne des retards. Certains types de données de diffusion peuvent entraîner plus de retards que d'autres, mais les retards ont un impact sur les performances de chaque équipement sur le réseau. Limitez la taille du domaine de diffusion avec un routeur ou un commutateur intelligent qui contrôle le retard dû à des diffusions excessives.

L'utilisation de composants comme les routeurs pour délimiter les domaines de diffusion peut améliorer les performances globales d'un réseau. Des routeurs installés entre plusieurs réseaux locaux (LAN) forment des limites logiques de domaine de diffusion. Etant donné que les routeurs filtrent le trafic réseau, un routeur peut être configuré pour ne faire suivre que des diffusions spécifiques vers d'autres domaines. L'utilisation d'un routeur pour ce processus est peut-être plus gourmande en temps, mais elle augmente l'efficacité de la transmission.

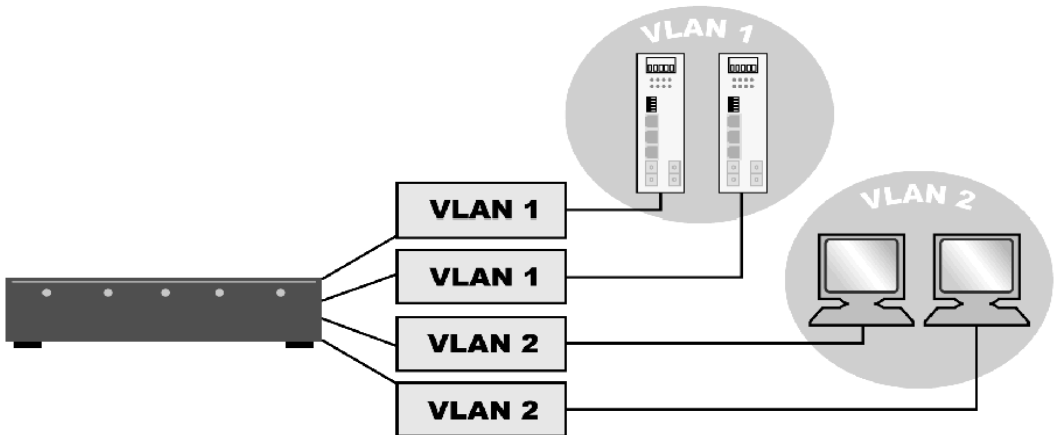
Réseaux VLAN

Un LAN virtuel regroupe des équipements qui peuvent être situés dans différents emplacements physiques dans un réseau virtuel, tout en partageant des ressources, des serveurs et d'autres équipements parmi un groupe de travail. L'utilisation d'un VLAN pour segmenter le trafic peut accroître les performances réseau en réduisant la taille des domaines de collision et des charges de trafic. Elle constitue une manière plus souple et moins chère de modifier des groupes dans un environnement susceptible de changer. Le regroupement ajoute également une homogénéité à l'adressage et aux protocoles, un avantage pour l'administrateur, et requiert moins de ressources du serveur local. Un VLAN apporte également des mesures de sécurité en plus.

Il existe plusieurs façons de regrouper des équipements dans un VLAN. Les VLAN équipés de ports sont des stations terminales regroupées par ports sur un commutateur. S'ils sont branchés sur certains ports terminaux, ils appartiennent au même groupe. Les ports VLAN peuvent être configurés à l'aide de commutateurs intelligents qui prennent en charge les configurations VLAN. Un autre type de configuration VLAN est le protocole VLAN (PVLAN), dans lequel le commutateur examine automatiquement tous les ports et regroupe les stations terminales par protocole. Les stations terminales peuvent également être groupées par adresse réseau IP. Lorsqu'une adresse IP est attribuée à une station terminale, elle est placée dans un VLAN spécifique.



Les stations terminales peuvent également être groupées sur la base de leurs adresses IP. Une fois que l'adresse IP est attribuée à une station terminale, elle est placée dans un VLAN spécifique.



Les VLAN peuvent être implémentés sur des commutateurs de couche 3 (voir page 68) pour créer des domaines de diffusion multiples, comme les routeurs. Le moteur de commutation peut ensuite acheminer d'un VLAN à l'autre, améliorant les performances sur le LAN.

Des VLAN sont soumis à certaines limitations comme le nombre de diffusions et d'adresses Ethernet et des contraintes sur les ports.

IP sans fil

La communication sans fil (IEEE 802.11a/b/g) permet de réaliser des communications mobiles sans le coût des longueurs de câble ou de la maintenance à emplacement fixe. Elle ne remplace pas les réseaux câblés ; elle permet à un seul équipement d'accéder au réseau à partir de divers emplacements. La technologie sans fil pour les environnements industriels doit créer la même fiabilité, performance et redondance qu'aujourd'hui avec les réseaux câblés.

Matériel LAN

Récapitulatif

Un aperçu du matériel utilisé sur un réseau local est utile pour planifier un réseau robuste pour votre application industrielle. La description suivante fournit un bref aperçu et quelques recommandations pour le matériel LAN à utiliser pour construire une application (*voir page 86*) Ethernet industrielle Transparent Ready.

Matériel et couches de fonctionnement

Le tableau suivant montre sur quelle couche tombe chaque élément matériel, conformément au modèle OSI (*voir page 135*) :

Couche	Numéro de couche	Matériel
Application	7	passerelle (si la passerelle convertit également le protocole)
Réseau	3	routeurs/passerelles, commutateurs de couche 3
Liaison de données	2	commutateurs
Physique	1	concentrateurs

Concentrateurs (répéteurs)

Un concentrateur est un équipement actif avec des ports multiples qui relient les équipements entre eux et étendent la longueur du réseau. En général, les concentrateurs sont des équipements de type Plug and Play qui ne nécessitent aucune configuration. Les concentrateurs sont transparents pour les autres équipements et sont principalement des répéteurs qui étendent les segments de réseau. Ils reçoivent des informations par le biais d'un de leurs ports et les transmettent à tous leurs autres ports. Un nombre limité de concentrateurs peut être mis en cascade pour étendre la longueur du réseau.

Des équipements interconnectés par des concentrateurs occupent le même domaine de collision ; ils sont situés dans le même segment de réseau où des paquets d'informations peuvent entrer en collision. De ce fait, les concentrateurs diminuent l'efficacité du réseau.

Commutateurs

Les commutateurs sont des équipements actifs utilisés pour relier des équipements entre eux et étendre la longueur du réseau. Contrairement aux concentrateurs, les commutateurs reçoivent des informations par le biais d'un de leurs ports et les transmettent uniquement au port sur lequel l'équipement cible des informations entrantes est connecté. Un nombre illimité de commutateurs peut être mis en cascade pour étendre la longueur du réseau.

Les commutateurs sont transparents pour les équipements du réseau. Ils offrent de nombreuses fonctions pour gérer le trafic et fournir une sécurité (*voir page 151*).

Les commutateurs scindent les domaines de collision pour que les équipements interconnectés par des commutateurs occupent des domaines de collision différents.

Types de commutateurs

Il existe deux types de commutation : *en mode direct* et *stockage et retransmission*.

- Le commutateur en mode direct commence à transférer un paquet dès sa réception, ce qui peut entraîner une perturbation du réseau si le paquet est défectueux.
- La commutation de type "stockage et retransmission" attend que tout le paquet arrive et vérifie si celui-ci n'est pas corrompu avant de le transférer vers le port approprié. Ceci évite d'envoyer des paquets corrompus sur tout le réseau. Un commutateur de stockage et retransmission arrête également un paquet corrompu au premier commutateur qu'il atteint. Le retard du processus est minimal, inférieur à 1 ms sur un réseau industriel.

Les commutateurs de type "stockage et retransmission" sont recommandés par Schneider Electric pour les réseaux d'automatisation.

Emetteurs-récepteurs

Les émetteurs-récepteurs modifient le support physique : dans la plupart des cas, ce changement survient entre le cuivre et la fibre optique.

Ponts

Un pont a été utilisé pour connecter deux segments LAN avec des protocoles différents (Ethernet, Token Ring) ou pour connecter deux LAN, en utilisant des adresses Ethernet. Cependant, étant donné que les ponts offrent une performance de débit inférieure, une densité de port inférieure, un coût de transport supérieur et une flexibilité inférieure, l'utilisation des commutateurs est à préférer à celle des ponts.

Routeurs (passerelles)

Un routeur Ethernet est également appelé passerelle ou passerelle par défaut. Les routeurs connectent deux réseaux distincts. Ils créent ou gèrent une table des réseaux disponibles et utilisent ces informations pour déterminer le meilleur itinéraire pour un paquet de données spécifique depuis le réseau source vers le réseau cible.

Les routeurs peuvent être utilisés pour scinder des domaines de diffusion.

Commutateurs de routage de couche 3

Un commutateur de couche 3 est un routeur implémenté dans un matériel. Il fonctionne comme un routeur mais à une vitesse plus élevée.

Autres considérations LAN

Résumé

Vous trouverez ci-dessus des considérations supplémentaires sur la planification d'un réseau industriel robuste.

Comparaison entre les modes Full-Duplex et Half-Duplex

Schneider Electric recommande l'utilisation des commutateurs Full-Duplex, dans la mesure du possible. Les commutateurs Full-Duplex :

- offrent une meilleure bande passante (100 Mo dans les deux directions sur certains réseaux) ;
- permettent à un équipement d'envoyer des réponses tout en recevant d'autres requêtes ou trafic ;
- génèrent moins de retards et d'erreurs avec un équipement.

Quand utiliser un commutateur

Utilisez toujours des commutateurs dans la conception de votre réseau. Ils offrent davantage de fonctions intelligentes que les concentrateurs, à coût égal, voire moindre.

Les commutateurs industriels développés à l'heure actuelle sont parfaitement capables de fonctionner dans des conditions extrêmes, notamment en présence d'interférences électromagnétiques, de températures de fonctionnement élevées et avec des charges mécaniques importantes. Protégez vos commutateurs industriels à l'aide de connecteurs amovibles jusqu'à IP67 (*voir page 83*) et de câblage en anneau redondant.

Bande passante

10 Mo de bande passante peuvent être utilisés pour les équipements terminaux plus petits, mais pas pour les liaisons vers automate/SCADA ou vers les principales liaisons de réseau.

100 Mo sont suffisants pour la plupart des systèmes d'automatisation.

1 Go est suffisant pour la principale liaison de réseau. Une telle capacité n'est pas obligatoire mais permet de disposer d'une bande passante supplémentaire en cas de besoin. Elle devient toutefois nécessaire si d'autres services partagent le réseau avec le système d'automatisation.

Technologies WAN et conception réseau

Récapitulatif

Plusieurs LAN qui résident dans des emplacements physiques très éloignés peuvent être joints dans un réseau étendu WAN. Le WAN utilise généralement des services loués pour la connexion. Ces services comprennent :

- lignes louées point à point
- commutation de circuits
- commutation de paquets
- circuits virtuels
- accès commuté

Les technologies WAN fonctionnent au niveau des trois couches inférieures du modèle OSI (*voir page 135*) : la couche physique, la couche liaison de données et la couche réseau.

Lorsque vous planifiez une application Ethernet industrielle Transparent Ready, prenez en compte certains facteurs concernant votre WAN comme la taille et les emplacements du réseau proposé, le volume du trafic et le coût et la vitesse des différents services de transmission commerciaux.

Liaisons point à point (lignes louées)

Les liaisons point à point fournissent un chemin de communication WAN préétabli unique depuis votre site vers votre réseau distant, par le biais du réseau d'un fournisseur de services. Le fournisseur de services dédie le câblage et la bande passante pour répondre aux besoins de votre entreprise. Le coût dépend de la quantité de bande passante requise et de la distance entre les points de connexion.

Commutation de circuits

Un routeur peut initier des connexions à commutation de circuits le cas échéant, puis déconnecter le circuit une fois la communication terminée. Le coût dépend de l'heure à laquelle le circuit est utilisé, ce qui fait de la commutation de circuit une solution de sauvegarde répandue pour d'autres technologies WAN.

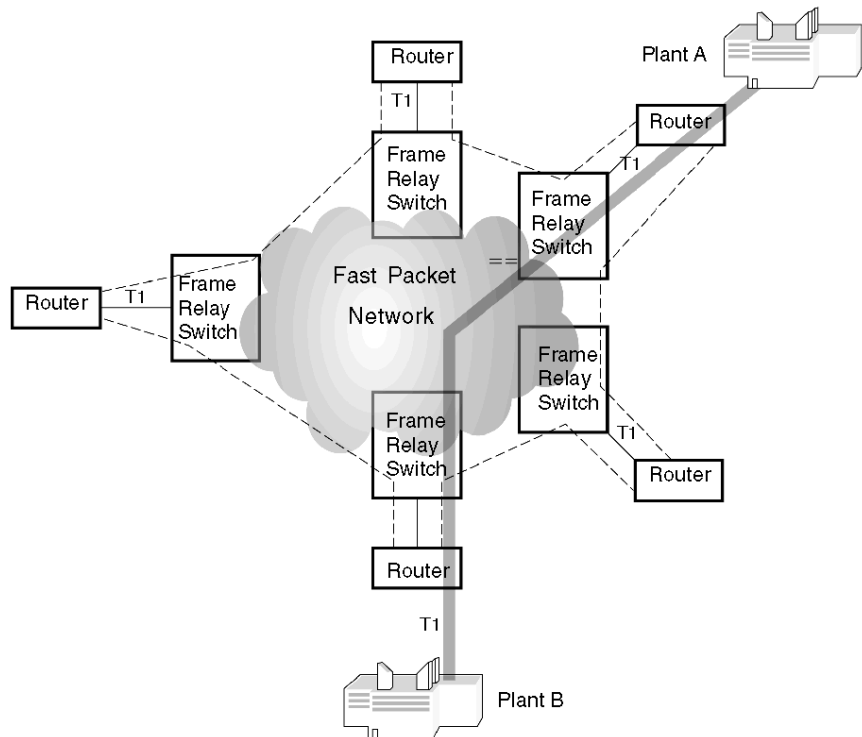
RNIS est un exemple de technologie rentable. Utilisés en tant que sauvegarde, les routeurs peuvent être configurés pour réacheminer le trafic automatiquement en cas d'échec des autres lignes WAN. RNIS prend en charge des vitesses de transfert de données de 64 Kbit/s. Il existe deux types de RNIS :

- BRI, un service de base, comprend deux voies de 64 Ko et une voie D pour transmettre les informations de contrôle.
- PRI, pour les utilisateurs nécessitant une plus grande capacité, comprend 23 voies B et une voie D (USA) ou 30 voies B et une voie D (Europe).

Commutation de paquets

La commutation de paquets implique le partage des ressources auprès d'un fournisseur de services. Le fournisseur de services alloue des portions d'une ligne ou de circuits virtuels que votre entreprise utilisera. La commutation de paquets scinde les paquets et les étiquette individuellement, les envoie de manière séquentielle sur le réseau en empruntant l'itinéraire le plus approprié, puis les rassemble au point de destination. Ceci est plus efficace et plus rentable pour le transporteur, tout en diminuant le coût pour l'utilisateur par rapport à des services dédiés. Les exemples les plus courants de technologies WAN à commutation de paquets sont relais de trame, ATM et MPLS.

Le relais de trame (qui repose sur une technologie à commutation de paquets) prend en charge des vitesses de transfert de données de T-1 (1,544 Mbit/s) et T-3 (45 Mbit/s). Le relais de trame peut constituer une solution économique pour les applications industrielles.



Circuits virtuels

Les circuits virtuels sont des circuits logiques créés au sein d'un réseau partagé. On en distingue deux types :

- les circuits virtuels commutés (SVC), qui sont dynamiquement établis sur demande et interrompus une fois la transmission terminée
- les circuits virtuels permanents (PVC), une option plus onéreuse pour des situations dans lesquelles le transfert de données entre équipements est constant

Services d'accès commuté

Les services d'accès commuté d'un WAN peuvent constituer une solution économique lorsque votre entreprise ne génère pas un trafic de transmission volumineux. L'accès commuté est aussi fréquemment utilisé comme sauvegarde pour d'autres technologies WAN. Les gestionnaires réseau peuvent procéder à un dépannage à distance sur un modem connecté à un routeur sur une ligne d'accès commuté bon marché si la ligne principale est en panne.

Matériel WAN

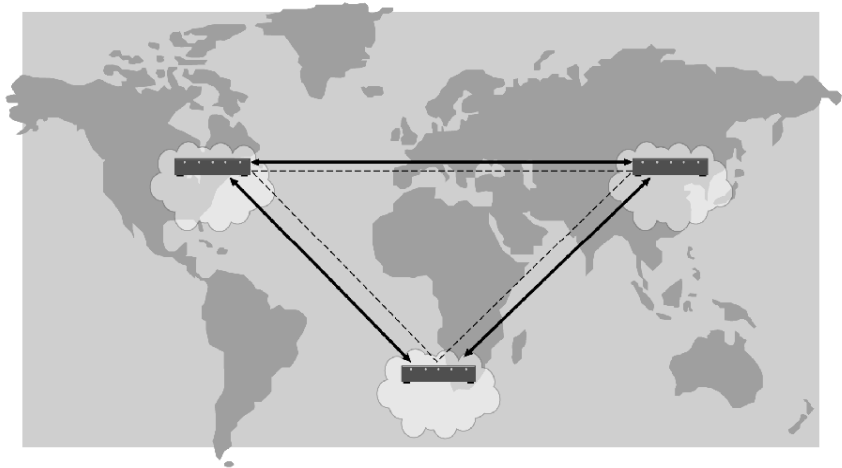
Récapitulatif

Pour connecter votre réseau à d'autres réseaux, certains équipements sont requis :

- routeurs
- commutateurs WAN
- serveurs d'accès
- modems
- CSU/DSU
- adaptateurs de terminaux RNIS

Routeurs

Un routeur est un commutateur logique qui relie votre réseau au WAN et permet de connecter le WAN à votre autre emplacement de réseau. Il y a un routeur à chaque extrémité du WAN. Certains routeurs intègrent parfois la connexion physique, mais l'équipement de connexion physique peut aussi être externe.



Commutateurs WAN

Les commutateurs ont des fonctionnalités de couche 3, qui combinent les avantages de la commutation et du routage dans un équipement unique.

Serveurs d'accès

Les serveurs d'accès permettent aux utilisateurs d'avoir des connexions entrantes et sortantes. *Serveur à accès distant, page 159*

Modems

Les modems convertissent les signaux analogiques et numériques et prennent en charge des connexions au réseau sur des lignes téléphoniques de type vocales. Ils peuvent être intégrés à d'autres composants du réseau ou achetés séparément.

Trois options d'équipement peuvent être utilisées pour se brancher à un routeur :

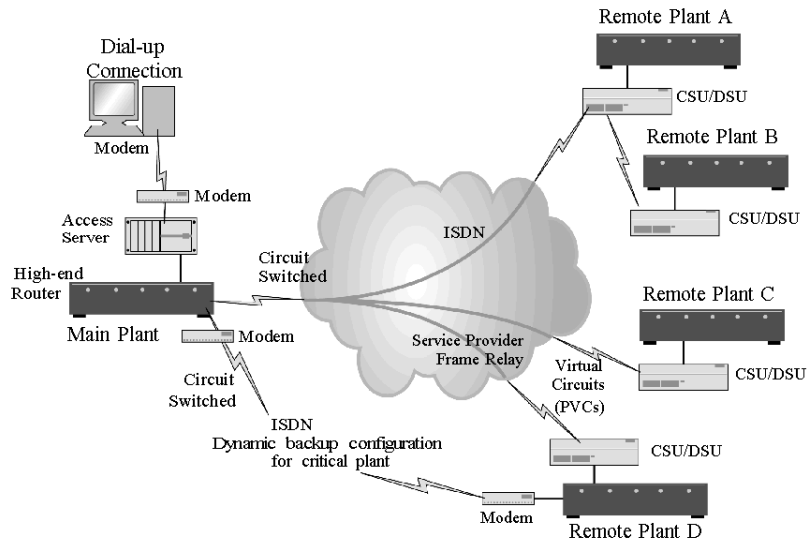
- modems
- CSU/DSU
- adaptateurs de terminaux RNIS

Le matériel CSU/DSU se branche sur un routeur pour fournir une connexion à un réseau numérique comme une ligne T1. Ce matériel peut se connecter en tant que composant externe ou être intégré à des composants réseau plus avancés. Les fournisseurs de services proposent souvent des CSU/DSU ; si ce n'est pas le cas, ils peuvent vous aider à configurer votre CSU/DSU pour l'adapter à la configuration de leur ligne.

Un adaptateur de terminal RNIS est un modem utilisé pour relier des connexions Basic Rate Interface (BRI) RNIS à un routeur. Ces adaptateurs peuvent être des équipements distincts ou intégrés à un routeur.

Topologie WAN

Le schéma ci-dessous illustre un WAN comprenant un site principal connecté à plusieurs sites distants.



L'usine principale est connectée aux usines distantes C et D par une connexion à relais de trame à commutation de paquets utilisant des circuits virtuels (PVC dans ce cas). L'usine principale est connectée à l'usine distante A par des lignes RNIS. Un site critique (usine distante D) est également connecté à une connexion RNIS à commutation de circuits agissant comme sauvegarde de la liaison de relais de trame. Cette connexion RNIS est configurée dynamiquement sur le routeur haut de gamme pour se réaliser uniquement en cas d'échec de la connexion du relais de trame. Un serveur d'accès commuté est également illustré (en haut à gauche) ; il prend en charge le dépannage lié à la gestion du réseau depuis des emplacements distants en cas de perte totale de la connectivité WAN avec le site principal. Les autres matériels WAN comprennent les routeurs, les modems, les CSU/DSU (aux usines distantes A, B, C et D) et un adaptateur de terminal RNIS (à l'usine distante D).

2.3 Exigences liées à l'environnement

Vue d'ensemble

Un réseau Ethernet industriel Transparent Ready permet de connecter des automates industriels en se basant sur la connectivité Ethernet (automates, stations E/S, capteurs, actionnaires, etc.) et les équipements industriels de l'infrastructure Ethernet (câbles, connecteurs, commutateurs, concentrateurs, etc.).

Schneider Electric propose trois catégories environnementales :

- bureau
- industrie légère
- industrie lourde

Ce sous-chapitre décrit les exigences environnementales pour un réseau Ethernet industriel.

Le terme *industriel* fait référence à des conditions environnementales extrêmes (protection mécanique, climatique et contre le captage) auxquelles les appareils sont exposés, ainsi qu'aux variables de l'immunité au bruit.

Un réseau Ethernet industriel doit présenter des performances prévisibles ainsi qu'un niveau de convivialité assez élevé, afin de compenser ces conditions extrêmes.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Résumé des normes environnementales	77
Exigences liées à la mécanique	78
Exigences liées à la protection climatique	80
Exigence de protection contre la pénétration de corps étrangers	82
Emission électromagnétique et exigences d'immunité	85

Résumé des normes environnementales

Normes pour les variables environnementales

La plage de valeurs pour les variables environnementales d'un système (par exemple, la température comme variable climatique) est définie dans des normes de l'industrie établies par divers organismes : UL, CE, CEI, CSA CENELEC, etc. (*voir page 78*)

Même si de nombreuses normes sont de portée internationale et globalement acceptées, les principaux organismes de normalisation poursuivent leurs efforts afin de rapprocher les normes existantes et d'en créer de nouvelles qui s'accordent les unes avec les autres. Les normes varient souvent d'une région à une autre, d'une application à une autre et d'un équipement à un autre. Schneider Electric recommande que vous preniez en compte ces divergences lors de la conception de votre réseau Transparent Ready.

Normes industrielles et de télécommunication

Pour ce qui est des normes pour l'Ethernet industriel, deux aspects supplémentaires doivent être mentionnés.

- Les groupes responsables des télécommunications et des technologies de l'information, tels que le TIA, définissent des normes pour l'Ethernet industriel en plus des organisations de normalisation industrielles traditionnelles.
- Contrairement aux normes spécifiques aux automates industriels, les normes pour les équipements de l'infrastructure Ethernet industriel (concentrateurs, commutateurs, routeurs, etc.), les câbles et les connecteurs ne sont pas encore clairement définies. Un grand nombre d'équipementiers pour l'infrastructure Ethernet ont adopté les normes utilisées pour les automates industriels (automates, stations d'E/S, etc.) et les considèrent comme adaptées aux équipements Ethernet.

Conformité aux normes

Ce sous-chapitre tente de fédérer les recommandations pour la sécurité environnementale établie par les normes émergentes pour l'Ethernet industriel, ainsi que les normes pour les télécommunications et les technologies de l'information. En plus de ces recommandations, il est important de noter les points suivants :

- Lors de la conception d'une installation Ethernet industriel, vous devez vous conformer aux réglementations établies par vos organisations de normalisation régionales, à la fois pour les types d'équipements que vous avez l'intention d'utiliser et les applications que vous ciblez. Ces normes fournissent généralement des règles bien définies et des instructions pour des automates industriels.
- En ce qui concerne les câbles et les connecteurs, des normes émergentes sont en cours de définition. Les organisations Ethernet industriel, telles que Modbus, IDA et IAONA, fournissent des recommandations pour les câbles et les connecteurs. Les travaux en cours sur la normalisation des câbles et des connecteurs sont mentionnés dans d'autres rubriques de ce sous-chapitre.

Exigences liées à la mécanique

Introduction

Les exigences liées à la mécanique s'appliquent à tout composant électronique, électrique, mécanique ou tout assemblage de composants. Les tests et les indices pour la conformité mécanique aux normes incluent les éléments suivants :

- chocs
- vibrations
- résistance à la traction
- flexion
- écrasement
- impact

Exigences liées au choc

Le tableau ci-dessous décrit les limites admissibles recommandées en termes de chocs pour l'environnement Ethernet industriel.

Environnement	Limites en termes de chocs	Référence
Environnement industriel léger (faible charge d'activité)	15 g/11 ms (dans les trois plans)	CEI 60068-2-27 (Essais d'environnement. Partie 2 : Essais. Essai Ea et guide : Chocs EN 60068-2-27
Environnement industriel lourd (forte charge d'activité)	20 g/11 ms (dans les trois plans)	CEI 60068-2-27 27 (Essais d'environnement. Partie 2 : Essais. Essai Ea et guide : Chocs EN 60068-2-27

Exigences liées aux vibrations

Les vibrations sont définies en tant qu'oscillations mécaniques produites par les mouvements d'un membre ou d'un corps à partir de sa position de repos pendant des périodes régulières ou irrégulières. Les vibrations peuvent entraîner des dommages matériels, des pertes de contrôle de l'équipement et une efficacité réduite dans le fonctionnement de la machine.

Le tableau ci-dessous décrit les limites admissibles recommandées en termes de vibrations pour l'environnement Ethernet industriel.

Environnement	Limites en termes de vibrations	Référence
Environnement industriel léger (faible charge d'activité)	2 g à 10 - 500 Hz	CEI 60068-2-6 (Essais d'environnement. Partie 2 : Essais. Essai Fc : Vibrations (sinusoïdales) EN 60068-2-6
Environnement industriel lourd (forte charge d'activité)	5 g à 10 - 500 Hz	CEI 60068-2-6 (Essais d'environnement. Partie 2 : Essais. Essai Fc : Vibrations (sinusoïdales) EN 60068-2-6

Exigences liées à la résistance à la traction

Le tableau ci-dessous décrit les limites admissibles recommandées en termes de résistance à la traction pour les câbles Ethernet industriels.

Environnement	Exigences liées à la de résistance à la traction	Référence
Environnement industriel léger (faible charge d'activité)	75/100/200 N pendant 1 min	CEI 60966-1
Environnement industriel lourd (forte charge d'activité)	100/200 N pendant 1 min	IEC 60966-1

Exigences liées à la flexion

Le tableau ci-dessous décrit les limites admissibles recommandées en termes de flexion pour les câbles Ethernet industriels.

Environnement	Exigences liées à la flexion
Environnement industriel léger (faible charge d'activité)	5 N 1 000 opérations +/-90 degrés
Environnement industriel lourd (forte charge d'activité)	5 N 1 000 opérations +/-90 degrés

Exigences liées à l'écrasement

Le tableau ci-dessous décrit les limites admissibles recommandées en termes d'écrasement pour les câbles Ethernet industriels.

Environnement	Exigences liées à l'écrasement
Environnement industriel léger (faible charge d'activité)	Projet de norme ISO/CEI en cours de rédaction et non encore publié.
Environnement industriel lourd (forte charge d'activité)	

Exigences liées à la protection climatique

Introduction

Les exigences climatiques pour un réseau Ethernet industriel sont les suivantes :

- température ambiante en fonctionnement
- température de stockage
- humidité
- exposition aux UV

Exigences liées à la température

La température peut affecter les automates industriels et les composants de l'infrastructure du réseau Ethernet, tels que les câbles, les connecteurs et les accessoires, de différentes manières.

Des valeurs extrêmes de température peuvent avoir un effet sur la performance. Par exemple, un froid extrême peut rendre les câbles rigides, cassants et difficiles à manipuler, alors que les températures élevées peuvent ramollir, voire même faire fondre le plastique utilisé dans les câbles. L'affaiblissement dans le câble CAT 5E standard augmente à un taux de 0,4% par degré Celsius, au-dessus de 20 degrés Celsius.

La température ambiante est la température de l'environnement autour de l'équipement. Mesurez la température ambiante pour un équipement à une distance située entre 30 et 40 cm de la surface externe de l'équipement, afin de tenir compte de la circulation d'air à proximité immédiate.

Les deux tableaux ci-dessous décrivent les plages de température ambiante lors du fonctionnement ou du stockage. Si la température ambiante lors du fonctionnement de l'équipement se situe dans la plage donnée, l'équipement est utilisé selon ses caractéristiques de température.

Tableau des températures en fonctionnement

Environnement	Plage de fonctionnement	Référence
Industrie légère	0 à 60 degrés C	CEI 60654-1
Industrie lourde	-20 à +85 degrés C	CEI 60654-1

Tableau des températures de stockage

Environnement	Plage de fonctionnement
Industrie légère	-25 à +70 degrés C
Industrie lourde	-25 à +70 degrés C

Autres facteurs environnementaux

L'humidité et l'exposition aux UV peuvent également affecter la performance des câbles.

Les tableaux ci-dessous décrivent la plage d'humidité admissible (en pourcentage) lors du fonctionnement de l'appareil ainsi que le nombre d'heures admissibles d'exposition aux UV.

Tableau relatif à l'humidité

Environnement	Humidité
Industrie légère	5 à 95 % sans condensation
Industrie lourde	0,1 à 95 % sans condensation

Tableau relatif à l'exposition aux UV

Environnement	Exposition aux UV
Industrie légère	3 000 h
Industrie lourde	6 000 h

Exigence de protection contre la pénétration de corps étrangers

Introduction

Des corps solides étrangers, tels que la poussière, l'eau, l'humidité et autres polluants, peuvent pénétrer dans une enveloppe d'équipements industriels. La protection contre la pénétration de corps étrangers renvoie à la capacité de l'enveloppe à ne pas laisser pénétrer ces corps. Elle implique également que toute personne doit rester à distance des pièces tournantes situées à l'intérieur de l'enveloppe.

Deux types de régulations définissent les variables de protection contre la pénétration des corps étrangers :

- degré de pollution
- degré de protection

Degré de pollution

La présence de pollution, telle que l'humidité ou la poussière, sur la surface des équipements peut réduire leur capacité d'isolement. La norme CEI 1010 définit les différents types d'environnements de pollution. Les environnements fortement pollués doivent bénéficier d'un isolement renforcé. Il est également possible de créer des micro-environnements propres pour les circuits et les équipements sensibles utilisant des boîtiers, des méthodes d'enrobage et des joints hermétiques.

Quatre niveaux de pollution ont été définis par la norme CEI 60664-1 (*Coordination de l'isolement des matériels dans les systèmes (réseaux) à basse tension - Partie 1 : Principes, prescriptions et essais*) :

Niveau de pollution	Description
Niveau 1	Absence de pollution ou uniquement pollution sèche, non conductrice. Ce type de pollution n'a aucune influence électromagnétique ou autre.
Niveau 2	Normalement, uniquement la pollution non conductrice. Une conductivité occasionnelle due à la condensation peut toutefois survenir.
Niveau 3	Pollution conductrice ou pollution sèche non conductrice devenant conductrice à cause de la condensation. La pollution de niveau 3 survient dans les environnements industriels et de chantier considérés comme difficiles.
Niveau 4	Pollution générant une conductivité persistante due à de la poussière, de la pluie ou de la neige conductrice.

Tableau de pollution pour Ethernet industriel

Le tableau ci-dessous répertorie les niveaux de pollution recommandés autorisés pour les automates industriels et les composants d'infrastructure Ethernet :

Environnement	Niveau de pollution autorisé	Référence
Industrie légère (faible charge d'activité)	Niveau 2	CEI 1010
		CEI 60664-1
Industrie lourde (forte charge d'activité)	Niveau 3	CEI 1010
		CEI 60664-1

Degré de protection : code IP

Le degré de protection est défini par la norme CEI 60529. Cette norme décrit un système de classification international composé des lettres *IP* (*Ingress Protection* en anglais), suivies de deux ou trois chiffres. Ce code IP détermine l'efficacité du joint des enveloppes de matériels électriques à les protéger contre l'intrusion de corps solides étrangers, tels que la poussière, les outils, les doigts, etc.

Le premier chiffre (le plus à gauche) du code IP indique le degré auquel les personnes sont protégées de tout contact avec les pièces tournantes (à l'exclusion des arbres à rotation lente) ainsi que le degré auquel les équipements sont protégés contre toute pénétration de corps solides étrangers.

Premier chiffre	Degré de protection : objets solides
0	Aucune protection spéciale.
1	Protection contre l'introduction de parties du corps, comme une main, et d'objets solides supérieurs à 50 mm de diamètre. Ne prévoit aucune protection contre les accès délibérés.
2	Protection contre l'introduction de doigts ou d'autres objets inférieurs à 80 mm de longueur et 12 mm de diamètre.
3	Protection contre l'introduction d'outils, de fils et d'autres objets solides ayant un diamètre ou une épaisseur supérieurs à 1,0 mm.
4	Protection contre l'introduction d'objets solides ayant un diamètre ou une épaisseur supérieurs à 1,0 mm.
5	Protection contre l'introduction de poussière en quantité importante présentant un risque d'interférence avec le fonctionnement de l'équipement.
6	Enveloppe étanche aux poussières.

Le second chiffre du code IP indique le degré de protection de l'équipement contre la pénétration nuisible d'eau et d'humidité sous diverses formes.

Second chiffre	Degré de protection : Humidité
0	Aucune protection spéciale.
1	Protection contre le suintement d'eau.
2	Protection contre le suintement vertical d'eau.
3	Protection contre les vaporisations d'eau.
4	Protection contre les éclaboussures d'eau.
5	Protection contre les projections d'eau par les buses.
6	Protection contre les fortes arrivées d'eau ou les jets d'eau puissants.
7	Protection contre l'immersion.
8	Protection contre les immersions totales prolongées dans l'eau. L'utilisateur final doit spécifier la profondeur et la durée d'immersion. L'exigence doit être supérieure à IP67.

Un troisième chiffre est parfois utilisé s'il existe une seule classe de protection, et un X est alors inséré pour l'un des chiffres. Par exemple, IPX1 indique que l'équipement est protégé contre le suintement d'eau uniquement.

Degrés de protection recommandés pour Ethernet industriel

Environnement	Degré de protection recommandé	Référence
Industriel léger (faible charge d'activité)	IP20	CEI 60529 - Degrés de protection procurés par les enveloppes (Code IP)
		EN 60529
Industriel lourd	IP67	CEI 60529 - Degrés de protection procurés par les enveloppes (Code IP)
		EN 60529

Emission électromagnétique et exigences d'immunité

Introduction

Il existe deux types d'exigence CEM :

- l'émission : quantité de CEM qu'un produit ou un câble peut émettre, et
- l'immunité : degré de tolérance CEM d'un produit ou d'un câble.

Les normes applicables dépendent de l'environnement pour lequel vous concevez votre système Transparent Ready.

Les deux principales organisations de normalisation en termes de CEM sont la CEI et le CENELEC. Deux normes internationales font référence en matière de réglementation de l'émission électromagnétique et de l'immunité :

- CEI 61000-6-2: 1999 *Compatibilité électromagnétique (CEM) - Partie 6-2 : Normes génériques – Immunité pour les environnements industriels*
- CEI 61000-6-4: 1997 *Compatibilité électromagnétique (CEM) - Partie 6 : Normes génériques - Section 4 : Norme sur l'émission pour les environnements industriels*

Norme CEI 1000-4

La norme CEI 1000-4 établit une référence commune pour l'évaluation de la performance des instruments de mesure et de contrôle des procédés industriels, lorsque ceux-ci sont exposés à des perturbations électriques ou électromagnétiques. Elle décrit les essais de sensibilité aux perturbations destinés à démontrer l'aptitude de l'équipement à fonctionner correctement dans des environnements de travail.

Avant de déterminer le type d'essai à effectuer, évaluez tout d'abord les types de perturbations auxquelles l'équipement est soumis à son emplacement d'installation. Les facteurs suivants doivent également être pris en compte :

- méthode avec laquelle le circuit électrique et les blindages sont reliés à la prise de terre ;
- qualité du blindage ;
- environnement.

Les sections CEI 1000-4-2 à 1000-4-5 (*voir page 531*) de la norme sont abordées plus en détail dans ce manuel.

2.4 Choix des composants Ethernet industriel

Vue d'ensemble

Ce chapitre fournit des informations sur le choix des composants Ethernet industriel appropriés. Il décrit les connecteurs recommandés pour les utilisations de bureau et industrie légère ainsi que pour les utilisations en industrie lourde. Les câbles en cuivre pour réseau Ethernet industriel et l'outillage propre à la fabrication de ces câbles sont également traités.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Câbles cuivre Ethernet	87
Câbles à fibre optique	91
Spécifications de la couche physique 10/100BaseF	95
Connecteurs Ethernet pour les réseaux en cuivre	96
Connecteurs pour fibre optique	99
Equipements d'infrastructure recommandés pour Ethernet industriel	101

Câbles cuivre Ethernet

Introduction

Les câbles Ethernet servent à acheminer les signaux émis entre les équipements. Avant de fabriquer un câble, il est donc impératif de savoir quels types d'équipements seront connectés. La plupart des réseaux Ethernet utilisent des routeurs, des commutateurs et des concentrateurs pour gérer les flux d'informations. Ces équipements requièrent des types de câble différents de ceux qui connectent deux terminaux communiquant directement entre eux.

Le réseau Ethernet industriel Transparent Ready doit utiliser des câbles à paire torsadée blindée CAT 5E ou supérieure.

Câbles à paire torsadée

Le câblage à paire torsadée est une forme de câblage courante, dans laquelle deux conducteurs sont enroulés l'un autour de l'autre pour supprimer les perturbations électromagnétiques (diaphonie). Le nombre de torsades au mètre est une caractéristique importante : un nombre élevé de torsades diminue la diaphonie. La torsion des paires, la qualité du matériau conducteur, le type d'isolant et le blindage sont d'autres facteurs déterminants de la vitesse de transmission des données.

Classification et catégories de câbles

Les câbles LAN, communément appelés câbles UTP (à paire torsadée non blindée), sont identifiés par un numéro de catégorie. La norme ANSI/EIA 568, développée par l'American National Standards Institute et l'Electronic Industries Association, est l'une des nombreuses normes qui définit les différentes catégories de systèmes de câblage à paire torsadée (fils, jonctions et connecteurs), en termes de débit de données pouvant être supporté sans problème. Elle spécifie le matériau du câble et les types de connecteurs et blocs de jonction requis pour satisfaire aux exigences de chaque catégorie.

Catégorie	Débit de données maximal	Application courante
CAT 1	Jusqu'à 1 Mbit/s (1 MHz)	Câble téléphonique à paire torsadée non blindée classique pour voix. Non recommandé pour une utilisation en réseau.
CAT 2	4 Mbit/s	Câble à paire torsadée non blindée certifié pour les transmissions de données jusqu'à 4 Mbit/s. Ce câble possède quatre paires torsadées. Il ne doit pas être utilisé pour les applications réseau haute vitesse.
CAT 3	16 Mbit/s	Convient pour des signaux jusqu'à 16 MHz et gère les réseaux Ethernet 10 Mbit/s, anneau à jeton 4 Mbit/s et 100 VG-AnyLAN. Ce câble est enroulé pour une meilleure immunité au bruit. Il est installé sur de nombreux sites comme câble téléphonique.

Catégorie	Débit de données maximal	Application courante
CAT 4	20 Mbit/s	Convient pour des signaux jusqu'à 20 MHz et certifié pour gérer les anneaux à jeton 16 Mbit/s. Ce câble possède quatre paires.
CAT 5	100 Mbit/s 1 000 Mb/s (4 paires)	Convient pour des signaux jusqu'à 100 MHz à une distance maximale de 100 m. Les réseaux Ethernet 100Base-TX, FDDI et ATM à 155 Mbit/s utilisent ce câblage. Il présente une faible capacité et une faible diaphonie, dues à son nombre élevé de torsades au mètre. Câble prédominant dans les nouveaux bâtiments depuis le début des années 1990. N'est plus en usage aujourd'hui : remplacé par 5E.
CAT 5E	Jusqu'à 350 Mbit/s	Le câble CAT 5 amélioré présente toutes les caractéristiques du CAT 5, mais avec une fabrication de qualité supérieure pour minimiser la diaphonie. Il possède davantage de torsades et convient à des fréquences allant jusqu'à 200 MHz, soit le double des capacités de transmission du CAT5. Cependant, à ces fréquences, la diaphonie peut devenir problématique et, le câble n'étant pas blindé, il ne peut pas réduire la diaphonie. Ce câble est défini dans la norme TIA/EIA-568A-5 (Amendement 5).
CAT 6	Jusqu'à 400 MHz	Conçu pour supporter des fréquences de plus de 200 MHz, grâce à des composants dédiés permettant de réduire la distorsion du temps de propagation et autres problèmes. Les organisations TIA et ISO ont travaillé ensemble sur cette catégorie.
CAT 7	600/700 MHz	Conçu pour supporter des fréquences jusqu'à 600 MHz. Outre les paires qui sont chacune blindées, le câble est également recouvert d'une gaine blindée. Les connecteurs devraient faire l'objet d'une conception propriétaire dédiée. Les organisations TIA et ISO ont travaillé ensemble sur cette catégorie.

Les deux catégories les plus largement installées sont les catégories CAT 3 (réseaux 10Base-T) et CAT 5 (réseaux 100Base-T). Même s'ils paraissent identiques, le câble CAT 3 a, lui, été testé sur une série de spécifications plus basses et est susceptible de générer des erreurs de transmission s'il est poussé à des vitesses plus rapides. Les câbles CAT 3 sont certifiés paradiaphoniques uniquement pour les signaux de 16 MHz, alors que les câbles CAT 5 doivent satisfaire à une exigence de 100 MHz. Le câble CAT 5 a récemment été remplacé par le CAT 5E comme norme de référence.

Blindage des câbles à paire torsadée

Il existe essentiellement deux types de paires torsadées : les paires torsadées blindées (STP) et les paires torsadées non blindées (UTP).

En général, les câbles STP et UTP possèdent deux paires de câbles (4 conducteurs). La paire torsadée écrantée (ScTP) est une paire torsadée non blindée de 100 Ω à quatre paires, toutes recouvertes d'une feuille ou d'un écran tressé afin de réduire les rayonnements EMI et la sensibilité au bruit extérieur. La paire ScTP est également appelée paire torsadée à feuille (FTP) ou paire UTP tressée (sUTP). Elle peut être considérée comme la version blindée des câbles UTP CAT 3, 4 et 5 et s'utilise dans les applications Ethernet de la même manière que le câblage UTP de catégorie équivalente.

NOTE : Le réseau Ethernet industriel Transparent Ready doit utiliser des câbles blindés CAT 5E.

Autres caractéristiques de câble

Les câbles UTP et STP existent sous deux formes : la forme massive et la forme toronnée. Le terme *massif* renvoie au fait que chaque conducteur interne est constitué par un seul fil. Le terme *toronné* signifie que chaque connexion se compose de plusieurs fils plus petits. Le seul avantage du câble toronné (en général beaucoup plus coûteux) par rapport à la forme massive est son petit rayon de courbure, qui lui permet d'être enroulé autour d'angles plus petits avec moins de perte. A tout autre égard, les deux formes de câbles affichent des performances identiques.

Caractéristiques de la couche physique

Le tableau ci-dessous récapitule certaines des nombreuses caractéristiques de couche physique définies pour Ethernet.

Standard	Débit de données	Technologie connecteur	Forme	Longueur maximale des segments de câble	
				Half Duplex	Full Duplex
10Base-T	10 Mbit/s (20 Mbit/s en mode Full Duplex optionnel)	RJ45	Deux paires de câble UTP 100 Ω CAT 3 ou supérieure	100 m	100 m
100Base-TX	100 Mbit/s (200 Mbit/s en mode Full Duplex optionnel)	RJ45	Deux paires de câble UTP 100 Ω CAT 5 ou supérieure	100 m	100 m
1000Base-T	1 Gbit/s	RJ45	Quatre paires de câble 100 Ω CAT 5 ou supérieure	100 m	100 m

Le standard 100Base-TX gère des transmissions sur plus de 100 m de câblage UTP 100 Ω CAT 5. Les câbles CAT 5 (pour 100Base-T) offrent une qualité de câblage supérieure aux câbles CAT 3 (pour 10Base-T). Ils conviennent pour des transmissions jusqu'à des fréquences de 100 MHz, alors que les câbles CAT 3 gèrent uniquement les transmissions jusqu'à 16 MHz. Le standard 100Base-TX permet l'utilisation optionnelle de câbles STP 150 Ω .

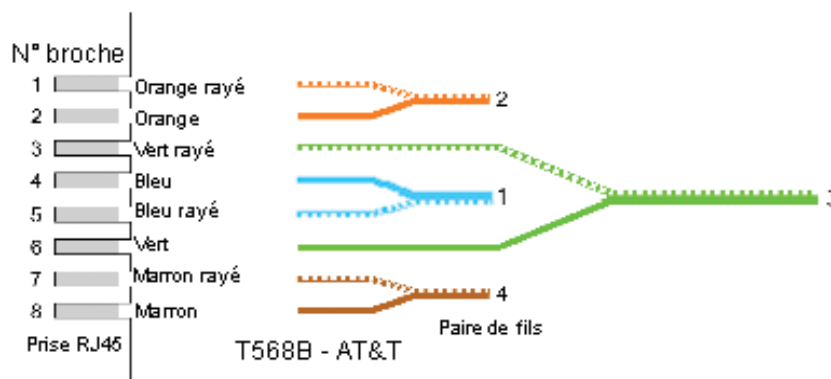
Caractéristiques de couleur des câbles

La norme EIA/TIA-568B spécifie le brochage des fils dans les prises et les connecteurs modulaires RJ45 à 8 broches. Elle définit également le code couleur applicable aux 8 fils des quatre paires. (Le code couleur est indépendant du type de réseau.) Reportez-vous à la norme EIA/TIA-568B pour connaître toutes les caractéristiques du brochage.

Les couleurs définies pour les 4 paires/8 câbles sont les suivantes :

Paire 1	Bleu/Blanc rayé bleu
Paire 2	Orange/Blanc rayé orange
Paire 3	Vert/Blanc rayé vert
Paire 4	Marron/Blanc rayé marron

Le code couleur de brochage spécifié pour le connecteur RJ45 est illustré ci-dessous.



Schneider recommande l'utilisation de la gaine de câble verte RAL 6018.

Différence entre les normes EIA/TIA 568A et EIA/TIA 568B

Dans ces deux codes couleur, la paire 2 (orange) et la paire 3 (verte) sont interverties. La norme EIA/TIA 568B reste la plus largement utilisée.

NOTE : Aucune différence n'est constatée entre ces deux schémas de câblage, que ce soit en termes de connectivité ou de performance, pour les connexions entre deux équipements (entre la prise et le panneau de raccordement, RJ-45 et RJ-45, etc.), tant que ces deux équipements sont câblés suivant le même schéma (A ou B).

Vous pouvez également vous reporter au chapitre Installation (*voir page 102*) pour obtenir plus d'informations sur l'installation du câblage.

Câbles à fibre optique

Résumé

Les câbles à fibre optique offrent une solution de câblage alternative aux câbles en cuivre, remplaçant les câbles UTP et STP classiques. Les câbles à fibre optique sont généralement utilisés dans les réseaux fédérateurs, en environnements bâtiments et campus. Grâce aux récentes évolutions en terme de performance, de connectivité et de test des fibres optiques, celles-ci représentent la meilleure solution pour les connexions LAN sur des longues distances, pour relier par exemple les usines de fabrication ou les installations industrielles. Cumulée à l'amélioration des émetteurs-récepteurs et à la baisse des coûts des câbles, la technologie des fibres optiques est sans conteste une option haute performance très attractive.

Normes applicables aux câbles à fibre optique

Les normes TIA/EIA existantes en matière de fibres optiques ne définissent pas d'architecture, comme les normes TIA/EIA 568-B et ISO/CEI 11801. Les normes de fibre optique s'appliquent, au contraire, à toutes les installations de fibre, quel que soit leur emplacement ou leur utilisation. Actuellement, ces normes n'établissent aucune distinction, en termes d'installation, entre les câbles à fibre optique suspendus sous l'eau ou en surface, placés à l'intérieur ou à l'extérieur d'un bâtiment, ou utilisés dans les réseaux fédérateurs ou dans les avions.

Description technique des câbles à fibre optique

Les câbles à fibre optique sont composés de deux longs brins fins de verre ultra pur (silice) ou de plastique qui transmettent des signaux optiques (lumineux) sur des longues distances. Ces brins de verre sont extrêmement fins (à peu près la taille d'un cheveu) et organisés en faisceaux, appelés câbles optiques.

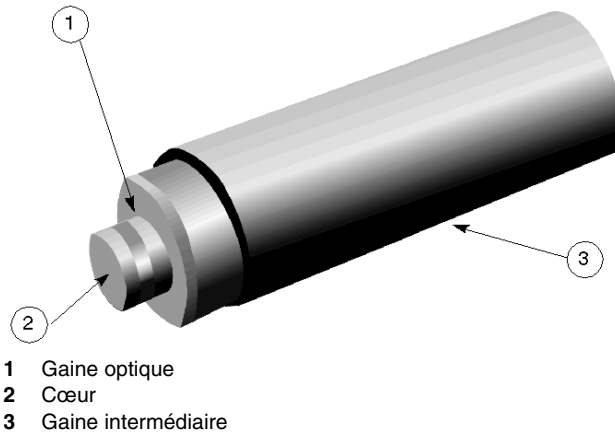
Un câble optique consiste en un cœur central de verre, enveloppé d'une gaine optique en verre et d'une gaine externe plastique. Les photons de lumière sont transmis via le cœur central et réfléchis le long des parois par le matériau réfléchissant de la gaine optique. Une fine gaine externe plastique (renforcée par des fibres spéciales) recouvre et protège les deux cœurs internes. Selon les types de câbles, la fibre optique peut contenir un cœur métallique renforçant la robustesse du câble.

Les câbles à fibre optique sont capables de transmettre des signaux sur des distances plus longues et à plus haute vitesse que les câbles cuivre. De plus, comme ces câbles transmettent de la lumière, ils ne génèrent aucune interférence électromagnétique, si problématique avec les câbles cuivre. Ils représentent donc une solution idéale pour les environnements industriels difficiles et les connexions extérieures entre les usines, grâce à leur excellente immunité à l'humidité et à la foudre.

Composition d'un câble à fibre optique

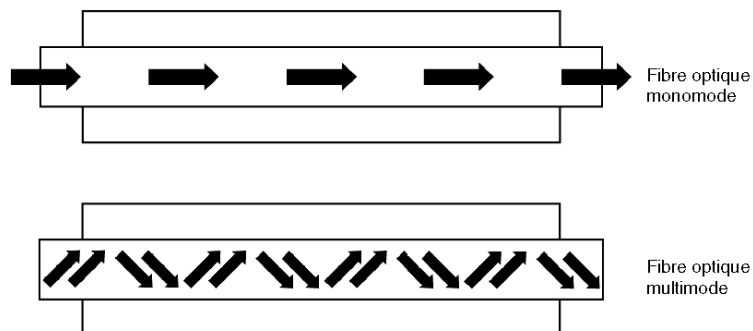
Un câble à fibre optique se compose normalement de trois parties distinctes :

- le cœur : partie centrale fine en verre de la fibre qui transmet la lumière ;
- la gaine optique : matériau optique externe qui enveloppe le cœur et réfléchit la lumière vers le cœur ;
- la gaine intermédiaire : gaine plastique externe qui protège chaque fibre des dommages et de l'humidité.



Types de câbles à fibre optique : introduction

Les signaux optiques se propagent à travers le cœur d'une fibre, en suivant un seul chemin (fibre optique monomode) ou plusieurs chemins (fibre optique multimode).



Types de câbles à fibre optique : multimode

Les fibres optiques multimodes ont un large diamètre de cœur (environ $2,5 \times 10^{-3}$ po. ou $62,5 \mu\text{m}$) et transmettent, à partir de diodes électro-luminescentes (DEL), de la lumière infrarouge (longueur d'onde = 850 à 1300 nm). Les câbles à fibre optique multimode sont essentiellement utilisés dans les réseaux LAN basés sur des DEL, les réseaux campus et les réseaux métropolitains de courte distance.

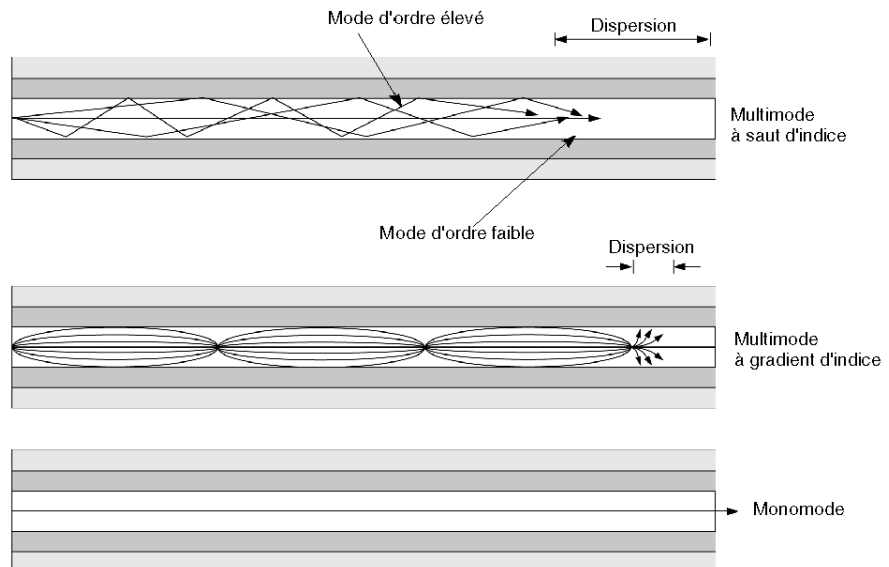
Il existe deux types de fibres multimodes :

- à saut d'indice : qui présentent un changement brusque entre le cœur et la gaine optique ; limitées à 50 Mbit/s environ ;
- à gradient d'indice : qui présentent un changement graduel entre le cœur et la gaine optique ; limitées à 1 Gbit/s.

NOTE : Les caractéristiques de cœur des fibres optiques multimodes à saut d'indice et à gradient d'indice sont généralement 50, 60,5 ou 100 μm . Le diamètre de la gaine optique des fibres à saut d'indice est de 125 μm .

Lorsque la fibre est graduée, l'indice de réfraction diminue à mesure que l'on s'éloigne du cœur. Etant donné que la lumière voyage plus rapidement lorsque la réfraction est faible, la lumière réfléchi par le matériau externe voyage donc plus vite qu'au centre du cœur.

Le schéma suivant illustre respectivement une fibre optique multimode à saut d'indice, multimode à gradient d'indice et monomode :



Types de câbles à fibre optique : monomode

Les fibres optiques monomodes ont un petit diamètre de cœur (environ $3,5 \times 10^{-4}$ po. ou $9 \mu\text{m}$) et transmettent de la lumière laser infrarouge (longueur d'onde = 1300 à 1550 nm). Elles n'offrent qu'un seul mode optique qui force la lumière à suivre un chemin linéaire à travers l'extrémité du câble, mais fournissent davantage de bande passante que les fibres multimodes. Les câbles à fibre monomode sont essentiellement utilisés dans les applications LAN intercentraux de longue distance à laser, les réseaux tout terrain et les liaisons sous-marines internationales. Les câbles utilisés sur des longues distances peuvent contenir entre 100 et 800 fibres/câble.

Comparaison entre les fibres monomodes et multimodes

Les fibres optiques monomodes bénéficient d'une plus grande capacité de données, d'une faible atténuation et d'un coût plus bas. Ce type de câble est le plus coûteux et le plus difficile à manipuler, mais il fournit la bande passante la plus large et les meilleures capacités en distance. Les avantages offerts par les fibres multimodes sont des coûts de connexion et d'électroniques bas, se traduisant par une baisse des coûts totaux d'installation.

Comparaison entre les câbles à fibre optique et cuivre

Les câbles à fibre optique présentent certains avantages par rapport aux câbles cuivre. Ceux-ci sont préférés pour une utilisation dans les réseaux fédérateurs et autres zones des réseaux LAN et Ethernet.

Ces avantages sont les suivants :

- Coût réduit : les câbles optiques sont moins coûteux que les fils en cuivre, pour des longueurs équivalentes
- Capacité de données accrue : la quantité importante de faisceaux de fibres optiques qu'ils contiennent permet de faire circuler davantage d'informations qu'un câble cuivre de même diamètre
- Dégradation restreinte du signal : les fibres optiques génèrent moins de perte de signal que les fils en cuivre, sur des distances équivalentes
- Plus fines, flexibles et légères : les fibres optiques peuvent être extraites avec un diamètre plus fin que les fils en cuivre, les rendant plus légères et flexibles et aussi plus faciles à placer dans des espaces confinés
- Faible puissance : les signaux optiques se dégradent moins et requièrent donc des émetteurs de faible puissance pour amplifier les signaux
- Aucune perturbation ou autre risque : l'absence de courant électrique à travers les fibres optiques évite tout risque d'interférences électromagnétiques, d'incendie ou de mise à la terre

Spécifications de la couche physique 10/100BaseF

Introduction

10/100BaseF renvoie à des spécifications de la couche physique particulières, applicables aux câbles à fibre optique transportant des signaux Ethernet.

Spécification du câble 10Base-FL

Le réseau Ethernet classique (10 Mbit/s) inclut des spécifications pour la couche physique 10Base-FL. Le 10Base-FL gère les réseaux fédérateurs de câbles à fibre optique jusqu'à 4 km. La norme de câblage des immeubles commerciaux TIA/EIA approuve l'utilisation du 10Base-FL pour les interconnexions entre les bâtiments de campus. Le 10Base-FL affiche une vitesse de transmission de 10 Mbit/s (20 Mbit/s en mode Full Duplex optionnel), avec une longueur de segment maximale de 2 000 m. Le câble standard est un câble à fibre optique multimode, de type 62,5/125 (cœur de 62,5 μm et gaine optique de 125 μm), avec une longueur d'onde de 850 nm.

Spécification du câble 100Base-FX

La spécification de couche physique 100Base-FX est approuvée par la norme IEEE 802.3u, applicable au réseau Fast Ethernet (100 Mbit/s) sur câble à fibre optique. Le 100Base-FX affiche une vitesse de transmission de 100 Mbit/s (200 Mbit/s en mode Full Duplex optionnel), avec une longueur de segment maximale de 2 000 m (Full Duplex). Le câble standard est un câble à fibre optique multimode (cœur de 62,5 μm et gaine optique de 125 μm), avec une longueur d'onde de 1300 nm.

Recommandations Schneider à propos des fibres optiques

Pour les applications Ethernet industriel Transparent Ready, Schneider recommande l'utilisation de fibre de type 62,5/125, avec une quantité minimale et une qualité maximale de fibre. Schneider prend en charge les communications sur des longueurs d'onde comprises entre 850 nm (10Base-FL) et 1 300 nm (100Base-FX). Le câble peut contenir d'autres fibres ou conducteurs électriques. Les spécifications de protection pour le câble doivent être compatibles avec vos conditions d'installation.

Environnement	Couche physique	Fibre recommandée	Longueur d'onde	Longueur maximale du segment
Environnement industriel léger et lourd	10Base-FL	62,5/125 (multimode)	850 nm	2 000 m
	100Base-FX	62,5/125 (multimode)	1 300 nm	200 m (Full Duplex)

Connecteurs Ethernet pour les réseaux en cuivre

Résumé

Après avoir mené une analyse approfondie des tendances de marché, des propositions de l'industrie et du travail de normalisation en cours, et en l'absence de normes internationales sur le câblage cuivre dans les réseaux Ethernet industriel au moment de la rédaction de ce guide, Schneider Electric a défini les types de connecteurs à utiliser dans les produits Ethernet industriel Transparent Ready.

Schneider Electric recommande l'utilisation du connecteur RJ45 dans les environnements de bureau et industriels légers (*voir page 76*) et l'utilisation du connecteur circulaire M12 codage D à quatre pôles dans les environnements industriels lourds.

Connecteurs cuivre Ethernet recommandés

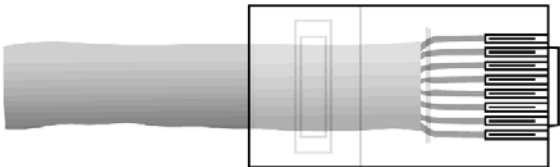
Le tableau suivant répertorie les caractéristiques des connecteurs en cuivre Ethernet industriel recommandés par Schneider Electric.

Environnement	Connecteurs	Caractéristiques générales	Référence
Industriel léger (faible charge d'activité)	RJ45		CEI 60603-7 et TIA/EIA 568B
		Brochage : ISO/CEI 8802-3	
		Code couleur du brochage : TIA/EIA 568B	
		Blindé	
Industriel lourd (forte charge d'activité)	M12 codage D à 4 pôles		CEI 61076-2-101
		Blindé	

Connecteur RJ45

Comme défini dans les normes Ethernet IEEE 802.3 et ISO/CEI 8802-3, le connecteur spécifié pour les couches physiques Ethernet 10Base-T et 100Base-TX est le RJ45 (installations en cuivre). L'appellation *RJ* (Registered Jack - prise enregistrée) est définie dans le Code des règlements fédéraux des Etats-Unis.

Le connecteur RJ45 est utilisé pour terminer les câblages à paire torsadée. Le schéma suivant illustre un connecteur RJ45 type :

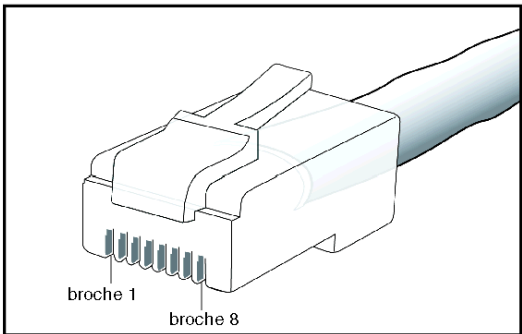


Connecteur RJ45 blindé (ou écranté)

Schneider Electric recommande l'utilisation de connecteurs RJ45 blindés dans les environnements de bureau et industriels légers, et l'utilisation de câbles blindés CAT 5E pour les réseaux Ethernet industriel 10Base-T et 100Base-TX. Si certains de vos équipements utilisent des connecteurs à prise blindée et sont mis à la terre en externe, le blindage du câble doit alors être mis à la terre aux deux extrémités du câble.

Broches RJ45 et signaux Ethernet

Le connecteur RJ45 possède 8 (huit) broches ou connexions électriques, numérotées de 1 à 8 de la gauche vers la droite.



Pour les réseaux 10Base-T et 100Base-TX, les broches RJ45 sont affectées comme suit :

Broche RJ45	Signal Ethernet
1	Emission + (TX+)
2	Emission - (TX-)
3	Réception + (RX+)
4	Non utilisé
5	Non utilisé
6	Réception - (RX-)
7	Non utilisé
8	Non utilisé

Lorsque vous fabriquez des câbles Ethernet, si vous envisagez d'utiliser uniquement 2 paires (4 conducteurs), vous devez tous les relier. Si vous utilisez 4 paires (8 conducteurs), Schneider vous recommande de les connecter comme spécifié par la norme EIA/TIA 568B, même si les broches 4, 5, 7 et 8 n'ont pas de signal affecté. Pour le code couleur recommandé basé sur la norme TIA/EIA 568B, reportez-vous à *Caractéristiques de couleur des câbles*, page 90.

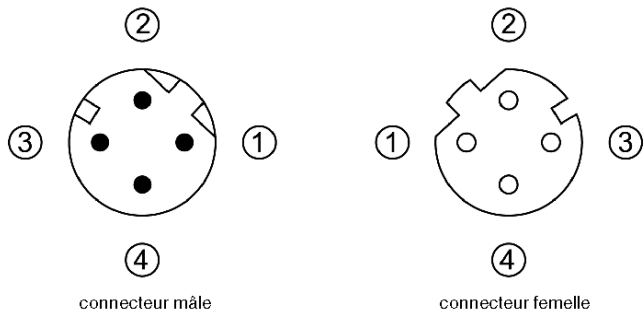
NOTE : Lorsque vous utilisez un câblage CAT 5/5e, les broches 4, 5, 6 et 8 ne sont pas nécessaires pour les couches physiques 10Base-T et 100Base-TX.

Connecteurs circulaires M12

L'utilisation des connecteurs circulaires M12 n'est pas encore régie par une norme spécifique. Toutefois, le connecteur circulaire M12 est utilisé au niveau du bus de terrain dans de nombreuses applications industrielles lourdes. Schneider Electric recommande le connecteur M12-4 (à 4 pôles) codageD pour les réseaux Ethernet industriel Transparent Ready installés dans les environnements industriels lourds.



Broches du connecteur circulaire M12 et signaux Ethernet



Pour les réseaux Ethernet 10Base-T et 100Base-TX, les signaux Ethernet sont affectés comme suit aux broches du connecteur circulaire M12 :

M12	Signal Ethernet
1	Emission + (TD+)
2	Réception + (RD+)
3	Emission - (TD-)
4	Réception - (RD-)

Connecteurs pour fibre optique

Développement de connecteurs pour fibre optique

Il existe plusieurs types de connecteurs pour fibre optique. Le connecteur pour fibre optique (FC) a été le premier connecteur développé avec une férule en céramique de 2,5 mm. Cette férule correspond au capuchon du connecteur qui enveloppe l'extrémité d'une gaine optique, par laquelle se fait la connexion. Le connecteur à terminaison droite (ST) a fait son apparition peu de temps après. Il est doté de la même férule en céramique, mais est plus simple à introduire en raison de son joint. Le connecteur abonné (SC) a été développé ensuite, devenant rapidement populaire. Les connecteurs à terminaison de masse (MT) et MT/RJ constituent les dernières avancées dans l'industrie du connecteur.

Connecteurs SC

Le connecteur SC est en passe de devenir le connecteur le plus répandu avec les câbles à fibre optique. Avec sa face avant carrée, il est plus facile à installer dans des espaces confinés.

Connecteurs ST

Le connecteur ST a été développé par AT&T. C'est le plus répandu dans les réseaux à fibre optique installés, puisqu'il a bénéficié d'une large popularité ces dernières années. Ressemblant à un connecteur BNC par sa forme conique, il est doté d'un joint à baïonnette permettant une insertion simple et rapide.

Connecteurs LC

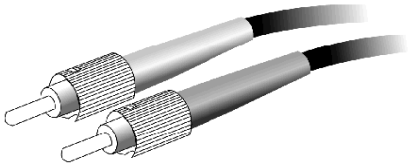
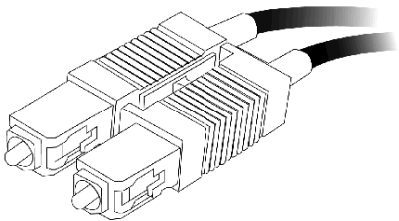
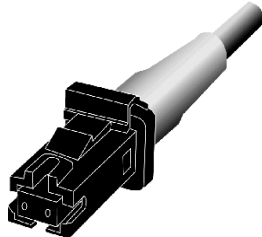
Le connecteur LC ressemble à un petit connecteur SC. Il a été développé par Lucent pour une utilisation en environnements de télécommunications. Il est régi par la norme EIA/TIA-604-10.

Connecteurs MT/RJ

Les connecteurs à faible encombrement (SFF), tel que le connecteur MT, sont apparus plus tardivement sur le marché des connecteurs optiques. Le connecteur MT se réfère aux 12 ou 24 fibres qu'il connecte. Son cousin duplex, le connecteur MT/RJ, a lui été nommé d'après le connecteur cuivre RJ-45 auquel il ressemble.

Connecteurs pour fibre optique

Schneider Electric recommande les connecteurs suivants pour toute utilisation dans le réseau Ethernet industriel Transparent Ready :

Environnement	Couche physique	Connecteur recommandé	Illustration
Environnement industriel lourd et léger	10Base-FL	ST	
	100Base-FX	SC	
	100Base-FX	MT-RJ	

Equipements d'infrastructure recommandés pour Ethernet industriel

Recommandations

Recommandations de Schneider Electric pour l'utilisation d'équipements d'infrastructure Ethernet industriel	
Généralités	Utilisez des commutateurs dès que possible pour supprimer les collisions, améliorer les performances et simplifier la conception du réseau. Eviter les concentrateurs dans la mesure du possible. Déterminez le trafic sur le réseau et segmentez correctement le réseau. Respectez les recommandations environnementales fournies dans ce manuel.
Lorsqu'une large disponibilité de bande passante est requise	Utilisez des commutateurs Full-Duplex (10Base-T/100Base-TX). Déterminez le trafic sur le réseau et segmentez correctement le réseau.
Pour les applications nécessitant une interruption d'application minimale	Utilisez un anneau auto-régénérant ou un anneau auto-régénérant redondant.
Pour les réseaux nécessitant un diagnostic de base (par ex., aucune liaison ou défaillance d'une alimentation)	Utilisez des commutateurs non gérés avec relais alarme.
Pour les réseaux nécessitant des services de haut niveau et une gestion du trafic	Utilisez des commutateurs gérés.
Pour les applications nécessitant une surveillance et une découverte de réseau	Utilisez des commutateurs gérés.
Pour les applications nécessitant l'interconnexion d'équipements éloignés les uns des autres (> 100 m)	Utilisez des produits à fibre optique. Fibre optique multimode : jusqu'à 2 km entre les nœuds. Fibre optique monomode : jusqu'à 15 km entre les nœuds. Remarque : Selon la fibre et le budget alloué aux produits optiques, il est possible d'atteindre 4 km en multimode et 30 km en monomode.
Pour les réseaux nécessitant une immunité aux interférences électromagnétiques	Utilisez des produits dotés de ports à fibre optique.
Pour les applications nécessitant un changement de support physique	Utilisez des émetteurs-récepteurs ou des commutateurs avec une combinaison de ports en cuivre et à fibre optique.
Pour les applications nécessitant un montage (IP67) externe du commutateur	Utilisez des commutateurs et des câbles IP67.

2.5 Installation

Vue d'ensemble

Ce sous-chapitre décrit les mesures que vous pouvez prendre afin d'empêcher les interférences électromagnétiques (EMI) de dégrader sérieusement votre réseau ou de causer des problèmes intermittents difficiles à diagnostiquer. La mise à la terre (également appelée mise à la masse), la liaison équipotentielle des équipements, armoires et bâtiments ainsi que la planification des chemins de câbles au sein du site sont également abordées en détail, avec une attention particulière accordée aux mesures à prendre pour un système de communications d'automatisation industriel.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Règles d'installation CEM pour les réseaux Ethernet	103
Liaison équipotentielle	105
Liaison équipotentielle de votre bâtiment	106
Liaison équipotentielle locale des équipements et des machines	108
Câblage de réseau Ethernet compatible avec CME et les chemins de câbles	109
Types de câbles cuivre Ethernet	115
Outils pour câbles cuivre Ethernet	118
Comment fabriquer un câble Ethernet	119
Administration du câblage	121
Documentation de câblage	123

Règles d'installation CEM pour les réseaux Ethernet

Introduction

Les méthodes suivantes, lorsqu'elles sont correctement intégrées dans la planification de votre réseau, peuvent vous permettre d'éviter les perturbations électromagnétiques et de créer un environnement compatible CEM.

La protection du réseau Ethernet contre les interférences électromagnétiques (EMI) est une préoccupation qui concerne l'ensemble de votre installation. Même s'il est important de considérer l'immunité aux EMI sur l'ensemble de votre système, ce sous-chapitre décrit uniquement les méthodes s'appliquant au réseau Ethernet. En réalisant la liaison équipotentielle, la mise à la terre, le câblage approprié et le blindage de votre site et de vos équipements, vous pouvez déjà réduire de manière significative une bonne partie de vos problèmes d'EMI.

Pour plus d'informations sur la norme CEM, reportez-vous à la section Exigences environnementales (*voir page 76*).

Pour plus d'informations sur les EMI, reportez-vous à la section EMI (*voir page 536*).

Mesures d'installation pour lutter contre les EMI dans les réseaux Ethernet

La liste suivante décrit les mesures clés à prendre en compte dans votre installation afin de réduire les interférences électromagnétiques dans un réseau Ethernet industriel :

- mise à la terre et liaison équipotentielle ;
- câblage et chemins de câbles compatibles CEM ;
- circuits d'équilibrage ;
- sélection des câbles ;
- blindage ;
- filtrage ;
- placement des équipements ;
- placement des fils ;
- transposition des lignes de départ/de retour ;
- isolation électrique.

Définition de la mise à la terre et de la liaison équipotentielle

La mise à la terre est la méthode utilisée pour transporter une charge électrique jusqu'au sol (la terre) le long d'un conducteur. Ces conducteurs peuvent être un fil électrique, une conduite métallique ou une armoire métallique.

La liaison équipotentielle est le fait de connecter des pièces conductrices, afin de créer un contact électrique à faible résistance pour le courant continu et les courants alternatifs basse fréquence. Cette interconnexion répartit le flux d'interférences sur plusieurs chemins, évitant ainsi leur concentration en un seul point.

Dans la plupart des cas, le système de liaison équipotentielle est mis à la terre. Le flux d'interférences termine donc dans la terre. Le flux d'une charge électrique est dispersé dans le sol, loin des équipements et des lignes de communication sensibles. La norme EN 50310 requiert que les bâtiments dotés de systèmes d'informations soient équipés d'un réseau de liaison commun (CBN) constitué d'éléments conducteurs multiples.

Liaison équipotentielle

Introduction

La liaison équipotentielle établit une interconnexion des parties conductrices qui disperse les flux d'interférences électromagnétiques en plusieurs chemins, les connectant à la terre via un système de mise à la terre. La conception d'un tel système est régie par les conditions et les exigences locales. Le niveau de simplicité ou de complexité qu'il doit présenter est déterminé par la configuration de votre bâtiment et de toutes les machines installées à l'intérieur.

Les rubriques suivantes décrivent en détail toutes les étapes à réaliser pour créer une liaison équipotentielle et des systèmes de mise à la terre sur votre site, afin de le protéger contre toute interférence électromagnétique. Pour plus d'informations, reportez-vous au sous-chapitre *Compatibilité électromagnétique*, page 536.

Composants du système de mise à la terre

Un système de mise à la terre type comprend trois composants :

- la *terre réelle*, qui conduit le courant jusqu'à la terre via une électrode de terre, un canal ou un conducteur métallique ;
- le *conducteur de terre principal*, un système conducteur auquel sont connectées la terre et toutes les parties nécessaires de l'installation ;
- les *conducteurs de terre*, qui connectent les parties de l'installation au conducteur de terre principal.

Liaison équipotentielle de votre bâtiment

Introduction

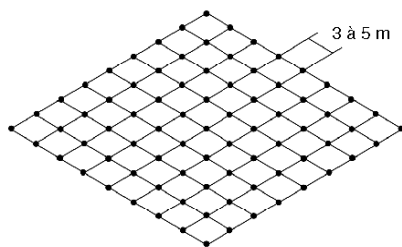
La norme EN 50310 requiert que les bâtiments dotés de systèmes de télécommunications soient équipés d'un réseau de liaison commun (CBN) constitué d'éléments multiples. Cela nécessite la création d'un connecteur de terre principal et le raccordement de tous les objets et structures métalliques du bâtiment à ce connecteur principal. Le CBN est ensuite connecté à un système d'électrodes de terre extérieur qui termine dans la terre.

Terminologie

Plan de terre : Grille maillée composée de barres d'armatures soudées, coulées dans la dalle en béton ou placées dans un faux sol dont la grille est constituée de conducteurs en cuivre.

Le *bus en anneau de mise à la terre* est la forme de connecteur de terre principal la plus efficace. Il est généralement installé au sous-sol ou au rez-de-chaussée des bâtiments équipés de systèmes de télécommunications. Les gaines métalliques des câbles, conduites, armoires et tuyaux d'eau et de chauffage sont connectées au connecteur de terre principal par le chemin le plus court.

Le schéma ci-dessous illustre un système de mise à la terre avec un plan de terre et un bus en anneau de mise à la terre :



Procédure

La procédure suivante décrit comment créer un système de mise à la terre pour un bâtiment. L'installation d'un système de mise à la terre constitue la première étape de création d'un environnement CEM (*voir page 536*).

Etape	Action
1	Créez un plan de terre et un bus en anneau.
2	Interconnectez toutes les structures métalliques du bâtiment.

Les structures métalliques incluent : les éléments structurels métalliques, les armatures soudées en béton, les tuyaux et gaines métalliques, les chemins de câbles, les conduites d'alimentation, les convoyeurs, les cadres de fenêtres et portes métalliques et les grillages. L'interconnexion forme un réseau de liaison commun qui constitue le principal système de mise à la terre du bâtiment.

NOTE : Concevez et créez un plan de terre à mailles serrées dans les zones de stockage ou d'utilisation de matériels sensibles, comme les équipements de mesure et de traitement de données.

Liaison équipotentielle locale des équipements et des machines

Introduction

Après avoir créé une liaison équipotentielle pour le bâtiment (*voir page 106*), vous pouvez créer une liaison équipotentielle basse fréquence et haute fréquence locale pour vos équipements et vos machines.

Etape	Action	Conseils
1	Interconnectez systématiquement toutes les structures métalliques de chaque équipement pour créer des systèmes de mise à la terre locaux (trames de mise à la terre).	Toutes les structures, des armoires avec leurs plaques de plan de terre aux chemins de câbles, tuyaux et cadres métalliques des machines, doivent être interconnectées.
2	Si besoin, ajoutez des connecteurs de terre pour les interconnexions entre des pièces conductrices exposées.	Vérifiez que les extrémités utilisées et non utilisées de tous les conducteurs de câbles sans exception sont connectées au système de mise à la terre.
3	Connectez le système de mise à la terre de trame local au système de mise à la terre du site en fournissant le nombre maximum de connexions distribuées.	-

Connexion des armoires au système de mise à la terre local

Vérifiez qu'une plaque de plan de terre est bien installée au fond de chaque armoire.

Toutes les pièces métalliques exposées des composants et des appareils encastrés dans une armoire doivent être directement vissées sur la plaque de plan de terre, afin de fournir un contact intermétallique haute qualité et durable.

NOTE : En raison de sa longueur excessive, le connecteur de terre principal vert/jaune ne peut généralement pas fournir une mise à la terre haute fréquence de qualité.

Câblage de réseau Ethernet compatible avec CME et les chemins de câbles

Classification des signaux

Dans un environnement industriel, les signaux sont classés en quatre catégories en fonction de leurs performance CME. Cette classification est nécessaire pour appliquer les règles de câblage.

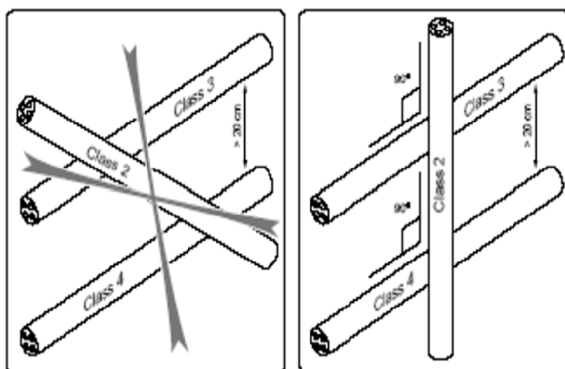
Performance CME			
Catégorie	Sensibilité	Interférence	Exemple de circuit ou d'appareil
-	Automates	Transformateurs dans l'armoire	-
	PCBs	Contacteurs	
	Régulateurs	Disjoncteurs	
	Câbles connectés aux entrées et aux sorties	Fusibles	
		Commuter les alimentations	
	Câbles de catégorie 1 ou 2 transportant des signaux analogiques	Convertisseurs de fréquence	
		Unités à vitesse variable	
		Alimentations CC	
		Horloges à microprocesseur	
		Câbles connectés à ces composants	
		Les lignes d'alimentation	
		Câbles d'alimentation	
1: Sensible	Le signal est très sensible	-	Circuits état bas avec des sorties analogiques)
			Les capteurs
			Circuits de mesure (les sondes, les capteurs, etc.)
2: Légèrement sensible	Le signal est sensible. Peut perturber les câbles de catégorie 1	-	Circuits en logique programmée connectés à des charges résistives
			Circuits numériques état bas)
			Circuits de niveau faible avec sorties tout ou rien
			Alimentations cc état bas

	Performance CME		
Catégorie	Sensibilité	Interférence	Exemple de circuit ou d'appareil
3: Créée de légères interférences	-	Le signal perturbe les câbles de catégories 1 et 2	Circuits en logique programmée avec des charges inductives et une protection adéquate
			alimentations CA propres
			Alimentations principales connectées à des appareils électriques
4: Interférences	-	Le signal perturbe d'autres catégories de signaux	Machines à souder
			Circuits électriques
			Régulateurs de vitesse électroniques
			Commuter les alimentations

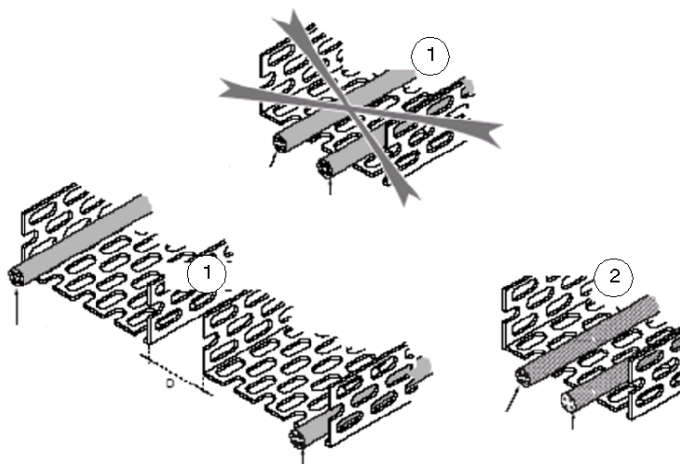
L'émission de données, telles que celles qui se trouvent sur un réseau Ethernet, est un signal de catégorie 2.

Recommandations générales de câblage

- Liez le site et les armoires de manière équipotentielle.
- Eloignez les sources possibles d'interférence des équipements sensibles.
- Ne combinez pas les signaux de réseau Ethernet avec des signaux de catégories 3 ou 4 dans le même câble ou conducteur en faisceau.
- Essayez toujours d'accroître la distance entre le câble de réseau Ethernet et les câbles transportant des signaux de différentes catégories, surtout des signaux interférents (3-4). Plus le chemin de câbles est long, plus le dégagement requis entre les câbles sera élevé.
- Pour tirer profit des effets de protection haute fréquence, aplatissez toute connexion contre des structures sous courant exposées de manière équipotentielle. Pour des connexions internes à des armoires et des machines, aplatissez systématiquement les câbles contre les supports métalliques.
- Assurez-vous que les câbles de réseau Ethernet croisent perpendiculairement tous les câbles transportant des signaux interférents (3-4) comme dans l'illustration ci-dessous :



- Si vous avez besoin de co-localiser des câbles transportant des signaux de catégories différentes dans une seule goulotte de câble, utilisez des câbles blindés comme dans l'illustration ci-dessous :

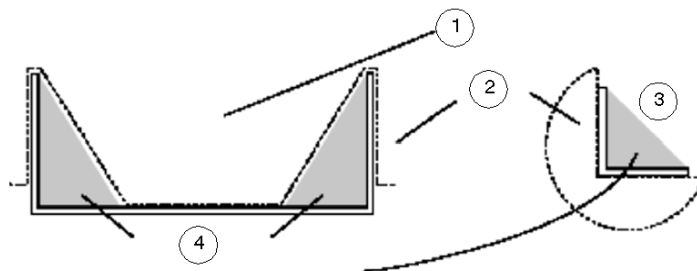


- 1 câbles non blindés
2 câbles blindés

- Etablissez la continuité du plan de terre entre deux armoires, machines, ou pièces d'équipement. Placez tous les conducteurs contre le plan de terre de bout en bout (le panneau situé au bas de l'armoire, les parties conductrices exposées des boîtiers métalliques, les structures équipotentielles de machine ou d'immeuble, les conducteurs d'accompagnement, les goulottes de câbles, etc.).
- Suivez les règles de blindage décrites dans ce sous-chapitre.

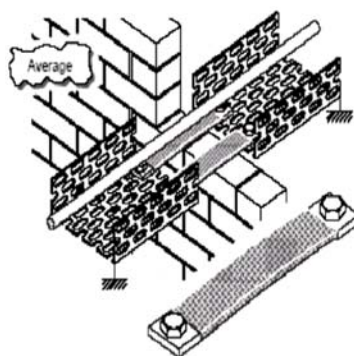
Recommandations pour les chemins de câbles

- Utilisez des goulottes de câbles métalliques. Lorsqu'ils sont connectés correctement, ils fournissent un câble blindé très efficace.
- Les effets d'écran, protecteurs, ou de blindage d'une goulotte de câble métallique dépend de la position du câble. Installez les câbles de réseau Ethernet dans les coins d'une gaine de câble comme dans l'illustration ci-dessous :



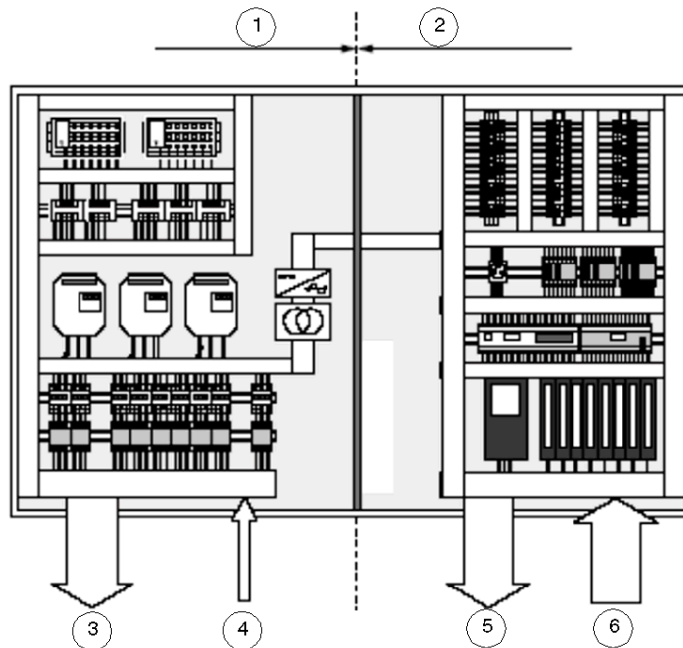
- 1 gaine de câble ouverte
- 2 zone exposée aux perturbations EMI
- 3 angle de coin
- 4 zone surtout protégée contre les perturbations EMI

- Si pour des raisons particulières le câble de réseau Ethernet devait être installé dans la même goulotte que les câbles de type 3 et 4, laissez la goulotte du câble ouverte. *Ce type d'installation n'est pas recommandé.*
- Dans la mesure du possible, utilisez deux gaines métalliques, une pour les signaux interférents (alimentation, relais et des varistors) et l'autre pour les câbles de signaux (les capteurs, les données, les télécoms.). Ces deux gaines peuvent être en contact si elles sont inférieures à 30 m. A partir de 30 à 100 m, espacez les de 10 cm, soit l'un à côté de l'autre soit l'un au-dessus de l'autre.
- A tout moment, chevauchez et boulonnez les extrémités des gaines de câbles métalliques ensemble. Si cela n'est pas possible, installez un lien torsadé large qui joint les deux gaines sous chaque table comme le montre l'illustration ci-dessous :



Recommandations sur le routage des câbles dans une armoire

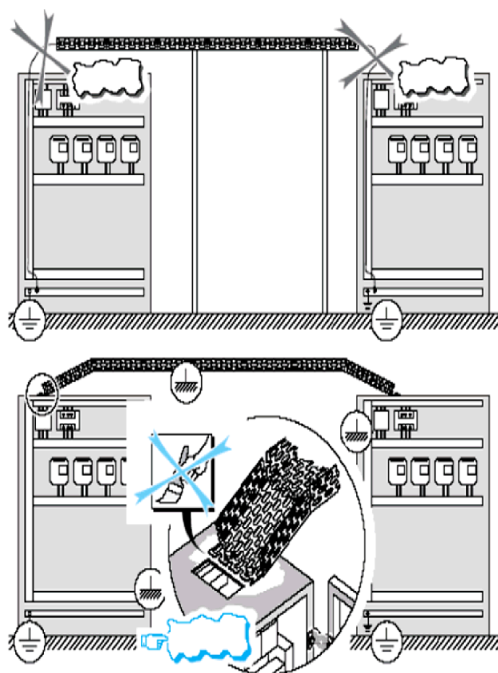
- Adoptez les bonnes pratiques de câblage.
- Suivez les recommandations applicables aux chemins de câbles décrites ci-dessus.
- Essayez toujours de séparer et de placer les composants et les câbles brouilleurs et sensibles dans des armoires distinctes.
- Dans les armoires de petite taille, un simple partitionnement des types de signaux par des panneaux métalliques vissés au châssis peut être suffisant. Dans les armoires plus larges, affectez une armoire à chaque classe de composant. Lorsque cela est possible, déployez les câbles dans les conduites métalliques.



- 1 Puissance
- 2 Niveau faible
- 3 Vers les composants d'alimentation
- 4 Secteur
- 5 Actionneurs
- 6 Capteurs

Routage des câbles à l'extérieur et entre les armoires

- Utilisez des conceptions en métal pour toutes les conduites supérieures à 3 m de longueur.
- Vissez les extrémités des conduites et des chemins de câbles métalliques sur les armoires métalliques, afin de sécuriser les connexions, comme illustré ci-dessous :



Routage des câbles à l'extérieur et entre les bâtiments

Il existe généralement un manque de liaison équipotentielle entre deux bâtiments. Les deux connexions à la terre (une par bâtiment) doivent être raccordées. Tous les chemins de câbles entre deux bâtiments doivent être doublés avec large superficie de ligne équipotentielle (35 mm^2). Dans les applications Transparent Ready, utilisez un câble à fibre optique pour les liaisons de données entre les bâtiments. Les liaisons optiques éliminent les problèmes de boucle entre les bâtiments.

Types de câbles cuivre Ethernet

Câbles Ethernet

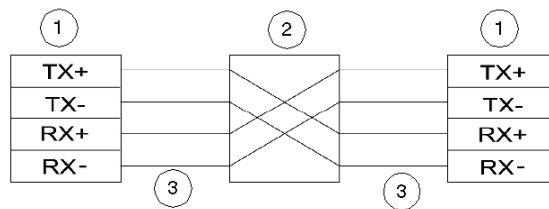
Vous pouvez fabriquer deux types de câble Ethernet : un câble simple ou un câble inverseur.

Câble simple

Les équipements d'infrastructure Ethernet, tels que les commutateurs et les concentrateurs, sont toujours placés entre deux terminaux. En général, ces équipements d'infrastructure *croisent* le signal. Par conséquent, le câble entre le terminal et le concentrateur ou le commutateur doit être un câble simple.

Brochage d'un câble simple

Les normes EIA/TIA 568B et IEEE 802.3u définissent le brochage d'un câble simple Ethernet, comme illustré ci-dessous :



- 1 Equipement terminal
- 2 Equipement intermédiaire
- 3 Câble simple

Le raccordement des broches d'un connecteur RJ45 entre un équipement terminal et un équipement intermédiaire s'effectue via des câbles simples, conformes aux spécifications de code couleur de signal (*voir page 90*).

Signal (dans un équipement terminal à prise)	Broche RJ45	Broche RJ45	Signal (dans un équipement intermédiaire à prise)
TX+	1	1	RX+
TX-	2	2	RX-
RX+	3	3	TX+
Non utilisé	4	4	Non utilisé
Non utilisé	5	5	Non utilisé
RX-	6	6	TX-
Non utilisé	7	7	Non utilisé
Non utilisé	8	8	Non utilisé
Equipement terminal	Câble simple		Equipement intermédiaire

1 Orange rayé

2 Orange

3 Vert rayé

4 Bleu

5 Bleu rayé

6 Vert

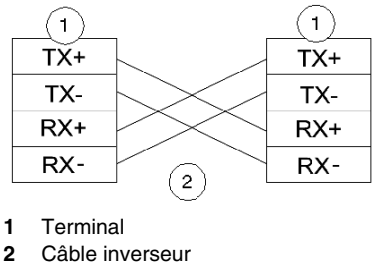
7 Marron rayé

8 Marron

Câble inverseur

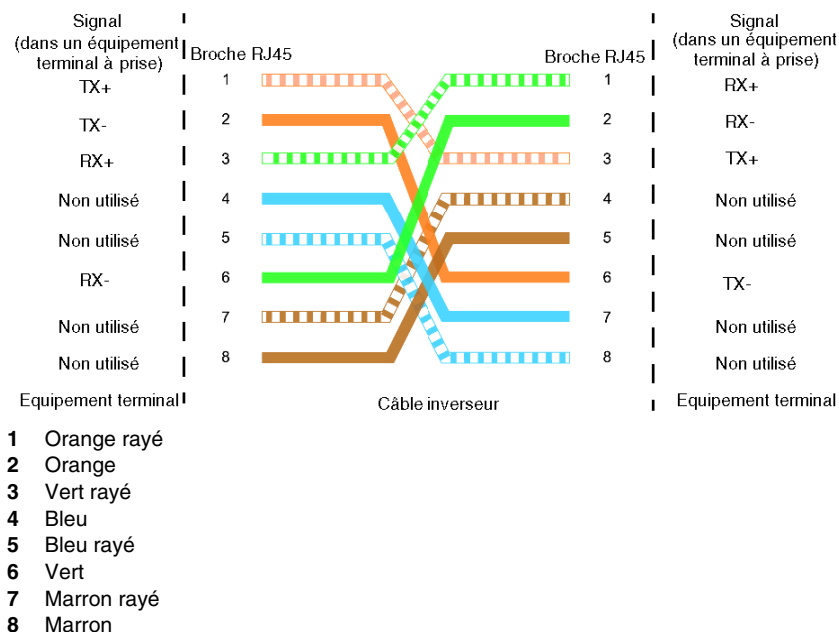
Lorsque deux terminaux sur un réseau Ethernet communiquent entre eux sur une connexion directe, les signaux d'émission d'un terminal doivent être reliés aux signaux de réception de l'autre terminal, et inversement.

Pour établir une connexion directe entre deux terminaux, utilisez un câble inverseur. Une connexion directe implique qu'aucun équipement intermédiaire n'est installé entre les deux terminaux que vous connectez.



Brochage d'un câble inverseur

La norme EIA/TIA 568B définit le brochage d'un câble inverseur Ethernet. La connexion directe des broches entre deux terminaux s'effectue via un câble inverseur conforme aux spécifications illustrées ci-dessous.



MDI/MDI-X

Aujourd'hui, la plupart des équipements d'infrastructures disponibles sur le marché (concentrateurs, commutateurs, routeurs, etc.) prennent en charge la fonction MDI/MDI-X (interface dépendante du médium/interface croisée dépendante du médium) dans leurs ports Ethernet. Cette fonction permet la commutation automatique des paires d'émission et de réception. Pour connecter ce type d'équipement d'infrastructure, utilisez un câble simple ou un câble inverseur ; l'équipement détecte et gère les paires TX/RX.

Outils pour câbles cuivre Ethernet

Introduction

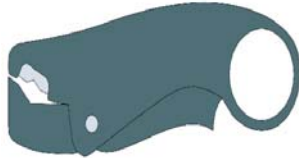
Pour fabriquer un câble cuivre Ethernet, vous devez disposer des trois outils suivants :

- Pince à dénuder
- Coupe-câble
- Pince à sertir

Pour savoir comment utiliser ces outils pour fabriquer un câble, reportez-vous à *Comment fabriquer un câble Ethernet, page 119*.

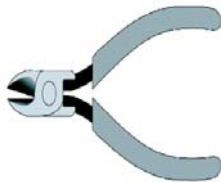
Pince à dénuder

Les outils à dénuder servent à retirer l'enveloppe de protection extérieure du câble pour faire apparaître le matériau d'âme conducteur.



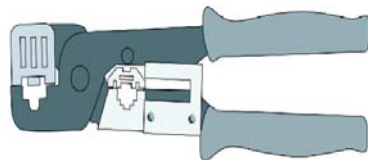
Coupe-câble

Les outils de coupe permettent de couper proprement un câble dans le sens du diamètre, afin d'obtenir deux longueurs. Choisissez un coupe-câble en veillant à ce que sa taille soit appropriée au diamètre du câble à couper.



Pince à sertir

Les outils de sertissage servent à placer la gaine autour du câble et à la fixer par pression.



Comment fabriquer un câble Ethernet

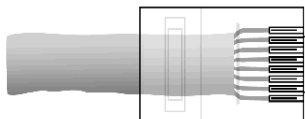
Avant de commencer

Assurez-vous que vous disposez des équipements suivants :

- connecteurs RJ45(deux pour chaque câble plus des suppléments) ;
- câble Ethernet ;
Pour 10Base-T, un câble Ethernet STP CAT 3 ou CAT 5, 5e ou 6 est recommandé ; 100 m ou moins ;
- Pour 100Base-TX, un câble Ethernet STP CAT 5, 5e ou 6 est recommandé ; 100 m ou moins ;
- outils de fabrication de câbles (*voir page 118*)de base.

Fabrication d'un câble cuivre Ethernet

Etape	Action	Commentaire
1	A l'aide de l'outil à dénuder, dénudez 2 po. de la gaine plastique sur une extrémité du câble.	-
2	Tenez la base de la gaine plastique avec une main et enlevez les fils avec l'autre main. Ne laissez pas les fils se détordre à l'intérieur de la gaine.	Conservez les paires de fils colorées ensemble et dans le même ordre : marron, bleu, vert et orange.
3	Tenez fermement les fils à l'endroit où ils sont insérés dans la gaine plastique. Placez votre coupe-câble bien droit sur les fils séparés à environ 0,5 po. du bord de la gaine plastique.	Veillez à placer bien droit votre coupe-câble sur les fils pour qu'ils soient tous coupés à la même longueur (0,5 po.).
4	Faites une coupe franche sur les quatre paires de fils.	Maintenez fermement la gaine lorsque vous coupez les fils. Ne laissez pas les fils se détordre à l'intérieur de la gaine pendant la coupe.
5	Tenez fermement la prise RJ45 entre deux doigts et faites glisser les fils dans la prise. Veillez à bien respecter le code couleur de brochage correspondant au type de câble que vous fabriquez.	Si les fils résistent, continuez à les enfoncer, jusqu'à ce qu'ils soient insérés dans la prise, comme requis. Ne relâchez pas les fils tant qu'ils ne sont pas insérés.
6	Enfoncez les fils jusqu'à ce qu'ils touchent pratiquement l'avant de la prise.	La gaine plastique doit être placée à environ 3/8 po. à l'intérieur de la prise.
7	Insérez la prise dans la pince à sertir et serrez très fort la pince jusqu'à ce que la prise soit solidement sertie sur l'extrémité du câble.	Si vous n'avez pas réussi à la sertir correctement la première fois, repositionnez la pince et réessayez.
8	Contrôlez la prise afin de vous assurer que le sertissage est sécurisé.	Examinez l'avant de la prise afin de vous assurer que les connexions en cuivre ne compriment pas les fils. Examinez l'arrière de la prise afin de vous assurer que la gaine plastique est enfoncée de 3/8 po. environ dans la prise. Remarque : Veillez particulièrement à ce qu'aucun fil ne dépasse de l'arrière de la prise.



Fabrication d'un câble à fibre optique Ethernet

La fabrication d'un câble à fibre optique Ethernet nécessite des procédures et des outils spécifiques. Demandez l'aide d'un technicien qualifié et formé pour cette opération.

Administration du câblage

Introduction

La norme EN 50174-1 décrit les spécifications relatives à l'administration du câblage. L'administration du câblage implique la gestion des éléments suivants :

- codes et méthodes d'identification ;
- étiquetage des câbles et des composants ;
- emplacement et application des étiquettes ;
- durée de vie et qualité des étiquettes ;
- contrôle et mise à jour de l'étiquetage ;

Actuellement, il n'existe aucune norme internationale qui régit ces aspects du câblage.

Norme EN 50174-1 et identificateurs

Pour connaître les directives générales relatives à l'étiquetage des câbles et aux identificateurs, reportez-vous aux chapitres 7.2 et 7.5 de la norme EN 50174-1:2000. Une synthèse de ces directives est fournie ci-après.

La maintenance des composants d'un système de câblage est généralement assurée par plusieurs personnes, ce qui requiert l'utilisation d'identificateurs, afin de marquer toute information pertinente sur le composant. Par exemple, vous pouvez appliquer un identificateur, que ce soit sous la forme d'une étiquette ou d'un code barre, afin de préciser l'endroit où est installé un câble à paire torsadée blindée CAT 5E dans le système de câblage horizontal d'un bâtiment. Le chapitre 7.5 de la norme EN 50174 spécifie les composants de câblage qui requièrent ce type d'identification.

Étiquetage des câbles et des composants

L'étiquetage des câbles et des composants est obligatoire lors de la phase d'installation. Vous pouvez soit attachez des étiquettes au composant, soit les fixer directement sur le composant. Dans certains cas, les composants peuvent être étiquetés plusieurs fois. L'exigence minimale en vigueur recommande d'étiqueter un câble aux deux extrémités.

Les exigences suivantes sont spécifiées dans la norme EN 50174-1 :

- Les étiquettes doivent être :
 - faciles d'accès ;
 - faciles à lire ;
 - faciles à changer ou modifier (le cas échéant).
- Les étiquettes doivent être solides et leurs marquages lisibles sur toute la durée de vie du câblage.
- Les étiquettes ne doivent pas être abîmées par l'humidité, ni être tâchées lors des manipulations.
- Les étiquettes destinées à un usage en extérieur ou en environnement difficile doivent être conçues de façon à supporter les conditions rigoureuses de ces environnements.
- Lorsque vous devez apporter des changements à un système de câblage, par exemple au panneau de raccordement, examinez les étiquettes pour vérifier si les informations sont correctes ou si elles nécessitent une mise à jour.

Documentation de câblage

Introduction

Les normes ISO/CEI 14763-1 et EN 50174-1 décrivent les spécifications relatives à la documentation du câblage. Ce sous-chapitre reprend les différentes directives et exigences spécifiées dans la norme EN 50174-1:2000, chapitre 6.1 et fournit des recommandations pour la gestion de la documentation.

Création de la documentation

Lors de l'installation du câblage, vous devez créer une documentation à la fois pendant et après la phase d'installation. Cette documentation doit décrire en détail les caractéristiques d'installation. Les recommandations fournies ci-après peuvent vous aider à déterminer le niveau de documentation nécessaire pour votre installation.

NOTE : Il est recommandé de conserver un niveau de détails identique pour votre documentation lors des phases de conception et d'installation.

Recommandation 1 : installations commerciales

La documentation commerciale doit inclure toutes les informations techniques et contractuelles concernant les exigences utilisateur final et l'installation en cours.

Elle doit également inclure les éléments suivants :

Caractéristique d'installation	Voir norme EN 50174-1:200, chapitre 5.2
Plan qualité	Voir norme EN 50174-1:200, chapitre 5.3
Documentation de câblage final	Voir norme EN 50174-1:200, chapitre 6.2

Recommandation 2 : test de réception des composants

Lorsque cela est nécessaire, votre documentation doit fournir des informations détaillées sur les essais de réception des composants. Elle doit notamment comprendre :

- une preuve de la conformité (par exemple, pour les câbles, les connecteurs et les ensembles câbles) ;
- les rapports d'essais de réception des câbles et informations associées ;
- les rapports d'essais de réception des ensembles câbles et informations associées ;
- les informations de livraison (par exemple, identificateurs de câbles et de composants uniques, comme les dates de réception et les numéros de lots ou les codes d'identification).

Recommandation 3 : identificateurs de câblage

Avant de commencer, établissez un schéma d'étiquetage. Pour associer les résultats d'essais de câblage aux composants correspondants, veillez à ce que le nom spécifié sur l'essai corresponde à l'étiquette fixée sur le panneau de raccordement ou sur la prise. Pour plus d'informations, reportez-vous aux directives d'étiquetage décrites au sous-chapitre Etiquetage des câbles et des composants (*voir page 122*).

Recommandation 4 : gestion des résultats d'essai

Vos données d'essai doivent être correctement organisées et stockées. Une gestion appropriée des résultats d'essai est une condition déterminante de la réussite d'une installation. Les résultats d'essai valident la performance et la conformité CEM d'un système de câblage, permettant ensuite d'évaluer les composants et de disposer d'un historique de données fiable et pertinent. C'est en réalisant des essais de câblage précis que vous pourrez réellement vérifier que votre installation répond aux exigences de conception initiales et est conforme aux normes régionales et internationales. Selon le type d'installation, vous devrez peut-être inclure les données d'essai dans votre documentation d'installation. (Voir Recommandation 2 (*voir page 123*))

2.6 Vérification d'un réseau Ethernet industriel Transparent Ready

Aperçu

Ce chapitre décrit le processus de vérification de votre installation de câblage basé sur les exigences de la norme ISO/CEI 11801. La vérification est une étape clé et délicate qui vous permet d'assurer la conformité de votre installation aux normes en vigueur. Vous devez aussi bien tester l'intégralité de l'installation de câblage que chacun des composants du réseau. Vous avez la possibilité de tester chaque section du réseau au cours de l'installation (recommandé) et/ou de planifier une étape de vérification finale, lors de laquelle vous pourrez tester l'intégralité de l'installation. Etant donné que ces tests sont le seul moyen de vérifier que votre installation satisfait bien aux normes internationales et locales, Schneider Electric souhaite que vous vous familiarisiez avec les recommandations énoncées dans ce chapitre et dans le Chapitre 3.

Pour le moment, il n'existe pas de norme internationale pour la planification et l'installation d'un réseau Ethernet industriel. Toutefois, des recommandations émises par des organisations Ethernet industriel ainsi que les activités continues ont conduit à la création d'un projet de norme. Cette norme devrait être publiée sous le nom ISO/CEI 24702 à la fin de 2006.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Recommandations de vérification de réseaux Ethernet industriel Transparent Ready	126
Liaisons permanentes	127
Voies	129
Test d'une installation en cuivre	131

Recommandations de vérification de réseaux Ethernet industriel Transparent Ready

Introduction

Schneider Electric recommande de respecter les exigences de réseaux Ethernet industriel préalablement décrites dans ce chapitre.

Un réseau Ethernet industriel Transparent Ready certifié doit remplir les conditions suivantes :

Exigences des réseaux Ethernet industriel Transparent Ready	
(1) – Exigences d'installation	Installation correcte telle que définie par la norme ISO/CEI 11801. Installation correcte telle que spécifiée dans ce guide. Installation correcte telle que requise par l'application, par exemple, câblage d'un équipement ou d'une machine conformément aux spécifications fournies par le fabricant.
(2) – Exigences de performance	Critères de performance tels que spécifiés par la norme ISO/CEI 11801.
(3) – Exigences environnementales	Protection environnementale telle que décrite dans ce guide.

La discussion suivante fournit des informations sur la manière de tester un réseau et de vérifier sa conformité aux exigences spécifiées en (1) et (2) du tableau ci-dessus.

Recommandations supplémentaires

Outre les exigences spécifiées par la norme ISO/CEI 11801, Schneider Electric vous recommande les pratiques suivantes :

- 1 Sélectionnez les composants appropriés, comme définis dans ce guide, de telle sorte que le réseau soit conforme aux exigences de performance et environnementales d'un réseau Ethernet correctement installé. Lisez attentivement ce guide avant de sélectionner les composants ou de commencer à installer votre réseau Ethernet industriel Transparent Ready.
- 2 Utilisez des outils homologués pour mesurer et vérifier la qualité de votre installation et sa conformité aux réglementations.
- 3 Faites appel à des installateurs de réseaux Ethernet certifiés au niveau local et/ou international.

Liaisons permanentes

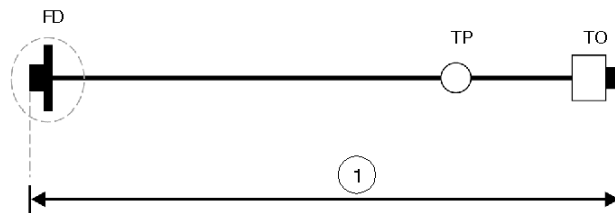
Résumé

Une liaison permanente, utilisée pour les tests, consiste en un câble horizontal doté d'une prise pour station de travail, d'un panneau de raccordement et d'une rallonge de câble de 2 m à chaque extrémité pour les tests. Elle peut avoir une longueur maximale de 90 m, conformément à la norme TIA/EIA 568B. La liaison permanente se compose uniquement des sections passives d'un câble et du matériel de connexion. Un point de transition, pour la connexion des câbles, peut être inclus dans le sous-système horizontal de la liaison.

La liaison permanente va du connecteur à prise RJ45, à une extrémité de câble, à la prise RJ45, à l'autre extrémité. Lorsqu'un testeur est connecté au câble, l'effet induit par le câble et les autres équipements du testeur connectés au câble est automatiquement supprimé des mesures par le testeur. Cette même mesure supprimée apparaît avec le câble connecté entre la dernière prise RJ45 et le voyant distant requis pas le testeur.

Exemple 1

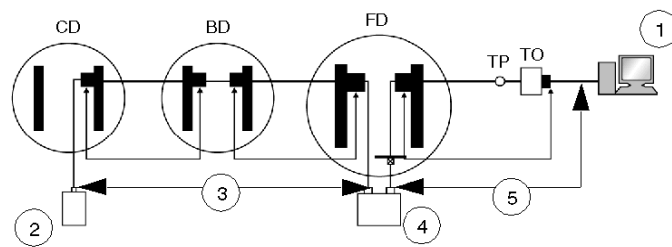
Une liaison permanente entre un répartiteur sol (FD) et une prise de terminal (TO) est illustrée ci-dessous. Un point de transition (TP) est inclus dans le sous-système horizontal :



1 Liaison permanente

Exemple 2

Le schéma ci-dessous illustre des terminaux dans une zone de travail, connectés à un serveur hôte via trois liaisons permanentes, soit deux liaisons par fibre optique et une liaison par câble équilibré :



- 1 Terminal
- 2 Hôte
- 3 Câble à fibre optique
- 4 Convertisseur optoélectronique optionnel
- 5 Voie de câble équilibré

Les liaisons par câble à fibre optique et par câble équilibré sont connectées entre elles à l'aide d'un convertisseur de fibre optique en câble équilibré, d'un répartiteur et de deux câbles d'équipements. Des interfaces de câblage sont également prévues à chaque extrémité de la liaison permanente. Ces interfaces de câblage sont spécifiées à la prise de terminal et à tout point où des équipements spécifiques à l'application sont connectés au câblage. La zone de travail et les câbles des équipements ne sont pas inclus dans la liaison permanente.

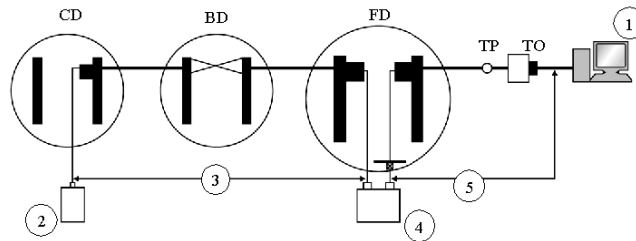
Voies

Introduction

Une voie est un ensemble de liaisons permanentes formées par les sections passives d'un câble, le matériel de connexion, les cordons des zones de travail, les câbles des équipements et les câbles de raccordement. Les voies ne croisent pas de commutateurs ou de concentrateurs, considérés comme des points limites dans n'importe quelle voie. Il est recommandé de tester toutes les liaisons permanentes individuellement, puis de tester les voies.

Exemple 1

Le schéma ci-dessous illustre des terminaux dans une zone de travail, connectés à un serveur hôte via deux voies, soit une voie par fibre optique et une voie par câble équilibré :

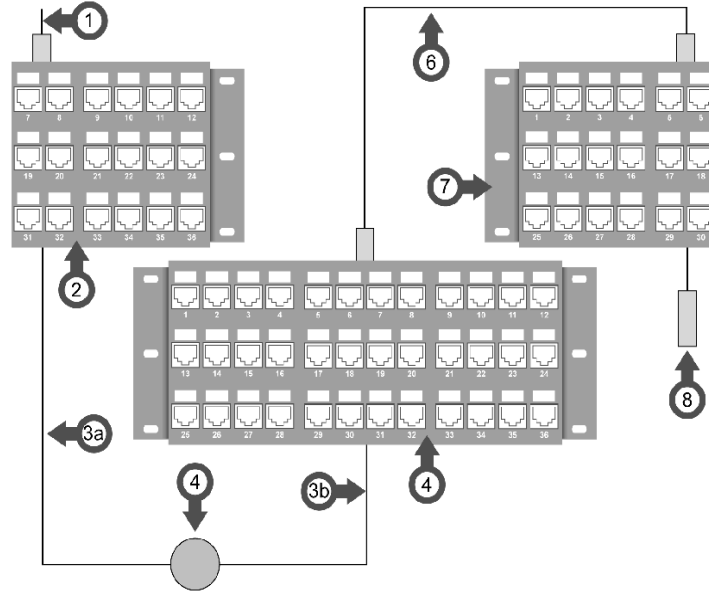


- 1 Terminal
- 2 Hôte
- 3 Câble à fibre optique
- 4 Convertisseur optoélectronique optionnel
- 5 Voie de câble équilibré

Les voies de câble à fibre optique et de câble équilibré sont connectées entre elles à l'aide d'un convertisseur de fibre optique en câble équilibré. Quatre interfaces de voie sont également prévues, deux aux extrémités de la voie en cuivre et deux aux extrémités de la voie à fibre optique. Les connexions des équipements ne font pas partie de la voie. Les cordons des zones de travail, les câbles des équipements et les câbles de raccordement sont inclus dans la voie.

Exemple 2

Le schéma ci-dessous illustre une voie de câble connectant une station de travail aux armoires de répartition (TC). Contrairement aux liaisons, les voies englobent le matériel de connexion, les câbles des équipements, les cordons des zones de travail et les câbles de raccordement. La voie de câble va du câble de raccordement (1) de la station de travail au câble de raccordement (8) situé à l'intérieur d'une armoire étendue. Elle connecte la zone de travail aux armoires sur un sous-système horizontal composé de deux câbles et d'un point de transition (TP).



- 1 Câble de raccordement
 - 2 Panneau de raccordement
 - 3a Câble horizontal
 - 3b Câble horizontal
 - 4 Point de transition
 - 5 Panneau de raccordement
 - 6 Câble de raccordement
 - 7 Panneau de raccordement
 - 8 Câble de raccordement
- 3a = 3b = 90 m max.
 1 + 6 + 8 = 10 m max.

Test d'une installation en cuivre

Introduction

Vous devez tester une installation en cuivre, afin de valider la conformité de l'installation et des performances obtenues par rapport à la norme ISO/CEI 11801. Pour mener à bien les tests d'installation et de performance des liaisons permanentes et des voies, Schneider Electric recommande l'utilisation des outils et des testeurs disponibles dans le commerce. Certains de ces outils sont décrits ci-dessous. Schneider Electric recommande l'utilisation d'outils appropriés pour la certification des installations de câblage en cuivre et des performances.

Exemple de testeurs

OMNIsScanner 2 et DSP-4000 sont deux modèles d'outils agréés. Ils sont tous les deux utilisés pour tester, certifier et documenter les réseaux à fibre optique et cuivre haute vitesse. Vous pouvez vous les procurer auprès de Fluke Networks.

Comparaison des testeurs

Le tableau suivant compare les fonctionnalités des deux testeurs. Etant donné qu'ils sont complémentaires, vous devez utiliser les deux testeurs pour mesurer et enregistrer les paramètres de spécification définis par la norme ISO/CEI 11801.

	DSP-4300	OMNIsScanner 1
Affichage des diagnostics en schéma	x	-
Affichage diaphonie vs longueur	x	-
Affichage NEXT vs longueur	-	x
Affichage des informations de phase NEXT	-	x
Affichage impédance vs longueur	x	-
Affichage perte par retour vs longueur	-	x
Inclusion des bandes S réussites/échecs	x	-
Sauvegarde des tracés dans le domaine temporel	x	-
Exportation des informations d'amplitude et de phase	-	x

2.7 Considérations supplémentaires pour la conception d'un réseau Ethernet industriel Transparent Ready

Vue d'ensemble

Ce sous-chapitre aborde certains sujets supplémentaires qu'il est important de prendre en compte lorsque vous intégrez des fonctionnalités Transparent Ready dans votre réseau.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Internet et technologies IP dans un environnement d'automatisation	133
Modèle Open System Interconnection (ou modèle pour l'interconnexion de systèmes ouverts)	135
Modèle TCP/IP	137
Modèle Transparent Ready	139
Adresses IP et classes	142
Remarques concernant la multidiffusion	147
Filtrage de multidiffusion	149
Gestion du réseau	151
Routage	153
Présentation de l'accès à distance	155
Types d'accès distant	157
Méthodes d'accès au réseau	159
Automate connecté à Internet	162
Problèmes de sécurité	164

Internet et technologies IP dans un environnement d'automatisation

Remarques relatives à la conception réseau

Transparent Ready propose une large gamme d'équipements et de stratégies vous permettant de développer une infrastructure réseau prenant en charge les communications dans votre usine. La transparence et la flexibilité d'un réseau Ethernet Transparent Ready passent par la prise de certaines décisions lors de la conception de votre système. Ces décisions portent sur les points suivants :

- Comment le réseau sera-t-il utilisé ?
- Quels services de communication devra-t-il prendre en charge ?
- Quels chemins empruntera-t-il ?
- Les exigences en termes de temps de réponse/débit
- Les exigences en termes de redondance et de résilience

Pourquoi utiliser Ethernet ?

Notre monde actuel relève un défi, l'agilité : non seulement l'agilité en termes de technologies mais aussi la volonté d'adopter et de peaufiner des approches collaboratives pour partager des données en temps réel. Votre réseau de communications doit être *ouvert* pour prendre en charge des services, des connexions physiques et des composants nouveaux. Du fait de l'énorme succès rencontré par le protocole Ethernet TCP/IP dans le monde commercial, ses technologies évoluent beaucoup plus vite que les réseaux propriétaires, entraînant plus de solutions de rechange et des composants plus abordables.

Une solution Ethernet standard vous permet de vous éloigner des systèmes propriétaires onéreux tout en conservant la sécurité, la performance et la disponibilité requises pour prendre en charge des applications critiques. Grâce à une planification et une conception adaptées, vous pouvez améliorer les processus, réduire les dépenses et améliorer la productivité.

Prise en charge des normes ouvertes

Dans le domaine commercial et de l'automatisation, Ethernet TCP/IP prend en charge tous les types de communications, y compris :

- les pages Web Internet ;
- le transfert de fichiers ;
- les messages industriels ;
- d'autres services fondés sur des normes.

A chaque tâche de communication correspond un service, une norme et une organisation de gestion. Chacun de ces services doit être exécuté sur la couche réseau la mieux appropriée.

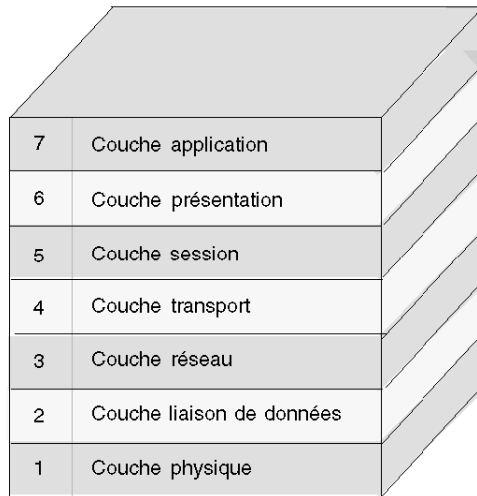
La liste suivante indique certains supports physiques et protocoles pris en charge par les normes TCP/IP ouvertes et les avantages qu'ils procurent aux environnements d'automatisation industriels :

- câbles en cuivre à paire torsadée pour une simplicité et un faible coût
- fibre optique pour l'immunité aux interférences sur de longues distances
- protocole IP pour la redondance des communications qui lui est propre
- radio et satellite pour surmonter les restrictions de câblage
- téléphone ou Internet pour un accès point à point distant à des coûts comparables à ceux des appels locaux
- composants d'infrastructure à bas coûts renforcés pour une utilisation en milieu industriel

Modèle Open System Interconnection (ou modèle pour l'interconnexion de systèmes ouverts)

Modèle OSI

Le modèle OSI définit un modèle à 7 couches pour les communications de données :



Les couches 1 ... 6 fournissent respectivement un ensemble de fonctions à la couche située au-dessus, et les couches 7 ... 2 reposent respectivement sur les fonctions fournies par la couche en dessous. Les messages peuvent traverser verticalement la pile en passant d'une couche à l'autre. Logiquement, chaque couche peut communiquer directement avec une couche homologue sur d'autres nœuds.

Les paragraphes suivants sont consacrés aux couches et aux fonctions du modèle OSI qui s'appliquent aux systèmes d'automatisation. Pour une description complète du modèle OSI, reportez-vous à la norme OSI 7498.

OSI et automatisation

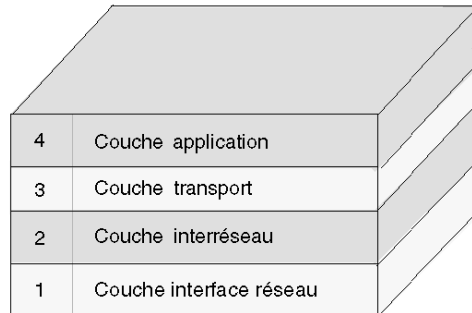
Lorsque le modèle OSI est appliqué à un environnement d'automatisation, des normes sont appliquées au niveau de chaque couche. Chaque couche peut remplir sa fonction (par exemple, la couche application Modbus transfère des données dans toute l'usine) sans rien savoir sur les couches situées en dessous. Vous pouvez adopter n'importe quelle norme appropriée pour chaque couche ; par exemple, sans fil ou câblé au niveau des couches inférieures et FTP pour le transfert de fichiers, ou Modbus pour le transfert de données au niveau des couches supérieures. Toute cette mise en place peut se réaliser sans modification des autres couches.

Ethernet est un système de transport de données physiques standard commun à tous les fournisseurs d'automates. Les protocoles d'application peuvent varier en fonction de l'environnement ; certains sont standard, d'autres spécifiques. Par exemple, FTP et HTTP sont standard et communs à tous les fournisseurs, tandis que Modbus et d'autres sont spécifiques à certains fournisseurs. Certains protocoles (Modbus, par exemple) sont des normes ouvertes ; d'autres ne sont disponibles qu'auprès d'un seul fournisseur.

Modèle TCP/IP

Récapitulatif

Le modèle TCP/IP a été développé en même temps que le modèle OSI (*voir page 135*) et est devenu le protocole choisi pour la plupart des réseaux de communication de données. Le modèle TCP/IP est constitué d'une pile de protocole à quatre couches qui est une version compressée du modèle OSI.



Cette pile de protocole n'a pas de mappage spécifique aux couches 5 et 6 du modèle OSI.

Couche application

La couche application exécute l'application et le protocole courants. Les applications communes sont Modbus, Ethernet IP, Profinet, Telnet, FTP, SMTP et Gopher. Les interfaces entre les couches application et transport sont définies par les numéros de port et les sockets. Le modèle TCP/IP peut exécuter simultanément différentes couches application, ce qui permet à un seul réseau d'automatisation de transporter un trafic SCADA (*voir page 300*), de la vidéo, des données, des données de programmation et des pages Web simultanément.

Couche transport

La couche transport fournit un transfert de données de bout en bout. Elle est responsable de la fiabilité de l'échange des informations. Il existe différents protocoles de couche transport, dont le principal est TCP. UDP est un autre protocole qui peut être exécuté dans la couche transport ; il est utilisé pour les applications qui nécessitent un mécanisme de transport rapide. Contrairement à TCP, UDP n'a pas la possibilité de scinder les longs messages et de rassembler leurs paquets dans l'ordre correct à l'autre extrémité, et est incapable d'envoyer de nouvelles tentatives. L'application qui envoie le message doit s'assurer que les messages sont envoyés dans leur intégralité ou, le cas échéant, retransmettre le message.

Couche interréseau

La couche interréseau sépare le réseau physique des couches situées au-dessus. IP est le protocole le plus important dans cette couche. IP est un protocole orienté données utilisé par les hôtes source et cible pour communiquer des données sur un réseau d'interconnexion à commutation de paquets. IP est un protocole en mode sans connexion qui ne prend pas en charge la fiabilité des couches inférieures. Il est parfois appelé *couche Internet* ou *couche réseau*.

IP ne fournit pas la régulation du flux ni la récupération après erreur. Ces fonctions doivent être fournies soit au niveau de la couche transport (si vous utilisez TCP), soit au niveau de la couche application (si vous utilisez UDP).

L'unité de message dans un réseau IP est appelée datagramme ou paquet IP. Un datagramme IP est transmis sur des réseaux TCP/IP. IP offre des fonctions de routage pour distribuer les datagrammes au destinataire correct pour la pile de protocole.

Les autres protocoles interréseau comprennent ICMP, IGMP, ARP et RARP. Ces protocoles ne remplacent pas IP, mais ils peuvent fonctionner à ses côtés.

Couche interface réseau

La couche interface réseau est l'interface vers le matériel courant. Elle est parfois appelée *couche liaison* ou *couche liaison de données*. Elle prend en charge des interfaces orientées paquets ou flux et ne garantit pas une livraison fiable.

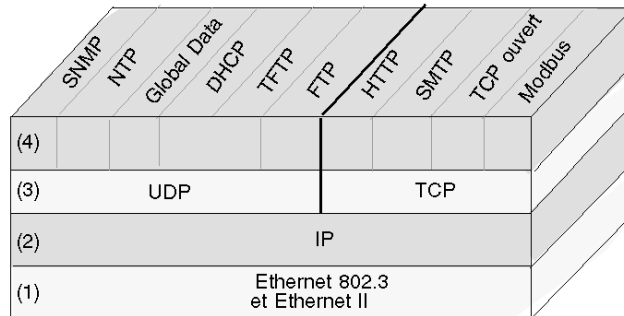
TCP/IP ne spécifie pas de protocole particulier pour cette couche. Il peut utiliser presque n'importe quelle interface réseau, ce qui en fait un réseau souple avec une compatibilité descendante pour une infrastructure héritée. IEEE 802.3, ATM et FDDI sont des exemples de protocoles d'interface réseau pris en charge par TCP/IP.

La capacité à exécuter la couche application et TCP/IP sur différentes couches physiques permet aux données (trafic SCADA, par exemple) de circuler sur une liaison par fibre optique vers des sites distants, puis sur une liaison en cuivre en étoile vers l'automate, voire une liaison par satellite. Tout ceci peut être fait sans modifier la couche application ni les couches TCP et IP pour l'adressage et la livraison de données.

Modèle Transparent Ready

Récapitulatif

Le diagramme suivant indique comment Transparent Ready met en œuvre le modèle TCP/IP (voir page 137) à quatre couches :



- 1 La couche interréseau est Ethernet 802.3 et Ethernet II.
- 2 La couche interface réseau est mise en œuvre avec IP.
- 3 La couche transport comprend UDP et TCP.
- 4 La couche application comprend 10 services Transparent Ready.

Ethernet II et IEEE 802.3

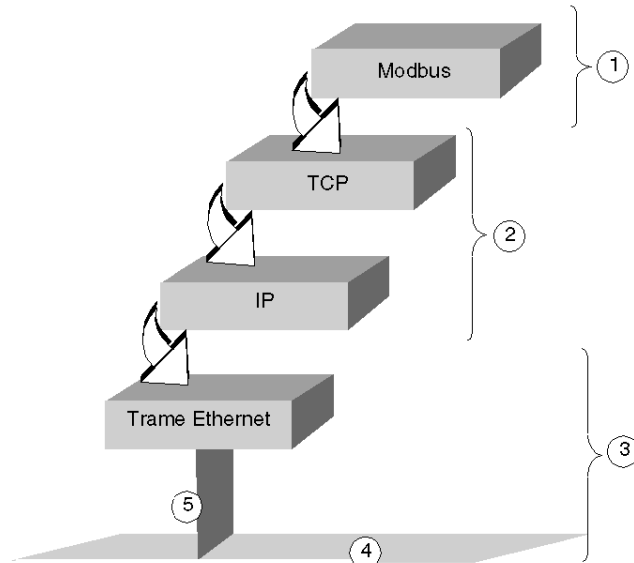
Ethernet II est le fruit d'un effort de développement conjoint de Xerox, Intel et Digital. Il a été lancé sur le marché en 1982. Un an plus tard, IEEE a sorti sa spécification 802.3. D'un point de vue fonctionnel, ils sont très semblables, mais la manière selon laquelle les deux formats définissent la trame de l'un des champs de données les rend mutuellement incompatibles.

Ethernet II et IEEE 802.3 se rapportent uniquement aux caractéristiques physiques du réseau :

- la manière dont les informations accèdent au réseau (CSMA/CD) ;
- la manière dont le réseau définit la trame des messages de données ;
- les caractéristiques physiques du réseau lui-même (sa topologie, le câblage requis, les connecteurs, l'infrastructure, etc.).

IEEE 802.3 et Ethernet II peuvent coexister sur le même câble physique et utiliser les mêmes signaux. La seule différence entre les deux tient au format des données.

Une trame de données peut être représentée comme un bloc dans lequel les informations voyagent le long du câble réseau :



- 1 Protocoles d'application
- 2 Protocoles Internet
- 3 Ethernet II ou IEEE 802.3
- 4 Topologie Ethernet
- 5 Accès au réseau (CSMA/CD)

Suite de protocoles Internet

Les professionnels du secteur de l'automatisation envisageaient initialement Ethernet comme une approche non déterministe d'un ensemble d'applications qui dépendaient largement de solutions en temps réel. La plupart des fournisseurs préférait se concentrer sur d'autres technologies, principalement propriétaires. Ce qui a finalement amené Ethernet à être adopté dans le secteur industriel est une combinaison de caractéristiques, appelée la suite de protocoles Internet.

Cette suite, connue sous le nom de TCP/IP, a été lancée sur le marché en 1983 en tant que méthode simple et fiable de communication à partir de plusieurs sites et avec des types de réseau différents. Le protocole TCP/IP est indépendant de la technologie réseau sous-jacente. Il peut être exécuté par-dessus Ethernet, IEEE 802.3, Token Ring, PPP, ATM, DSL et plusieurs autres technologies.

La suite regroupe beaucoup de protocoles, dont les plus connus sont TCP et IP. Parmi les autres éléments de la suite se trouvent :

- les protocoles de couche de liaison de données ARP et RARP ;
- les protocoles de transport tels que UDP ;
- les protocoles de gestion et d'informations tels que SNMP, DNS, BootP et NTP ;
- les protocoles de routage tels que EGP ;
- les protocoles d'application tels que FTP, TFTP, Telnet, SMTP et NFS.

Ces protocoles offrent différentes fonctions et se trouvent sur différentes couches du modèle.

Prise en charge du modèle pour les services Transparent Ready

Le modèle Transparent Ready prend en charge les services Ethernet universels tels que HTTP, BootP/DHCP et FTP. Il accepte également les services propres à Transparent Ready suivants :

- Messagerie TCP Modbus
- I/O Scanning
- FDR (Faulty Device Replacement - Remplacement d'équipements défectueux)
- Administration réseau SNMP
- Global Data
- Gestion de la bande passante
- Synchronisation horaire NTP
- Notification d'événements SMTP par message électronique
- TCP ouvert facultatif

Au niveau de la couche transport, UDP prend en charge six services et TCP, quatre :

Couche transport	Couche application	Service fourni
UDP	SNMP/MIB	Gestion de réseau
	NTP	Synchronisation horaire
	RTPS	Transfert de données globales
	DHCP	FDR (Faulty Device Replacement)
	TFTP	
TCP	FTP	
	HTTP	Serveur Web
	SMTP	Notification par message électronique
	TCP ouvert	
	Modbus	Gestion des messages
		Modbus I/O Scanning

Adresses IP et classes

Récapitulatif

Une adresse IP permet à un équipement d'avoir une adresse logique unique permettant de le localiser sur le réseau TCP/IP et de le regrouper avec d'autres équipements pour faciliter la conception et la gestion du réseau.

Notation décimale utilisant le point comme séparateur

Un ordinateur voit une adresse IP sous sa forme binaire de 32 bits. Pour plus de simplicité, ces 32 bits ont été divisés en quatre groupes de 8 bits. Chacun de ces groupes est converti en son équivalent décimal, soit quatre nombres décimaux séparés par des points. Par exemple, l'adresse IP binaire 10001011.00101101.00100100.00001100 peut être transcrite dans un format plus simple en convertissant chaque octet en une valeur décimale, soit 139.45.36.12.

10001011	00101101	00100100	00001100
139	45	36	12

Définition d'une adresse réseau

Une adresse IP comprend deux éléments : l'adresse du réseau et l'adresse de l'hôte ou de l'équipement. Le masque de sous-réseau est un filtre qui est appliqué à l'adresse IP pour déterminer la partie correspondant à l'adresse du réseau et celle correspondant à l'adresse de l'hôte ou de l'équipement. Dans une adresse IP, l'adresse du réseau identifie le sous-réseau auquel l'adresse appartient. Ce masque est une valeur de 32 bits qui utilise des bits 1 pour les parties consacrées au réseau et au sous-réseau, et des bits 0 pour la partie consacrée à l'hôte. Dans l'adressage avec classe, la partie de l'adresse IP correspondant à l'adresse du réseau comprend un, deux ou trois octets, en partant de la gauche.

Adresse IP	11000000	10100000	00010100	00110000	192.160.20.48
Masque de sous-réseau	11111111	11111111	11111111	00000000	255.255.255.0
Partie réseau de l'adresse IP	11000000	10100000	00010100	00000000	192.160.20.0

Adressage avec classe

Dans l'adressage avec classe, quatre classes d'adresses IP sont à votre disposition, selon la taille de votre entreprise :

- Classe A = 0.0.0.0/8 à 127.0.0.0/8
- Classe B = 128.0.0.0/16 à 191.255.0.0/16
- Classe C = 192.0.0.0/24 à 223.255.255.0/24
- La classe D = 224.0.0.0 à 239.255.255.255 est utilisée pour la multidiffusion (voir page 148).

Les adresses restantes regroupées sous l'appellation Classe E sont réservées à des fins d'expérimentation.

Une adresse comprend deux éléments :

- les informations sur le réseau,
- les informations sur l'hôte (le nœud ou l'équipement terminal).

L'adresse IP est constituée de quatre jeux de nombres décimaux, appelés octets, séparés par un point et dont la valeur comprise entre 0 et 255 représente un nombre binaire converti en nombre décimal.

Adressage sans classe

L'adressage sans classe (également appelé CIDR ou création de super réseaux) a été développé pour résoudre les problèmes actuels d'Internet concernant l'utilisation efficace de l'espace destiné aux adresses. Il permet également d'améliorer l'évolutivité du routage sur les réseaux. L'allocation d'un nombre important d'adresses à une entreprise en une seule fois a souvent entraîné le gaspillage de certaines adresses réservées. En incluant chaque réseau dans une table, on aboutissait à une surcharge. Par ailleurs, les PME correspondant à la classe B se sont multipliées jusqu'à utiliser en grande partie l'espace disponible dans cette classe. En flexibilisant le point de délimitation entre les informations du réseau et les informations de l'hôte, l'adressage sans classe a étendu le nombre d'adresses disponibles pour les entreprises de toutes tailles, tout en réduisant la taille des tables de routage.

Choix d'une plage d'adresses

Les adresses publiques, utilisables sur Internet, sont attribuées par une instance de régulation appelée IANA (Internet Assigned Numbers Authority). Toutefois, il se peut qu'une plage d'adresses ait déjà été attribuée à votre entreprise et que votre service informatique soit en mesure d'allouer toutes les adresses dont vous avez besoin. Si aucune plage d'adresses IP ne vous a été attribuée, sachez que l'IANA a réservé les trois blocs ci-dessous aux réseaux Internet privés :

10.0.0.0 à 10.255.255.255 (préfixe 10/8)

172.16.0.0 à 172.31.255.255 (préfixe 172.16/12)

192.168.0.0 à 192.168.255.255 (préfixe 192.168/16)

Adresses spéciales

Il existe trois types d'adresses spéciales :

- diffusion générale,
- boucle,
- réseau.

Un message de diffusion générale, habituellement utilisé pour les diagnostics et la gestion du réseau, est adressé à toutes les stations du réseau. L'adresse de destination d'un message de diffusion générale ne comprend que des 1 (255.255.255.255).

Une adresse de boucle permet de tester l'implémentation du protocole TCP/IP sur un hôte. Les couches inférieures sont court-circuitées par l'envoi du message à une adresse de boucle, ce qui permet de tester les couches supérieures (IP et au-dessus) sans détecter les problèmes au niveau des couches inférieures. 127.0.0.1 est l'adresse généralement utilisée pour effectuer des tests en boucle.

Comme expliqué dans la section précédente, l'adresse du réseau correspond à la partie réseau d'une adresse IP (Internet Protocol).

Adresses suffisantes

Lorsque vous planifiez votre réseau, vous devez anticiper le nombre d'adresses dont vous aurez besoin :

- pour la passerelle (une adresse),
- pour la diffusion générale,
- pour le nombre de services,
- pour les nouveaux équipements ajoutés au réseau.

Des outils sont disponibles sur Internet pour calculer le nombre d'adresses requis par votre réseau.

Création de sous-réseaux

La création de sous-réseaux divise un réseau important en segments plus facilement gérables, ce qui vous permet d'augmenter le nombre de réseaux, tout en n'utilisant qu'une seule adresse IP. Il est donc inutile de demander d'autres adresses IP.

Le trafic du réseau est réduit car les messages ne sont envoyés qu'à une partie limitée du réseau. La création de sous-réseaux révèle tout son intérêt dans un réseau gérant un volume important de trafic à diffusion générale. Elle est également très utile si la liaison WAN qui relie vos sites distants est lente.

Lors de la création d'un sous-réseau, le masque de sous-réseau par défaut est étendu aux bits d'adresse qui identifient normalement l'hôte. Dès lors que ces bits sont masqués, ils sont inclus dans la partie réseau et servent à identifier des sous-réseaux au sein du réseau.

Choisissez un sous-réseau de taille (nombre d'adresses) appropriée au nombre d'équipements, une taille qui autorise une certaine croissance sans pour autant gaspiller des adresses. Par exemple, si vous disposez de 50 équipements, choisissez un sous-réseau de 64 adresses, et non de 1 024. Le tableau ci-après contient une première colonne indiquant le nombre d'adresses et une seconde colonne indiquant le masque correspondant.

Masque de sous-réseau	Nombre d'adresses
0.0.0.0	4 294 964 086
128.0.0.0	2 147 482 048
192.0.0.0	1 073 741 024
224.0.0.0	536 870 512
240.0.0.0	268 435 256
248.0.0.0	134 217 628
252.0.0.0	67 108 864
254.0.0.0	33 554 432
255.0.0.0	16 777 216
255.128.0.0	8 388 608
255.192.0.0	4 194 304
255.224.0.0	2 097 152
255.240.0.0	1 048 576
255.248.0.0	524 288
255.252.0.0	262 144
255.254.0.0	131 072
255.255.0.0	65 536
255.255.128.0	32 768
255.255.192.0	16 384
255.255.224.0	8 192
255.255.240.0	4 096
255.255.248.0	2 048
255.255.252.0	1 024
255.255.254.0	512
255.255.255.0	256
255.255.255.128	128
255.255.255.192	64
255.255.255.224	32
255.255.255.240	16

Masque de sous-réseau	Nombre d'adresses
255.255.255.248	8
255.255.255.252	4
255.255.255.254	2
255.255.255.255	1

Pour un sous-réseau comportant 64 adresses, le masque de sous-réseau est 255.255.255.192. L'adresse IP serait donc 192.168.1.1, l'adresse réseau serait 192.168.0 et la plage d'hôtes irait de 0.1 à .63.

Utilisation de sous-réseaux dans une usine

En utilisant des sous-réseaux dans votre usine, vous divisez cette dernière en sections pour éviter toute surcharge de trafic. Utilisez un routeur pour acheminer le trafic entre les sous-réseaux. Un réseau ne doit pas comprendre plus de 200 à 300 équipements. Toutefois, il est préférable d'avoir un réseau plus petit, constitué de 50 à 100 équipements. Ajoutez des réseaux si vous devez prendre en charge un nombre d'équipements supérieur à celui recommandé.

Attribution d'adresses

Vous pouvez obtenir des adresses auprès de l'instance de régulation ou utiliser un sous-ensemble de celles qui vous ont déjà été attribuées. L'étape suivante consiste à attribuer une adresse unique à chaque équipement terminal à l'aide de l'une des méthodes proposées. Dans l'adressage statique, chaque utilisateur reçoit une adresse IP fixe qu'il doit utiliser chaque fois qu'il se connecte à Internet. Avec l'adressage dynamique, les adresses IP sont attribuées automatiquement selon les besoins. Le protocole BootP (Bootstrap Protocol) permet à un poste de travail de se configurer lui-même sans disque dur ni disquette. Le poste peut découvrir sa propre adresse IP, l'adresse IP d'un serveur et d'un fichier à charger en mémoire pour initialiser la machine. Le protocole DHCP attribue une adresse différente à un équipement lorsqu'il en demande une. Dans ce cas, c'est le logiciel et non l'administrateur (comme dans l'adressage statique) qui assure le suivi des adresses IP.

Remarques concernant la multidiffusion

Résumé

Méthode d'envoi sélectif de messages promue par un consortium de sociétés de premier plan, la multidiffusion IP est une nouvelle technologie qui va progressivement s'imposer pour :

- *la surveillance* : fabrication et autres types d'informations en temps réel, équipements de détection ou systèmes de sécurité.
- *les annonces* : temps réseau, planifications de sessions de multidiffusion, nombres aléatoires, clés, mises à jour de configuration, etc.
- *la distribution et la mise en cache des fichiers* : contenu de site Web, fichiers binaires exécutables
- *la distribution planifiée* de son et de vidéo
- *la distribution personnalisée d'informations* : titres de journaux, informations météorologiques, résultats sportifs, etc.

Sur Internet

Vous devez vous assurer que votre routeur et/ou vos commutateurs prennent en charge la multidiffusion, que vos postes de travail sont configurés pour se joindre à un groupe de multidiffusion et que vous avez installé les applications requises pour recevoir la multidiffusion.

Transport de la multidiffusion IP

Le protocole UDP est utilisé pour la multidiffusion IP. L'adresse de multidiffusion sélectionnée est importante car elle permet aux gestionnaires du réseau de contrôler la manière dont les hôtes (les équipements) deviennent membres de groupes, ainsi que le mode d'échange des informations de multidiffusion entre les routeurs.

Adresses de multidiffusion IP

Dans la multidiffusion IP, chaque groupe a son ID de groupe de multidiffusion et un jeu d'adresses IP de classe D permettant de spécifier la destination d'un message. Ces adresses sont comprises entre 224.0.0.0 et 239.255.255.255. Chaque adresse IP de multidiffusion peut être écoutée par plusieurs hôtes. Les hôtes peuvent appartenir à un groupe de multidiffusion auxquels les adresses IP sont associées. Chaque équipement configuré dispose d'une adresse IP de multidiffusion en plus de sa propre adresse IP.

Les adresses de classe D peuvent être catégorisées comme suit :

- *permanentes* : adresses comprises entre 224.0.0.0 et 224.0.0.255, attribuées de manière permanente par l'IANA à certaines applications comme les protocoles de routage. Par exemple :
 - 224.0.0.0 pour l'adresse de base ;
 - 224.0.0.1 pour tous les systèmes sur ce sous-réseau ;
 - 224.0.0.2 pour tous les routeurs sur ce sous-réseau ;
 - 224.0.0.4 pour les routeurs DVMRP.
- *non permanentes* : adresses comprises entre 224.0.1.0 et 238.255.255.255, utilisées pour les affectations sur Internet.
- *temporaires administrées* : adresses comprises entre 239.0.0.0 et 239.255.255.255, réservées pour les intranets privés.

Filtrage de multidiffusion

Récapitulatif

Vous pouvez utiliser deux services et une variation pour le filtrage de multidiffusion :

- IGMP
- Surveillance IGMP
- GMRP

IGMP

Le protocole IGMP est utilisé par un routeur pour établir l'appartenance à un groupe de multidiffusion et envoyer un message à un réseau comptant des membres de multidiffusion. Il interrompt la transmission du message lorsque le dernier destinataire d'un segment le reçoit. IGMP permet d'acheminer les messages de multidiffusion aussi bien sur Internet que sur un réseau local. Il fonctionne sur la couche 3, mais n'assure pas de filtrage au niveau du commutateur.

Surveillance IGMP

Cette méthode surveille passivement les informations d'enregistrement des paquets IGMP pour déterminer l'appartenance à des groupes. Ces informations permettent de compiler la liste des destinataires censés recevoir un message donné. IGMP effectue ce filtrage au niveau du commutateur en écoutant les messages des équipements et des routeurs, ainsi que le Querier IGMP. (Ce demandeur est normalement le routeur, mais si tel n'est pas le cas, un Querier IGMP est requis.)

GMRP

Le protocole GMRP permet de configurer dynamiquement les ports de commutation pour que le trafic de multidiffusion IP ne soit transmis qu'aux ports associés aux utilisateurs de la multidiffusion IP (hôtes). Un commutateur peut échanger des informations sur des groupes avec d'autres commutateurs, arrêter (ou *nettoyer*) le trafic de multidiffusion lorsque tous les destinataires abonnés ont reçu le message, ainsi que créer et gérer des groupes de multidiffusion. GMRP fonctionne sur la couche 2 avec des équipements de couche 2 comme les commutateurs Ethernet. Transparent Ready prend en charge GMRP.

Mappage d'adresses MAC à des adresses de classe D

Les cartes réseau échangent des informations en utilisant une adresse MAC unique et non une adresse IP. Pour vous joindre à un groupe de multidiffusion, vous devez exécuter une application sur un hôte qui va informer son pilote d'équipement réseau qu'il souhaite devenir membre de ce groupe. Le pilote d'équipement mappe l'adresse IP de multidiffusion à une adresse de multidiffusion physique.

Acquisition du statut de membre d'un groupe

Les appartenances aux groupes sont dynamiques. Les membres peuvent rejoindre et quitter un groupe lorsqu'ils le souhaitent. Les expéditeurs n'ont besoin que de l'adresse IP de multidiffusion pour envoyer les informations. Peu importe si des hôtes surveillent ou non les échanges à ce moment-là. Lorsqu'un hôte souhaite devenir membre d'un groupe de multidiffusion, il signale son intention au routeur situé sur le même sous-réseau.

Gestion du réseau

Récapitulatif

La gestion du réseau vous permet de contrôler :

- qui est sur le réseau,
- le trafic du réseau,
- les erreurs de trafic sur le réseau,
- les erreurs des équipements.

Composants de gestion du réseau

Pour gérer le réseau, vous devez utiliser un protocole qui autorise le système de gestion à communiquer avec des équipements et des terminaux, tels que des commutateurs et des routeurs, qui sont configurés pour prendre en charge ce protocole.

Protocole SNMP

SNMP est devenu le protocole standard pour la gestion des réseaux. Il comprend :

- un agent, le module logiciel de gestion du réseau, qui réside dans un équipement ;
- un gestionnaire (NMS) qui peut interroger les agents, en obtenir des réponses et définir des variables dans ces derniers ;
- un équipement contrôlé par une base MIB.

MIB

Un fichier MIB (Management Information Base) est une base de données contenant des objets contrôlés comme des messages de diffusion envoyés et reçus ou des paquets endommagés. Chaque instance d'un objet contrôlé est appelée variable MIB. La plupart des équipements prennent en charge MIB II avec certaines extensions pour les commutateurs.

Bases MIB privées

Une base MIB privée, installée en plus de la base MIB standard, est mise à disposition par un fournisseur pour ses produits. Schneider dispose de plusieurs bases MIB que vous devez charger dans un module pour gérer des équipements.

Installation d'un système de gestion de réseau

Pour installer un système de gestion de réseau, chargez le fichier MIB dans le gestionnaire. Le gestionnaire connaît les données et adresses requises pour *découvrir* les équipements sur le réseau. Il alimente les fichiers MIB et commence à surveiller le réseau.

Sécurité

Une chaîne de communauté, configurée sur un routeur ou un commutateur, est un mot de passe qui définit une communauté d'utilisateurs finaux qui ont accès aux informations SNMP sur un équipement réseau. Cette chaîne de communauté doit comprendre au moins 8 caractères alphanumériques. Ce type d'accès aux équipements est un gage de sécurité pour votre réseau.

Dans la version 3 de SNMP, la sécurité contrôle :

- la modification des informations ;
- l'usurpation d'identité ;
- la modification du flux de messages ;
- la divulgation d'informations.

SNMP version 3 offre un niveau de sécurité supérieur à celui des versions 1 et 2.

Effets sur le réseau

Lorsque vous installez un système de gestion de réseau, évaluez son impact sur la vitesse et la congestion du réseau. Si vous programmez le système pour qu'il assure une surveillance trop prégnante, vous risquez de surcharger le réseau. Une fréquence comprise entre 30 secondes et 1 minute est suffisante pour fournir des données intéressantes sans générer de trafic superflu.

Routage

Récapitulatif

Le routage est une méthode qui permet d'identifier l'itinéraire des messages d'un réseau à un autre. Internet utilise un processus dans lequel chaque nœud (routeur) consulte l'en-tête de chaque paquet, calcule le prochain *saut* sur le trajet jusqu'à la destination finale et transmet le paquet au nœud suivant qui répète le processus. Ce processus se déroule sur la couche 3.

Routeurs

Un routeur est un équipement qui relie plusieurs réseaux via une passerelle et transmet les paquets sur le réseau. Il est équipé d'une carte Ethernet ou d'une autre interface pour chaque réseau.

Processus de routage

Le message est analysé par l'équipement expéditeur. Si la destination est locale, le message est envoyé directement à l'équipement cible. Si la destination est située sur un autre réseau, le message est envoyé à la passerelle par défaut (le routeur local). Ce routeur utilise ses propres informations sur les réseaux connectés pour transmettre le message soit au réseau final (s'il est connecté directement), soit à un routeur plus proche de la destination finale.

Tables de routage

Une table de routage contient la liste des meilleurs itinéraires possibles pour atteindre un certain nombre de destinations réseau données. Elle regroupe les informations nécessaires à la définition de cette route : l'adresse IP de destination, l'adresse IP de la passerelle et l'identification de l'interface physique. Chaque routeur ne connaît que ses réseaux locaux, mais transmet ces informations à d'autres routeurs, ce qui permet de créer des tables. Il se peut que le routeur soit programmé pour ne connaître que le premier réseau connecté ou plusieurs réseaux en aval. S'il ne sait pas où envoyer un message, il le transmet à son routeur par défaut situé en amont sur le réseau, où le message sera traité. Les tables de routage sont créées manuellement sur un petit système ou automatiquement à l'aide de protocoles de routage.

Protocoles de routage

Les protocoles de routage décident du contenu des tables de routage. Dans un petit système stable, il est conseillé de programmer les tables de routage manuellement. Dans un système plus important qui requiert une certaine redondance, il vaut mieux choisir un protocole de routage.

Parmi les protocoles utilisés dans un système, citons RIP, un protocole de vecteur distance (le plus utilisé) et OSPF, un protocole de routage d'état de liaison (plus récent).

Un protocole de vecteur distance utilise la distance, mesurée en sauts de routage, pour déterminer l'itinéraire optimal d'un paquet. Chaque nœud partage sa table de routage avec les routeurs voisins. Dans un protocole de routage d'état de liaison, chaque nœud de commutation (routeur) reçoit une carte complète des connexions réseau, qui est transmise d'un nœud à l'autre. Le routeur utilise cette carte pour calculer le saut optimal suivant, en direction des destinations possibles sur le réseau.

Le protocole RIP est robuste, sa configuration est simple et son algorithme ne pénalise pas les capacités de calcul et de stockage. Toutefois, il présente plusieurs inconvénients : pas de prise en charge directe des sous-réseaux, bande passante importante requise, débogage compliqué, problèmes en cas de sauts nombreux sur un réseau important et faible sécurité.

Outre ses autres avantages, OSPF prend en charge les sous-réseaux, vérifie la liaison en envoyant un petit paquet et fonctionne bien sur les réseaux importants. En revanche, il consomme beaucoup de mémoire et de capacités de calcul, sans oublier sa relative complexité.

Pour choisir le protocole à utiliser, évaluez la capacité de votre système à gérer le nombre de routeurs, le temps de convergence (temps nécessaire pour créer les tables de routages après une modification) et le volume de trafic généré par le protocole lui-même.

Coût de chemin

Le coût du chemin, généralement basé sur des critères comme le nombre de sauts et la bande passante, permet de comparer le *coût* de transmission d'un paquet via différents itinéraires sur un réseau. Ce coût est défini pour chaque réseau et permet aux routeurs de choisir l'itinéraire optimal jusqu'à la destination finale. Plus cette valeur est faible, plus l'itinéraire est optimisé. Grâce à cette méthode, plus besoin d'envoyer des données en aveugle sur le réseau de routeurs.

Présentation de l'accès à distance

Récapitulatif

Dans une usine, l'accès au système de contrôle industriel est indispensable pour la capture des données, le dépannage, le contrôle et les ajustements mineurs. Les applications stratégiques et les processus industriels exigeant une attention de tous les instants, la capacité d'administration à distance des équipements réseau est de plus en plus recherchée. L'accès à distance est utile pour :

- les fabricants de matériels dont les machines peuvent être installées n'importe où dans le monde ;
- les utilisateurs finaux, qui n'ont pas d'équipe de support locale ;
- les intégrateurs de système qui cherchent à augmenter la valeur ajoutée de leur offre ;
- les systèmes qui requièrent la collecte de données à distance.

Exemples

Par exemple, une alarme signalant un réservoir trop rempli est envoyée à un opérateur. L'opérateur se connecte, vérifie l'état du réservoir, détermine s'il peut arrêter les pompes en toute sécurité et interrompt le processus jusqu'au lendemain matin pour analyser et corriger le problème.

Autre exemple, un fabricant de matériel expédie une machine à un client situé dans un autre pays. Le client choisit d'utiliser un autre type de capteur que celui spécifié par le fabricant. Mais, une fois démarré, le système ne fonctionne pas comme prévu. Avec l'accès à distance, le fabricant peut se connecter à l'usine, modifier le programme et réparer la machine du client tout en évitant un déplacement sur place coûteux à la fois en temps et financièrement.

Méthodes

Trois méthodes d'accès à distance sont fréquemment utilisées, chacune via un protocole différent :

- l'accès direct à un automate par un accès commuté ;
- le contrôle à distance d'un PC via un accès commuté ;
- l'accès à distance à la totalité du réseau.

Pour déterminer le type de connexion le plus approprié, vous devez définir la liste des fonctions que votre connexion à distance doit offrir. Les fonctions les plus répandues incluent :

- la collecte des données ;
- le dépannage à distance ;
- la programmation de logiciels ;
- SCADA ;
- la programmation à distance ;
- la sécurité.

Pour les réseaux privés d'entreprise, plusieurs points importants sont à prendre en compte s'agissant de l'accès à distance :

- la fiabilité ;
- les performances ;
- l'évolutivité ;
- la souplesse de gestion ;
- la connectivité sécurisée par le chiffrement et/ou l'authentification des utilisateurs et des équipements ;
- l'accessibilité.

Types d'accès distant

Accès commuté direct à l'équipement

L'accès commuté direct est géré par un modem relié directement à un automate d'usine ou un autre équipement. Un opérateur peut se connecter au modem et accéder au port de l'équipement comme dans une connexion locale. Pour accéder à un automate ou un équipement via Modbus, l'opérateur ne peut utiliser qu'un protocole série.

Contrôle à distance d'un PC via un accès commuté

L'accès commuté permet de prendre le contrôle à distance d'un PC sur site. En fait, l'opérateur distant utilise le PC sur site. Toutes les opérations effectuées à l'aide du clavier et de la souris distants sont envoyées au PC sur site, et l'affichage du PC sur site apparaît sur l'écran du PC distant.

Accès au réseau

L'accès au réseau implique l'extension du réseau Ethernet à une station distante. Vous pouvez établir cette connexion via un serveur à accès distant ou un VPN. La connexion Ethernet autorise un accès complet à tous les automates et autres équipements sur le réseau Ethernet du site. La station distante a accès aux pages Web, établit des diagnostics, effectue des tâches de programmation, se connecte à des imprimantes en réseau et consulte des documents hébergés sur des serveurs.

Connexion de l'automate à Internet

Lorsqu'une connexion est établie entre un automate et Internet, tout client connecté à Internet peut accéder à l'automate. Les clients distants ont accès aux pages Web, établissent des diagnostics, effectuent des tâches de programmation et exécutent de nombreuses autres fonctions.

Comparaison des options d'accès distant

Méthode	Systèmes accessibles	Accès au protocole de l'automate	Accès aux pages Web	Coût de la configuration	Coût continu	Difficulté de configuration	Exigences du client
Accès commuté direct à l'équipement	Un automate	Oui	Non	Bas	Frais de téléphone	Bas	Doit exécuter le logiciel automate/SCADA complet, etc.
Contrôle à distance d'un PC via un accès commuté	Tous les équipements	Oui	Oui	Bas	Frais de téléphone ou de connexion à Internet	Faible à élevée	Le logiciel de contrôle à distance doit être installé sur le PC local et le PC distant. Attention : dans ce cas, la sécurité peut être compromise.
Accès distant via un serveur à accès distant ou un VPN	Tous les équipements sur le réseau Ethernet local	Oui	Oui	Moyen	Frais de téléphone ou de connexion à Internet	Faible à élevée	Navigateur Web du logiciel automate/SCADA
Automate connecté à Internet	Tous les équipements ayant une connexion Internet	Oui	Oui	Moyen	Coûts du FAI (élevés)	Elevée	Navigateur Web du logiciel automate/SCADA

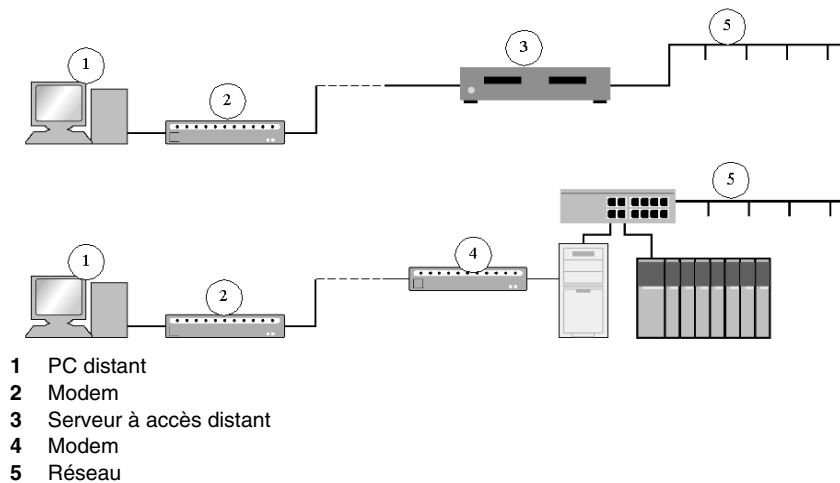
Méthodes d'accès au réseau

Récapitulatif

Le coût et le nombre d'utilisateurs à prendre en charge sont les deux principaux facteurs à considérer lors du choix d'une méthode d'accès à distance. Vous ne devez pas déployer de réseaux privés virtuels ou une technologie de sécurité sans mettre en place une politique (*voir page 164*) appropriée. Identifiez les données stratégiques sur votre réseau pour leur apporter la protection appropriée lors de leur transit sur Internet.

Serveur à accès distant

Deux structures de système à accès distant sont présentées ci-dessous, l'une avec un serveur à accès distant dédié et l'autre avec un PC serveur Windows.



Avantages du système avec serveur à accès distant

- Une nouvelle adresse IP globale n'est pas requise. L'adresse IP de l'automate peut être celle attribuée au réseau de l'entreprise.
- Aucun FAI n'est requis.
- La société qui utilise l'automate n'a aucun coût de maintenance.
- N'importe où dans le monde, vous pouvez fournir un système configuré qui devient opérationnel dès qu'une ligne téléphonique est connectée. (Vous devez avoir préalablement installé un modem compatible avec l'emplacement.)

Inconvénients du système avec serveur à accès distant

Une ligne téléphonique directe est requise entre le client distant et le serveur à accès distant. Les problèmes potentiels incluent :

- le coût ;
- la qualité médiocre de la liaison téléphonique ;
- la vitesse limitée.

Composants du système avec serveur à accès distant

- Vous devez ajouter un serveur à accès distant au réseau Ethernet connecté à l'automate.
- L'adresse IP de la passerelle par défaut de l'automate est celle du serveur à accès distant.
- Un modem est ajouté au serveur à accès distant. Un modem local de bonne qualité est recommandé.
- Les paramètres de sécurité et de pare-feu requis doivent être configurés sur le serveur à accès distant.
- Un modem est ajouté au client distant.
- Le client distant est configuré pour un accès commuté.

Mise en œuvre du serveur à accès distant

Que votre entreprise requière un serveur à accès distant dédié avec des fonctionnalités de sécurité et de pare-feu ou tout simplement un poste de travail ou un serveur Windows NT, prenez en compte les critères de système et de sécurité suivants lors de la conception de votre réseau :

- *Prise en charge des modems externes* : certains serveurs à accès distant ne prennent pas en charge les connexions par modem série.
- *Vérification de la sécurité* : notamment l'authentification Chap, PAP ou Windows. De nombreux systèmes offrent un niveau de sécurité supplémentaire avant que l'utilisateur puisse accéder à un réseau Windows. Si le réseau ne comprend aucun serveur Windows, le serveur à accès distant devient le principal point de vérification.
- *Rappel* : le serveur à accès distant et le modem peuvent être configurés pour rappeler un utilisateur à un numéro de téléphone préconfiguré. Cette fonctionnalité de sécurité requiert que quiconque tente d'accéder au système ait un numéro de téléphone donné. Le client appelle le serveur à accès distant et fournit un nom et un mot de passe. Ensuite, le serveur à accès distant raccroche et rappelle l'utilisateur à un numéro de téléphone prédéterminé. Si cette fonction offre un excellent niveau de sécurité, elle peut être extrêmement contraignante. Lorsqu'un fabricant de matériel livre un ordinateur de rappel à un client, c'est l'utilisateur final qui paie la majeure partie du coût des connexions du serveur à accès distant, car la liaison téléphonique est initiée par l'automate.

- *Protocoles autorisés* : de nombreux serveurs à accès distant peuvent être configurés pour n'autoriser que certains protocoles comme le trafic IP. Vérifiez que tous les protocoles dont vous avez besoin figurent dans la liste des protocoles autorisés.
- *Pare-feux* : certains serveurs à accès distant peuvent intégrer ou ajouter un pare-feu. Un pare-feu offre un environnement très sécurisé à l'automate et bloque la plupart des tentatives d'intrusion dans l'automate ou le réseau.

Réseau privé virtuel

Un réseau privé virtuel ou VPN crée des réseaux privés utilisant un mécanisme de transport comme Internet ou le réseau téléphonique public. Il achemine IP via un tunnel sécurisé créé entre deux réseaux. Le principe consiste à créer ce qui semble être une liaison privée dédiée sur un réseau partagé grâce à des techniques de chiffrement et de tunnel. La technologie VPN est une méthode économique qui offre une connexion sécurisée à des sites distants sur Internet. Vous pouvez utiliser des VPN site à site pour vous connecter à des locaux distants. Ce faisant, vous réduisez les dépenses liées au prix élevé des lignes louées. Les VPN sécurisent également la connexion à un réseau privé à partir d'une connexion Internet.

Environnements VPN communs

- *VPN à accès distant* : le cas le plus fréquent d'accès à distance est celui d'un utilisateur qui se connecte depuis un site distant (son domicile ou un hôtel en vacances, par exemple) à un réseau privé installé sur son lieu de travail. La meilleure méthode aujourd'hui consiste à utiliser un VPN, ce qui est à la fois plus rapide, plus économique, plus souple et plus pratique que les lignes privées ou louées.
- *VPN point à point* : la technologie VPN permet également de connecter des sites distants ou des succursales au réseau principal de l'entreprise. Les VPN remplacent ces technologies de réseau étendu (*voir page 70*) (WAN) comme les lignes louées, le relais de trame et ATM. Un VPN offre les fonctionnalités WAN traditionnelles, comme le transport de plusieurs protocoles, la haute disponibilité, l'évolutivité et la sécurité. Comme mentionné ci-avant, il offre également d'autres avantages par rapport aux services WAN privés.

Automate connecté à Internet

Récapitulatif

La connexion permanente d'un automate à Internet peut être coûteuse et difficile pour une petite entreprise ou un OEM. Toutefois, pour une grande entreprise possédant déjà une connexion permanente à Internet et familière avec le genre de questions telles que l'hébergement de ses propres serveurs Web, cette tâche constitue simplement une extension de son système existant.

Avantages et inconvénients de la connexion à Internet

Ce système présente plusieurs avantages par rapport à la configuration RAS précédente :

- L'automate est connecté en permanence à Internet. Cela permet un accès rapide à l'automate à partir de n'importe quel ordinateur connecté à Internet : aucun modem n'est requis.
- Aucun appel téléphonique longue distance n'est requis pour accéder à l'automate ; il vous suffit de vous connecter à votre FAI local.
- Le nombre de connexions à distance à l'ordinateur simultanées n'est pas limité par le nombre de modems sur le serveur RAS.

Cependant, il existe quelques inconvénients sérieux :

- Une connexion permanente à Internet est requise.
- Une adresse IP globale unique est requise pour l'automate. Celle-ci ne correspond pas forcément à l'adresse utilisée sur votre système local.
- Il n'existe aucun moyen simple de limiter l'accès à l'automate, contrairement à la solution de rappel pour serveur RAS, même si vous pouvez utiliser des pare-feux pour le contrôle d'accès.

Configuration générale du système Internet

La configuration générale du système est constituée comme suit :

- Vous devez trouver un FAI local afin d'avoir une connexion permanente de l'automate à Internet. Cela peut s'avérer très cher car la plupart des connexions permanentes utilisent des méthodes autres que le modem. Si vous prévoyez d'utiliser un modem, consultez votre FAI et votre opérateur téléphonique pour voir si une connexion téléphonique peut rester active indéfiniment.
- Obtenez une adresse IP unique permanente pour votre automate. Pour les petites entreprises, vous pouvez obtenir cette adresse auprès de votre FAI. La location de cette adresse auprès de votre FAI peut être chère car il existe un nombre limité d'adresses de la sorte dans le monde. De plus votre FAI peut louer une adresse à un utilisateur unique ou la partager avec de nombreux utilisateurs. Les entreprises plus grandes doivent déjà avoir une série d'adresses IP uniques permanentes.
- Faites configurer par votre FAI ou votre personnel informatique tous les routeurs requis pour accéder à cette adresse IP à partir du reste d'Internet. Configurez en outre l'adresse IP et la passerelle de l'automate.
- Un pare-feu (*voir page 165*) doit être installé pour séparer la partie du réseau connectant votre automate à Internet du reste de votre réseau. Cela permet d'éviter que les utilisateurs accèdent à d'autres parties de votre réseau. Vous pouvez également installer un pare-feu entre l'automate et Internet pour limiter le type d'accès que les utilisateurs peuvent avoir à l'automate. Actuellement, aucun pare-feu n'autorise les commandes de données Modbus (lecture/écriture de données) tout en empêchant les commandes de programmation (programmation de l'automate à l'aide de Concept, Proworx ou Modsoft).

Si vous prévoyez de connecter votre automate en permanence à Internet, Schneider Electric vous recommande de travailler en étroite collaboration avec votre service informatique ou, si possible, en partenariat avec un FAI local fiable.

Problèmes de sécurité

Récapitulatif

La sécurité d'un réseau peut être envisagée sous différents aspects : l'autorisation quotidienne d'un opérateur à accéder à un automate, le blocage des activités pénalisantes mais pas malveillantes, et l'application des autorisations et procédures de l'usine. Toutefois, le blocage des activités malveillantes est bien plus difficile à mettre en œuvre que les autres aspects. Parmi ces activités, citons les intrusions, l'interférence avec les données de l'entreprise, les attaques virales, les refus de service, le détournement de sites Web et de messagerie, la fraude et toute autre activité criminelle. La protection de votre réseau contre ces malveillances est particulièrement difficile à assurer et requiert les conseils d'experts en la matière. Le délai nécessaire pour sécuriser le réseau contre ces brèches varie selon les compétences des pirates, mais la sécurité implique une surveillance constante. En revanche, la protection contre les activités non malveillantes peut être assurée par du personnel qui ne possède pas ce niveau de spécialisation.

Politique de sécurité

Votre politique de sécurité définit les informations et services accessibles, leur mode d'accessibilité et les personnes autorisées à y accéder. C'est en définissant une politique de sécurité, et non simplement en en appliquant une sans plan, que vous prendrez en compte tous ces aspects. La planification permet de mieux déterminer les mesures de sécurité à appliquer lorsque vous modifiez votre réseau.

Mots de passe

Les mots de passe doivent être modifiés tous les mois. Pour éviter toute intrusion malveillante, choisissez des noms d'utilisateur et des mots de passe complexes. Il est impératif de modifier ou de désactiver les mots de passe par défaut de tous les équipements, car ces informations sont faciles à trouver dans les documentations utilisateur.

Accès physique

Empêcher l'accès physique au réseau est primordial pour assurer une sécurité efficace contre les attaques malveillantes. Il est très facile d'obtenir les mots de passe SNMP ou telnet si vous avez accès physiquement au réseau. Ainsi, la protection contre l'accès physique à l'infrastructure du réseau est cruciale pour assurer le contrôle de la structure du réseau. Tout le travail d'organisation du trafic du réseau peut être perdu si des utilisateurs rendent les réseau inexploitable ou bloquent les communications entre les équipements.

Pare-feux

Un pare-feu est un équipement ou un programme qui filtre les informations qui pénètrent dans votre réseau via une connexion. Il analyse chaque paquet et décide s'il est autorisé à pénétrer dans le réseau, en fonction de :

- l'adresse IP source ;
- l'adresse IP cible ;
- le numéro de port TCP cible (le protocole utilisé).

Placez des pare-feux aux jonctions stratégiques de votre réseau, comme :

- entre le réseau de l'entreprise et l'étage de l'usine ;
- entre différentes zones de l'usine ;
- entre les portables des sous-traitants et l'usine.

Avec des pare-feux de base, vous limitez l'accès à une zone de votre réseau ou à un équipement donné, selon les informations provenant de l'ordinateur qui tente d'accéder à la ressource concernée. Comme l'accès se fait par IP, il est impossible d'effectuer un filtrage par personne. Vous pouvez autoriser l'accès à un équipement, mais limiter les protocoles utilisables. Par exemple, vous pouvez autoriser l'affichage de pages Web, mais pas le transfert de microprogrammes par FTP.

Filtrage Modbus et pare-feux

Le filtrage Modbus ne permet pas d'autoriser la surveillance des données sans autoriser la programmation, car ces deux aspects sont gérés par le même protocole. L'une des solutions possibles consiste à autoriser plusieurs services OPC à accéder aux données et à bloquer tous les autres équipements. Ceci empêche également la surveillance avec un module de programmation.

Pare-feux avancés

De plus en plus de pare-feux avancés analysent les couches supérieures des paquets Ethernet et déterminent s'ils sont autorisés à pénétrer dans le réseau. Ceci permet non seulement de filtrer la couche des applications, mais signifie également que ces pare-feux n'autorisent pas les commandes de programmation Modbus. Plus lents que leurs homologues ordinateurs, ces pare-feux ne sont pas encore très répandus.

Configuration d'un pare-feu

La méthode utilisée pour configurer un pare-feu est importante. Il en existe deux :

- tout autoriser puis rejeter des éléments spécifiques ;
- tout rejeter puis autoriser des éléments spécifiques.

La méthode *tout rejeter* est la plus sécurisante, car elle prend en compte les cas auxquels vous n'aviez pas pensé. Il s'agit donc de la méthode recommandée.

Listes de contrôle d'accès

Une liste de contrôle d'accès est utilisée dans les commutateurs de couche 3 (*voir page 68*) et dans certains commutateurs de couche 2. Elle assure un service de filtrage similaire à celui d'un pare-feu, mais elle s'appuie sur un port source/cible ou un VLAN (*voir page 64*), au lieu d'une adresse IP. Vous pouvez l'utiliser sur les niveaux inférieurs d'un réseau (à l'étage de l'usine) pour empêcher une zone d'accéder à une autre. Dès qu'une liste de contrôle d'accès est configurée, le système bloque tous les types d'accès, comme une personne qui tente accidentellement de se connecter à un automate situé dans la zone suivante de l'usine. La méthode de configuration est la même que pour un pare-feu.

Sécurité des ports

L'équipement Schneider NxS272 protège chaque port. La sécurité des ports fonctionne de manière similaire à une liste de contrôle d'accès, mais limite les connexions entrantes selon leur adresse MAC. Les paramètres identifient les utilisateurs autorisés : toutes les adresses ou uniquement une. Si une adresse non autorisée est détectée, les paramètres déterminent la réponse : aucune, interception ou désactivation. Les paramètres sont définis avec l'adresse Web.

Contrôle d'accès à l'automate

Les ports Ethernet des automates Quantum/Premium et de la passerelle ETG prennent en charge les listes de contrôle d'accès pour la messagerie Modbus. Ils vous permettent de configurer les adresses IP autorisées à envoyer des requêtes Modbus à l'automate. En revanche, ils interdisent l'accès à d'autres protocoles. Soyez prudent lorsque vous configurez le contrôle d'accès car il restreint le fonctionnement des pages Web actives qui utilisent Modbus pour récupérer des données.

Problèmes de sécurité avec le sans fil

Les réseaux sans fil souffrent d'un déficit important en terme de sécurité par rapport aux réseaux traditionnels. Comme un réseau sans fil transmet les données sur des ondes radio, ces dernières sont plus facilement accessibles.

Ces options pour systèmes sans fil existent dans les systèmes d'automatisation :

- systèmes sans fil traditionnels pour réseaux série, Modbus Plus et solutions Ethernet personnalisées ;
- Ethernet sans fil basé sur des normes de bureau.

Les systèmes basés sur une solution sans fil non standard sont plus difficiles à intercepter car ils n'utilisent pas les protocoles standard. Cependant, les systèmes qui utilisent une technologie sans fil standard peuvent être interceptés par n'importe quel ordinateur portable équipé d'une connexion sans fil, ce qui les expose encore plus.

Chaque réseau sans fil reçoit un SSID ou nom de réseau qui l'identifie. Normalement, le SSID choisi est un nom logique. N'optez pas pour un nom logique comme le fournisseur du matériel ou le nom de votre entreprise. Il fournit des informations sur votre réseau.

Points d'accès

Un point d'accès (logiciel ou équipement) représente le concentrateur de connexion pour un équipement sans fil connecté à un réseau local câblé. Les points d'accès ont un SSID de diffusion. S'il est activé, le nom du réseau est diffusé et il est proposé aux ordinateurs qui tentent de se connecter. Désactivez la diffusion. Elle requiert une préconfiguration du SSID sur tous les ordinateurs pour qu'ils puissent se connecter au réseau. En majorité, les réseaux sans fil utilisent un serveur DHCP pour attribuer des adresses IP aux clients. Configurez le serveur pour qu'il attribue des adresses IP à certaines adresses Modbus Plus. Ne configurez aucune adresse de rechange supplémentaire. Limitez l'accès aux adresses MAC connues. Les points d'accès peuvent être configurés pour n'autoriser que la connexion des adresses IP et MAC connues. Sur la plupart des PC, et notamment les portables, vous pouvez modifier l'adresse MAC et utiliser celle existant sur le réseau.

WEP

WEP (Wired Equivalent Privacy) sécurise le réseau en cryptant les données transmises par les ondes radio. Activez ce paramètre. Choisissez une clé WEP qui vous autorise à surveiller le réseau. Générez systématiquement une clé WEP aléatoire et n'utilisez jamais de clé basée sur un mot. Les algorithmes de génération de clés à partir d'un mot sont connus et certains programmes sont capables de les déchiffrer. Par conséquent, bannissez les clés WEP générées à partir d'un mot. Il suffit de 3 heures à quelques jours à un pirate pour la décrypter.

VPN et pare-feu

La combinaison d'un VPN et d'un pare-feu est une solution idéale, mais coûteuse en termes de temps de gestion. Exécutez un client VPN sur les ordinateurs portables et un terminal de VPN à la jonction entre le réseau sans fil et le réseau principal. Ceci ajoute un cryptage supplémentaire (supérieur au cryptage WEP) aux données transmises. Exécutez un pare-feu entre le terminal du VPN et le reste du réseau pour sécuriser l'accès encore davantage.

Vue d'ensemble des services

3

Vue d'ensemble

Ce chapitre fournit les informations permettant de sélectionner le service Transparent Ready approprié pour chaque tâche de votre système automate. Vous y trouverez des informations concernant les avantages et les limites de chaque service, ainsi que sur le fonctionnement des périphériques qui l'utilisent.

NOTE : Les données de performances de Unity utilisées dans ce chapitre sont basées sur la version 2.0 du logiciel. Les autres versions de Unity peuvent être sensiblement différentes.

Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
3.1	Evaluation de la configuration du système	170
3.2	Service I/O Scanning	183
3.3	Messagerie Modbus	197
3.4	Service Global Data	217
3.5	Remplacement d'équipements défectueux	225
3.6	Synchronisation horaire	230
3.7	Service de notification par message électronique	239
3.8	Serveur Web standard	245
3.9	Serveur Web FactoryCast	253
3.10	Serveur Web FactoryCast HMI	259
3.11	Autres services	266
3.12	OPC Factory Server	280
3.13	SCADA/IHM	300
3.14	Redondance	314
3.15	Systèmes de passerelle/pont	335
3.16	Services pris en charge par équipement	344
3.17	Evaluation des performances système	352

3.1 Evaluation de la configuration du système

Vue d'ensemble

Cette section présente les services Transparent Ready, qui prennent en charge les communications Ethernet à chaque niveau de l'usine. Elle décrit également comment évaluer la configuration de vos communications et sélectionner les services les plus appropriés.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Services communs à chaque niveau de l'usine	171
Communication au niveau de l'entreprise	172
Niveau inter-automates	173
Communications au niveau du terrain	174
Sélection du service de communication	175
Services et protocoles de prise en charge de Transparent Ready	178

Services communs à chaque niveau de l'usine

Récapitulatif

Il est possible d'intégrer des produits industriels Transparent Ready aux architectures basées sur le réseau universel Ethernet TCP/IP. Aucune interface supplémentaire n'est nécessaire. L'architecture de base ci-dessous montre les différents niveaux et fonctions de communication requis par les applications industrielles pour satisfaire les exigences en matière d'échange de données dans une usine :

Les communications peuvent s'effectuer à quatre niveaux :

- Communication au niveau de l'entreprise (*voir page 172*) : entre les systèmes de commande et le système MES (système d'exécution de la fabrication) ou les systèmes de supervision ou d'information ERP (progiciel de gestion intégré)
- Communication au niveau inter automates (*voir page 173*) : pour la programmation, le diagnostic et le transfert de données ainsi que la communication entre les automates pour synchroniser les applications
- Communication au niveau du terrain (*voir page 174*) : entre les automates, les PC et les équipements terrain
- Communication distante transparente : communication distante via Internet, le téléphone ou une liaison radio

Communication au niveau de l'entreprise

Systèmes MSE/ERP et automates

Les communications au niveau de l'entreprise utilisent des infrastructures et des protocoles standard pour échanger des volumes élevés de données avec des systèmes de gestion de projet. Dans certains cas, l'automate doit s'adapter à un protocole spécifique au système connecté. Les temps de réponse ne sont pas critiques. Les services Transparent Ready utilisés sont les suivants :

- communication HTTP pour afficher les données et envoyer des commandes via des pages Web
- échange de données utilisant la norme OPC via un serveur de données OFS (*voir page 280*)
- messagerie Modbus TCP/IP (*voir page 197*)
- TCP ouvert
- émission de messages électroniques (*voir page 239*)
- publication directe dans des bases de données relationnelles via le serveur Web FactoryCast HMI actif (*voir page 259*)

Systèmes de supervision et automates

Les communications au niveau de l'entreprise peuvent transférer des volumes élevés de données d'un système de l'entreprise vers un groupe d'automates. Les temps de réponse doivent généralement se situer entre 0,5 et 2 s. Les services Transparent Ready utilisés sont les suivants :

- échanges de données utilisant la norme OPC via un serveur de données OFS (*voir page 280*)
- messagerie Modbus TCP/IP (*voir page 197*)
- TCP ouvert
- communication HTTP, intégrée au système de supervision pour afficher les pages Web à partir des équipements terrain dans les pages de supervision

Applications IHM et automates/équipements terrain

Une application IHM de base doit avertir le personnel de maintenance d'un événement et lui permettre de consulter l'état d'un équipement terrain. Les services Transparent Ready utilisés sont les suivants :

- notification par message électronique
- commandes d'affichage et de transmission des données via des pages Web

SNMP

Le protocole de gestion de réseau standard (SNMP) peut être utilisé par une station de gestion du réseau pour surveiller, contrôler et effectuer le diagnostic de tous les composants de l'architecture Ethernet (*voir page 269*).

Niveau inter-automates

Communication de transfert de données

Lorsque des données sont envoyées via le mode point à point selon des algorithmes de programmation d'automate et que les temps de réponse se situent entre 200 ms et 1 s, le principal service Transparent Ready à utiliser est la messagerie Modbus TCP/IP (*voir page 197*).

Synchronisation des applications

La communication de diffusion utilise des échanges en temps réel pour synchroniser plusieurs applications. Les volumes des données échangées sont faibles. Des temps de réponse situés entre 10 et 500 ms sont nécessaires. Le service Global Data (*voir page 217*) Transparent Ready est particulièrement adapté aux échanges synchronisés de données.

Communications au niveau du terrain

Communication entre les PC et le terminal opérateur sur le terrain

Les communications au niveau du terrain sont utilisées pour configurer, surveiller et gérer les équipements terrain pour les diagnostics et la surveillance. Les procédures de communication doivent être simples afin que le personnel moins qualifié puisse accéder aux diagnostics de premier niveau à partir d'un PC standard.

Le service Transparent Ready le plus adapté est l'affichage de diagnostics et de pages Web (*voir page 245*) personnalisées.

Le protocole Modbus et/ou d'autres protocoles industriels de bus terrain sont utilisés pour contrôler les équipements terrain.

Sélection du service de communication

Récapitulatif

La description suivante des services (ainsi que les tableaux des services présentés dans la rubrique suivante) peut vous aider à décider quels sont les meilleurs services pour votre application.

I/O Scanning

Le service I/O Scanning vous permet d'échanger des informations de façon répétitive entre un équipement central et un grand nombre d'équipements distants sans recourir à une programmation spéciale dans ces équipements.

Il s'utilise lorsque vous voulez échanger des données de façon répétitive et rapide (à une fréquence comprise entre 1 ms et 5 s). L'exemple type d'un équipement pouvant utiliser le service I/O Scanning est un lecteur de code barres devant scanner toutes les étiquettes de paquets circulant sur un convoyeur rapide.

Pour plus de détails, reportez-vous à la section *Service I/O Scanning, page 183*.

Messagerie Modbus

Le service de messagerie Modbus comprend des services client et serveur. Le client lance une requête vers le serveur via le protocole Modbus ; le serveur répond à la requête du client, ce qui se traduit par un échange d'informations. La messagerie Modbus prend en charge la lecture et l'écriture des données, ainsi qu'un ensemble de commandes de programmation.

La messagerie Modbus doit être utilisée lorsque des données doivent être échangées entre deux équipements selon des intervalles irréguliers ou peu fréquents. Il peut s'agir d'une commande visant à démarrer un processus ou à générer un rapport une fois le processus terminé. La messagerie Modbus permet d'établir des communications uniquement lorsqu'elles sont nécessaires, ce qui optimise l'utilisation du réseau et des équipements.

Pour plus de détails, reportez-vous à la section *Messagerie Modbus, page 197*.

Global Data

Le service Global Data permet à un équipement de publier des données vers un groupe d'équipements du réseau. Il est possible de configurer les équipements de ce groupe de distribution afin qu'ils souscrivent aux données publiées.

Le service Global Data doit être utilisé lorsqu'un équipement contient des informations d'état que plusieurs équipements du réseau doivent recevoir. L'équipement de publication utilise la multidiffusion pour envoyer efficacement des informations sur le réseau à son groupe de distribution.

Pour plus de détails, reportez-vous à la section *Service Global Data, page 217*.

FDR (Faulty Device Replacement, Remplacement d'équipements défectueux)

Le service FDR permet à un équipement central (le serveur FDR) de stocker les paramètres de configuration des équipements distants sur le réseau. En cas de panne d'un équipement distant, le serveur transmet automatiquement ses paramètres de configuration stockés à un équipement de remplacement afin que ce dernier puisse fonctionner avec la même configuration que celle de l'équipement défectueux. Le remplacement s'effectue sans configuration manuelle des paramètres.

Le service FDR doit être utilisé pour tous les équipements qui sont connectés à un réseau d'automatisme. Avec le service FDR, le personnel d'entretien n'a plus besoin de conserver les enregistrements de configuration à portée de main et le risque d'erreur humaine au moment de la saisie de la nouvelle configuration est réduit.

Pour plus de détails, reportez-vous à la section *Remplacement d'équipements défectueux*, page 225.

Synchronisation horaire

Le service de synchronisation horaire permet de proposer une source horaire centrale à plusieurs équipements du réseau. Lorsque tous les équipements ont une heure précise, vous pouvez synchroniser correctement les événements et gérer l'ordre des opérations dans l'usine.

Le service de synchronisation horaire doit être utilisé dans les environnements dans lesquels la synchronisation joue un rôle important dans les opérations. Il évite d'avoir à configurer manuellement l'heure sur chaque équipement du réseau. En outre, la précision peut approcher 1 ms dans tous les équipements, un niveau de précision qu'il est impossible d'obtenir en configurant l'heure manuellement.

Pour plus de détails, reportez-vous à la section *Synchronisation horaire*, page 230.

Notification par message électronique

Le service de notification par message électronique permet au personnel d'entretien d'être notifié de l'état de l'usine via un message électronique. Ce dernier peut inclure des données de traitement, des rapports de production, des alarmes, des événements et d'autres informations nécessaires pour évaluer l'état de l'usine. Un équipement qui propose le service de notification par message électronique peut créer automatiquement de courts messages électroniques. En outre, il est possible d'associer à ces messages des destinataires, des adresses électroniques et des objets prédéfinis. Le corps du message peut être modifié de façon dynamique pour inclure les données actuelles de l'usine ainsi que d'autres textes.

Le service de notification par message électronique est utilisé chaque fois que la notification par message électronique constitue une option pratique de communication pour informer quelqu'un de l'état de l'usine, des rapports d'exploitation ou des besoins de maintenance. Dans ce cas, vous êtes averti des besoins de maintenance, ce qui évite de vérifier régulièrement l'équipement pour savoir quand il doit subir des opérations de maintenance. Du fait des retards potentiels, ce service n'est pas recommandé pour les messages urgents qui nécessitent des temps de réponse courts et une intervention rapide.

Pour plus de détails, reportez-vous à la section *Service de notification par message électronique*, page 239.

Diagnostics intégrés (services Web standard)

Les diagnostics intégrés permettent d'exécuter des fonctions de diagnostic et de maintenance localement et à distance à l'aide d'un simple navigateur Internet. Ce service utilise un serveur Web intégré et un serveur de données en temps réel. Toutes les données sont présentées au format HTML (format Web standard) et sont accessibles via n'importe quel navigateur Internet.

Ce service est très utile pour surveiller l'état des équipements du réseau et les informations relatives au fonctionnement et à la configuration. Certains automates prennent en charge la configuration à distance via des pages Web. Par exemple, les variateurs Altivar donnent accès aux informations de vitesse courantes et vous permettent de configurer les taux d'accélération par l'intermédiaire de leur site Web.

Pour plus de détails, reportez-vous à la section *Serveur Web standard*, page 245.

Web/FactoryCast

A l'aide d'un simple navigateur Internet, le serveur Web FactoryCast offre tous les avantages d'un service de serveur Web intégré standard avec la possibilité de contrôler, configurer et surveiller les données de l'usine localement et à distance. La surveillance et le contrôle peuvent être améliorés à l'aide de pages Web personnalisées par l'utilisateur.

Le service Web/FactoryCast permet d'afficher et de modifier toutes les variables de l'usine en temps réel. Il vous permet de créer des liens hypertexte vers des serveurs Web externes pouvant contenir la documentation de l'usine. Le service Web FactoryCast HMI incorpore un serveur Web actif dans l'équipement, fournit des pages Web de meilleure qualité, prend en charge davantage de clients et assure la connectivité de la base de données.

Pour plus de détails, reportez-vous à la section *Serveur Web FactoryCast*, page 253.

Services et protocoles de prise en charge de Transparent Ready

SNMP

Le service SNMP permet de gérer les réseaux. Il s'agit d'un système de gestion réseau qui utilise les équipements compatibles SNMP recevant des demandes d'informations sur eux-mêmes et sur le réseau. SNMP est présent dans presque tous les équipements Ethernet et doit être utilisé comme la base dans la plupart des systèmes de gestion réseau. Il permet de découvrir, surveiller et configurer les équipements d'un réseau. Généralement, SNMP est utilisé pour transférer l'état d'un équipement et d'un réseau et non l'état de l'usine.

Pour plus de détails, reportez-vous à la rubrique *Service SNMP, page 269*.

FTP

FTP est une méthode d'échange de fichiers entre les équipements d'un réseau. Presque tous les systèmes d'exploitation intègrent aujourd'hui une fonctionnalité client ou serveur FTP, ce qui facilite les transferts de fichiers d'un équipement à l'autre. Beaucoup d'équipements réseau mettent en œuvre le protocole FTP comme méthode standard de transfert d'informations pour mettre à jour son logiciel ou micrologiciel interne.

Pour plus de détails, reportez-vous à la rubrique *Service FTP, page 267*.

TFTP

TFTP est un protocole de transfert de fichiers plus simple que FTP, généralement utilisé pour le transfert de petits fichiers sur des équipements moins complexes.

Pour plus de détails, reportez-vous à la rubrique *Service TFTP, page 271*.

Telnet

Le protocole Telnet fournit une session de communication de type client-hôte interactif, dans laquelle vous pouvez saisir des commandes pour consulter et manipuler un équipement distant. Il s'agit d'une interface utilisateur basée sur du texte et intégrée à de nombreux équipements aujourd'hui. Vous pouvez utiliser Telnet pour configurer des équipements simples tels que des commutateurs, des routeurs et des ponts série-Ethernet.

Pour plus de détails, reportez-vous à la rubrique *Service Telnet, page 272*.

Services de transfert des données d'usine

Service	Niveau, utilisation courante	Temps de réponse	Fréquence de transfert de données	Confirmation d'échange	Exemples	Topologie des communications
I/O Scanning	Equipement terrain et automate à automate Niveaux 2 et 3	10 ms+	1 ms à 5 s périodique	Etat de santé du scrutateur d'E/S pour le transfert des données et les valeurs de repli. Accusé de réception pour chaque transfert de données avec mécanisme de nouvelles tentatives	Contrôle de l'E/S Advantys Transfert de l'état de l'usine entre automates	Scrutateur central échangeant des données avec un ou plusieurs équipements
Messagerie Modbus	Equipements terrain, automate à automate et supervision Niveaux 1, 2 et 3	50 ms+	Occasionnel ou non périodique (rapports d'exception)	Accusé de réception pour chaque transfert de données avec mécanisme de nouvelles tentatives	Confirmation de fin de processus Communication s SCADA/IHM	Equipement client à équipement serveur
Global Data	Automate à automate Niveau 2	20 ms+	10 ms à 30 s périodique	Aucun	Distribution de l'état d'un équipement à un groupe d'équipements	Nombreux équipements de publication à nombreux équipements abonnés
TCP ouvert	Equipement terrain à automate, automate à automate et automate à superviseur Niveaux 1, 2 et 3	100 ms+	100 ms+ ou basé sur exception	Configurable par l'utilisateur	Programmation d'un nouveau protocole de communication s (par ex. IP Ethernet) pour communiquer avec un équipement tiers	Un client à un serveur

Services de transfert des données à distance

Service	Niveau, utilisation courante	Temps de réponse	Fréquence de transfert de données	Confirmation d'échange	Exemples	Topologie des communications
Notification par message électronique	Niveau de l'entreprise Niveau 1	Minutes	Rapport d'exception, jusqu'à plusieurs par minute	Confirmation d'envoi, pas de confirmation de livraison	Rappels de maintenance Rapports de production	Un client de messagerie à de nombreux destinataires
Messagerie électronique FactoryCast HMI						
Connectivité de base de données FactoryCast HMI	Niveau de l'entreprise Niveau 1	Secondes	1 s à 30 min	-	Envoi de rapports et de données de production directement à une base de données	Un équipement à une base de données
OPC	Niveau de l'entreprise Niveau 1	50 ms à plusieurs secondes	Rapport d'exception ou périodique	Confirmation par transaction	Serveur SCADA à clients SCADA Système de surveillance d'usine à équipements d'usine	Serveur OPC central avec Modbus TCP/IP vers équipements d'usine, puis OPC communique les données d'usine à d'autres applications SCADA ou IHM

Services de diagnostic

Service	Destinataire du diagnostic	Diagnostic d'un ou de plusieurs équipements	Diagnostic d'usine ou d'équipement	Exemples	Topologie des communications
Diagnostics intégrés	Personnes	Simple	Informations sur l'équipement interne	Accès distant aux informations sur l'état et la configuration du module via un navigateur Web	Plusieurs clients de navigateur Web
FactoryCast	Personnes	Simple ou multiple	Informations sur l'usine	Affichage de l'état du cycle de l'usine à l'aide de pages Web personnalisées simples	Plusieurs clients de navigateur Web

Service	Destinataire du diagnostic	Diagnostic d'un ou de plusieurs équipements	Diagnostic d'usine ou d'équipement	Exemples	Topologie des communications
FactoryCast HMI	Personnes/ machines	Simple ou multiple	Informations sur l'usine	Affichage distant efficace de l'état de l'usine à l'aide de pages et d'applications Web personnalisées avancées	Nombreux clients de navigateur Web
SNMP	Machines	Simple ou multiple	Informations sur le réseau d'équipements	Surveillance de l'état du réseau de l'usine par gestion réseau (HP Openview)	Système de gestion de réseau vers nombreux équipements SNMP
Telnet	Personnes	Simple	Equipement	Surveillance de l'état de l'équipement interne	Un client Telnet à un serveur Telnet sur un équipement

Services de configuration

Service	Configuration de	Configuré par	Exemple
FDR	Équipements sur le réseau par un serveur FDR	Un serveur FDR, fournissant la configuration automatique des équipements clients	Configuration automatique des paramètres d'exploitation d'un équipement d'E/S Ethernet distribué une fois l'équipement connecté au réseau
Diagnostics intégrés	Un équipement connecté par un utilisateur	Une personne	Configuration des paramètres d'exploitation d'un lecteur à vitesse variable via un navigateur Web
SNMP	Un équipement connecté par un utilisateur ou par un système de gestion de réseau	Une personne ou un système de gestion de réseau	Configuration des paramètres de composant d'infrastructure réseau à l'aide d'un système de gestion de réseau
Telnet	Un équipement connecté par un utilisateur	Une personne	Configuration des paramètres d'exploitation d'un réseau de pont série à Ethernet à l'aide d'une connexion directe

Contrôle de la compatibilité du service

Avant de sélectionner un service, assurez-vous que les équipements impliqués dans le transfert des données prennent en charge le service souhaité. Si un équipement ne le prend pas en charge, vous devez sélectionner un autre service. Si vous choisissez un autre service moins adapté, cela ne signifie pas nécessairement que l'interaction entre les équipements ne peut pas être réalisée, mais uniquement que l'utilisation du réseau et des ressources de l'équipement peut ne pas être optimale. Une fois que vous avez sélectionné le service, enregistrez-le dans la liste des communications de l'usine.

Combinaison de transferts de données

Une fois que tous les services ont été sélectionnés, les interactions entre les équipements semblables utilisant le même service peuvent être combinées. Cela peut s'avérer inapproprié pour certaines interactions (par ex. l'utilisation du protocole FTP pour transférer des fichiers à une fin particulière ne peut pas être combinée avec un transfert FTP distinct), mais peut être bénéfique pour d'autres. Par exemple, si vous utilisez la messagerie Modbus pour transférer l'état de 10 éléments différents, vous pouvez la combiner dans un transfert unique.

Evaluation du système

Réalisez une évaluation du système pour vous assurer que la combinaison de tous les transferts de données ne surcharge aucun service ou équipement. Une surcharge peut en effet entraîner la diminution des performances d'un service ou l'échec des transferts de données.

Conception réseau

Votre réseau doit être conçu afin de prendre en charge les services que vous sélectionnez ou, si le réseau est déjà en place, contrôlé afin de vérifier qu'il peut transporter les services requis. Les éléments à contrôler sont les suivants :

- réseaux, sous-réseaux (*voir page 144*) et adressage (*voir page 142*) ;
- bande passante ;
- routeurs (*voir page 153*) et pare-feux (*voir page 165*) ;
- RAS. (*voir page 159*)

3.2 Service I/O Scanning

Vue d'ensemble

Cette section décrit le service I/O Scanning et la manière dont il est utilisé pour échanger des données entre un équipement central et un grand nombre d'équipements distants.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Description du service I/O Scanning	184
Fonctionnement du scrutateur d'E/S	187
Périodes de répétition	192
Etats défectueux courants	194
Temps de réponse	195

Description du service I/O Scanning

Service I/O Scanning

Le service I/O Scanning est une tâche de communication autonome qui échange des données de registre entre un équipement exécutant le service et un grand nombre d'équipements distants sur le réseau, via le protocole Modbus TCP. Ce service ne nécessite qu'une simple opération de configuration au niveau du scrutateur d'E/S ; aucune programmation particulière n'est requise dans cet équipement ni dans les équipements distants.

L'équipement distant doit être un serveur Modbus TCP/IP. Voici quelques exemples d'équipements distants :

- E/S distribuées telles que Advantys STB et Momentum,
- équipements intelligents tels que les variateurs Altivar et les contrôleurs de circuit Sepam,
- automates tels que Quantum et Premium,
- équipements série Modbus tels que les relais moteur Lt6 accessibles par l'intermédiaire d'un pont,
- tout équipement tiers qui est un serveur Modbus TCP/IP.

Le scrutateur d'E/S lit et écrit les données de façon répétitive pendant une période définissable par l'utilisateur (entre 20 ms et 5 s). Ces échanges en lecture/écriture génèrent une charge sur le réseau. C'est la raison pour laquelle le scrutateur d'E/S est mieux adapté aux opérations périodiques critiques.

Le scrutateur d'E/S est configuré en fonction d'une liste d'équipements, de zones de données et de la vitesse à laquelle s'effectue l'échange des données de registre. Il établit une connexion avec l'équipement distant et échange les données en respectant la vitesse configurée. Il maintient la connexion avec l'équipement distant tout en gérant les erreurs éventuelles qui surviennent. Pour chaque équipement distant, un rapport est renvoyé à l'application, indiquant si les données sont transférées à la vitesse d'échange spécifiée.

Caractéristiques du scrutateur d'E/S

Le scrutateur d'E/S est un système ouvert ; vous n'êtes lié à aucune plate-forme particulière ni à une marque donnée. Le système de scrutation des E/S est constitué de deux parties, le scrutateur et le ou les équipement(s) distant(s).

Le scrutateur n'a aucun contrôle sur l'équipement distant. Par exemple, si l'équipement tombe en panne, le scrutateur d'E/S ne peut pas émettre son état de repli. Le scrutateur d'E/S est capable d'émettre l'état que sa valeur d'application devrait prendre en cas de perte de communication avec l'équipement distant. Il n'existe aucun écran de paramètres configurables individuel pour les équipements distants. Vous pourrez peut-être effectuer une écriture initiale sur l'équipement distant pour le configurer, si cette opération est prise en charge par l'équipement distant. Cependant, vous devrez désactiver cette entrée après la configuration initiale, car vous ne voulez pas que la requête d'écriture se produise à chaque période de répétition configurée. Le scrutateur d'E/S ne possède aucune information spécifique concernant l'équipement distant, à l'exception de son adresse IP. Etant donné que le système est ouvert, vous n'avez aucun contrôle sur le temps de réponse de l'équipement distant. Avec d'autres systèmes d'E/S, vous pouvez configurer ce temps de réponse. Dans un système de scrutation des E/S, aucune valeur n'est définie pour indiquer à quel moment s'effectue l'échange des données de registre, cette valeur pouvant varier d'un équipement distant à l'autre.

Voici d'autres caractéristiques du scrutateur d'E/S :

- La taille maximale des blocs de données transférables est égale à 100 mots écrits et 125 mots lus par entrée.
- Le nombre maximum de mots lus ou écrits est égal à 4 000.
- Il est possible d'échanger plusieurs blocs de données avec un même équipement distant.
- La vitesse de transfert répétitif des données (*voir page 192*) est définie par l'utilisateur (valeur comprise entre 1 ms et 5 s).
- Un rapport de défauts est généré pour chaque équipement distant.
- L'échange des données peut être activé/désactivé pour chaque équipement distant.

Chaque entrée de la configuration du scrutateur d'E/S crée un socket, incluant plusieurs entrées pointant vers le même équipement distant.

Exigences du service I/O Scanning au niveau de l'équipement distant

- Prise en charge de la messagerie Modbus TCP/IP ou de l'esclave série Modbus si un pont série-vers-Ethernet est utilisé
- Prise en charge des codes fonction Modbus 3 (lecture des registres), 16 (écriture des registres) et 23 (lecture/écriture des registres), selon les données échangées

Applications

Le service I/O Scanning doit être utilisé lorsqu'un équipement central doit échanger des données (lecture ou écriture) avec un équipement distant à une vitesse fixe, raisonnablement rapide. Les applications concernées sont les suivantes :

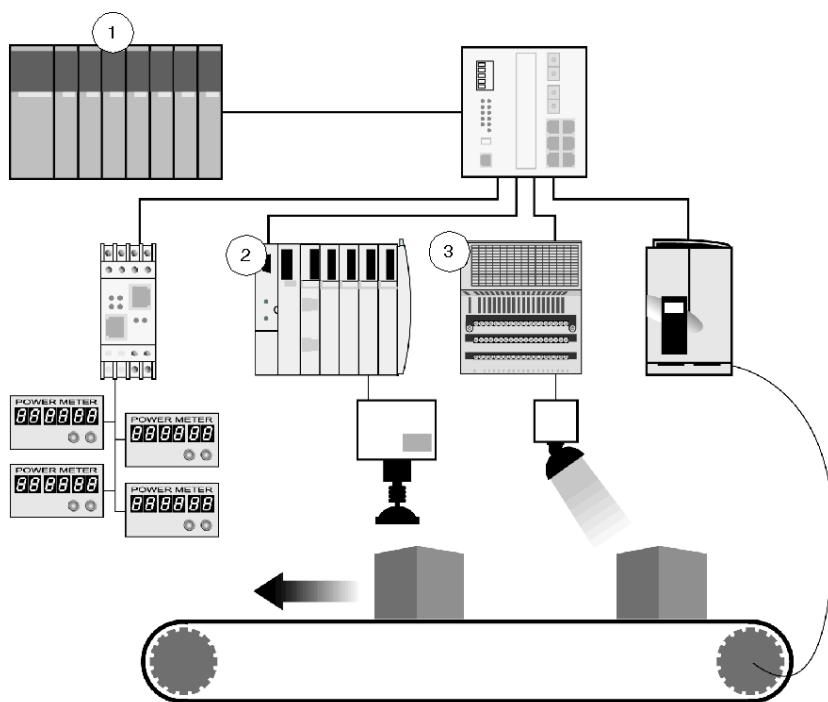
- communications répétitives rapides,
- applications qui demandent une communication entre un équipement et plusieurs équipements distants, et dans lesquelles des données différentes sont échangées avec des équipements distants différents,
- applications devant échanger des données avec plus d'équipements qu'il n'est possible en utilisant les blocs COMM existants,
- gestion automatique des erreurs,
- contrôle des équipements d'E/S,
- équipements devant échanger les mêmes données avec un grand nombre d'équipements, mais qui ne prennent pas en charge le service Global Data (*voir page 217*).

Du fait de la charge produite par les échanges de données au niveau du réseau et des équipements, le service I/O Scanning ne doit pas être utilisé pour les communications non périodiques, les actions déclenchées par des événements, la génération de rapports ou la notification d'événements. Il est nécessaire d'utiliser le service de messagerie Modbus dans ces situations.

Fonctionnement du scrutateur d'E/S

Récapitulatif

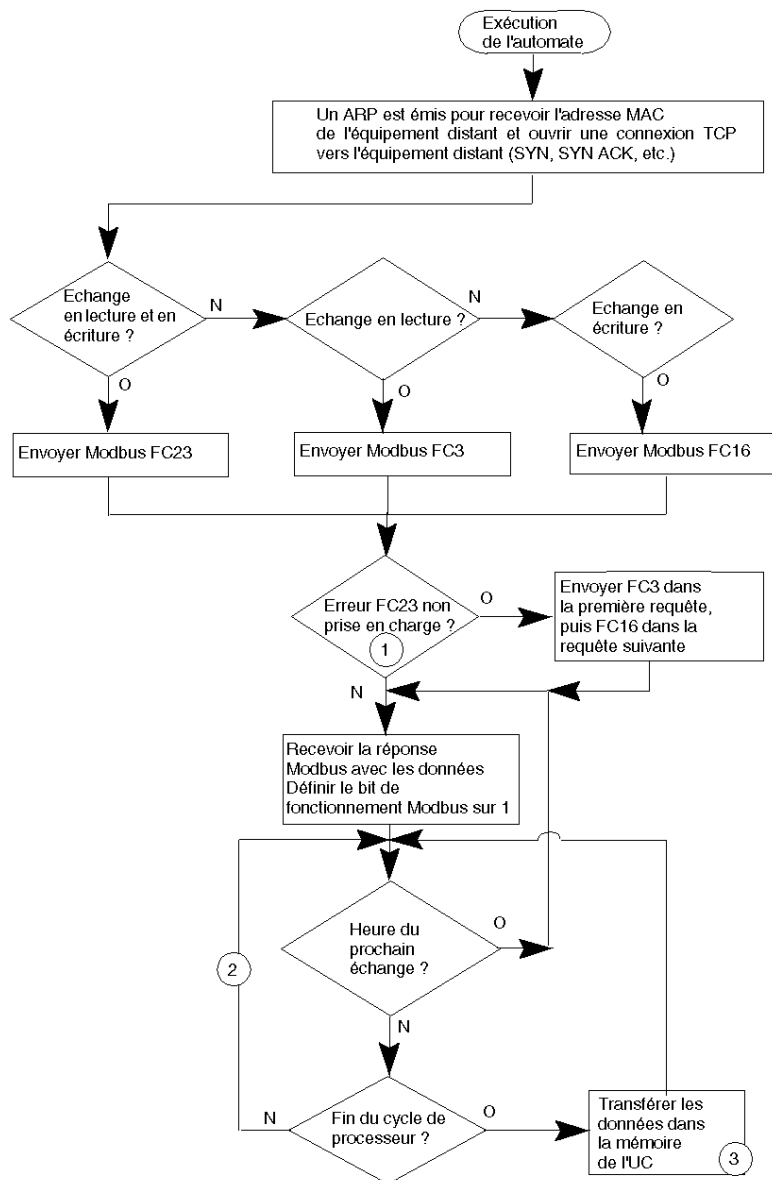
Le service I/O Scanning est mis en œuvre en tant que tâche de communication autonome distincte, soit dans un module de communication Ethernet, soit dans une UC avec un port Ethernet intégré. Lorsque le service est configuré, il reçoit une liste d'équipements à scruter et des zones mémoire où il peut lire et écrire dans les équipements distants. Il commence ensuite à échanger des données avec chaque équipement distant. Chaque entrée de la configuration du scrutateur d'E/S s'exécute indépendamment, même si plusieurs entrées échangent des données avec un équipement distant unique.



- 1 un automate
- 2 un équipement de sortie
- 3 un équipement de lecture

Fonctionnement du service

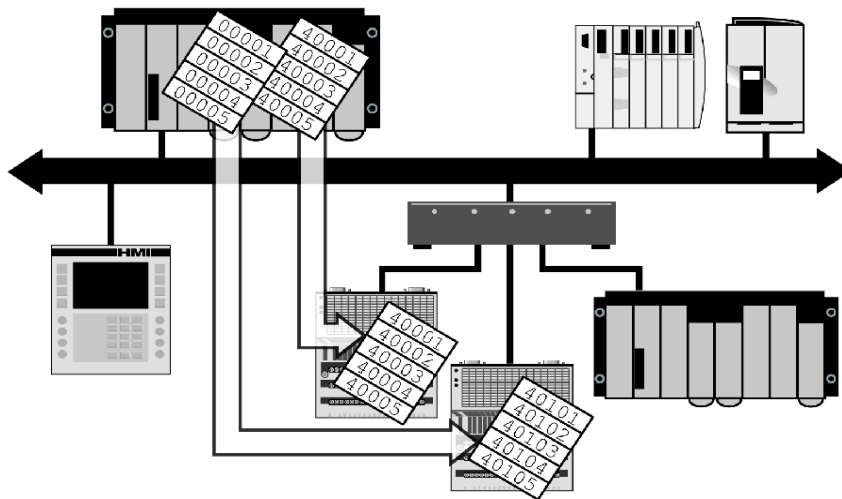
Chaque échange indépendant d'information est représenté par une entrée séparée dans la table de configuration du scrutateur d'E/S. Le diagramme suivant illustre comment le scrutateur d'E/S exécute un échange d'informations.



- 1 Si l'équipement distant ne prend pas en charge FC23, le scrutateur d'E/S utilise FC3 et FC16 pour exécuter le transfert de données. Lorsque ceci se produit, l'opération de lecture s'effectue dans le premier échange et l'opération d'écriture s'effectue lors de l'échange suivant. L'opération totale de lecture/écriture dure deux fois plus longtemps que le temps requis pour l'exécution de l'opération FC23.
- 2 La durée de cette boucle dépend de la période de répétition.
- 3 Toutes les entrées du scrutateur d'E/S échangent des données avec l'UC à la fin du cycle.

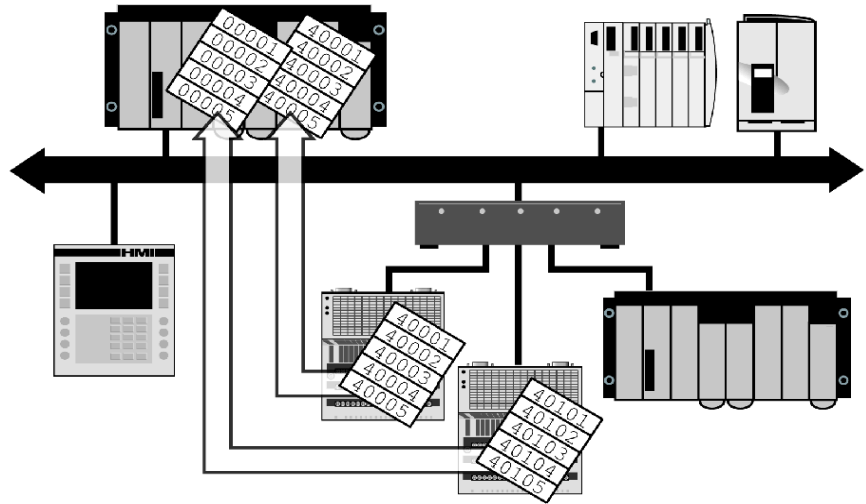
Opérations d'écriture

Le service I/O Scanning écrit les données d'une zone mémoire du scrutateur d'E/S dans une zone mémoire de l'équipement distant. Selon le scrutateur d'E/S, la mémoire contenant les valeurs à envoyer peut être des registres 16 bits (%MW ou 4x) ou des blocs de bits (%M ou 0x). Les données sont toujours écrites dans des registres 16 bits sur les équipements distants.



Opérations de lecture

Le scrutateur d'E/S lit les données des zones mémoire des équipements distants pour recueillir l'état de l'équipement terrain ou de l'entrée. Les équipements distants stockent toujours ces données d'état dans des registres 16 bits. Lorsque les données ont été lues, elles peuvent être stockées dans des registres 16 bits (%MW ou 4x) ou des blocs de bits (%M ou 0x) dans la mémoire du scrutateur d'E/S.



Gestion des erreurs

En cas de perte de communication avec un ou plusieurs équipements distants, le scrutateur d'E/S applique les valeurs de repli configurées aux zones mémoire correspondantes du scrutateur d'E/S. Si une défaillance de communication se produit, le scrutateur d'E/S ne contrôle plus le fonctionnement de l'équipement distant. Ces périphériques gèrent leurs propres états de repli.

Activer/désactiver

Activer/désactiver vous permet de démarrer et d'arrêter l'échange des données entre un équipement distant et le scrutateur d'E/S. Quatre registres à mot double sont désignés sur les 128 entrées dans la configuration du scrutateur d'E/S. Chaque entrée du scrutateur d'E/S est contrôlée par un seul bit. Lorsqu'un bit de contrôle est activé, l'échange des données est désactivé et le bit de fonctionnement est désactivé à l'issue de la période de temporisation. A ce stade, le socket TCP vers l'équipement distant est fermé.

Cette fonction peut être utilisée pour limiter le nombre de sockets simultanés vers un équipement distant. Par exemple, dans un pont Modbus Ethernet-série, qui prend en charge un nombre limité de sockets TCP simultanés, l'activation du bit de contrôle ayant été désactivé ouvre un nouveau socket et active la reprise de l'échange I/O Scanning. Toutefois, le bit de fonctionnement reste désactivé jusqu'à ce que le premier échange de données avec l'équipement distant soit terminé.

Fonctionnement du bit de fonctionnement

Le bit de fonctionnement indique si un échange de données s'est déroulé avec succès. Si une erreur se produit mais est résolue au cours de la période de temporisation, le bit demeure activé. Le bit de fonctionnement se désactive si l'échange de données n'est pas terminé/résolu au cours de la période de temporisation. La période de temporisation doit être plus longue que la période de répétition. Pour un module Ethernet Quantum NOE, la période de temporisation doit également être plus longue que la durée du cycle de processeur, du fait de la liaison avec les cycles de processeur.

Prise en charge du mot de diagnostic

Un mot de diagnostic est fourni pour chaque échange du scrutateur d'E/S. Ce mot fournit des informations de diagnostic supplémentaires sur les codes d'erreur. La mise en œuvre dépend de la plate-forme.

Utilisation du socket TCP

Le scrutateur d'E/S ouvre un seul socket TCP pour chaque échange de données configuré. Un équipement configuré pour plusieurs échanges a plusieurs sockets. Le scrutateur d'E/S utilise les numéros de port TCP source dans la plage 3000 - 4000.

Périodes de répétition

Récapitulatif

La période de répétition correspond au taux d'échange de données configuré pour le service I/O Scanning.

Périodes de répétition effectives

La période de répétition *effective* est le taux réel d'interrogation des données à partir des équipements distants. Ce taux peut être différent de la période de répétition configurée sur les différentes plates-formes d'automates et les modules d'option. La période effective est déterminée par l'installation du service I/O Scanning. La période de répétition effective est limitée par :

- le temporisateur du service I/O Scanning
- les temps de réponse des équipements distants
- le temps de cycle de processeur et le temps de transfert de données

Aucune nouvelle requête ne peut être émise avant que l'équipement distant n'ait répondu à la précédente.

Périodes de répétition/horloges internes

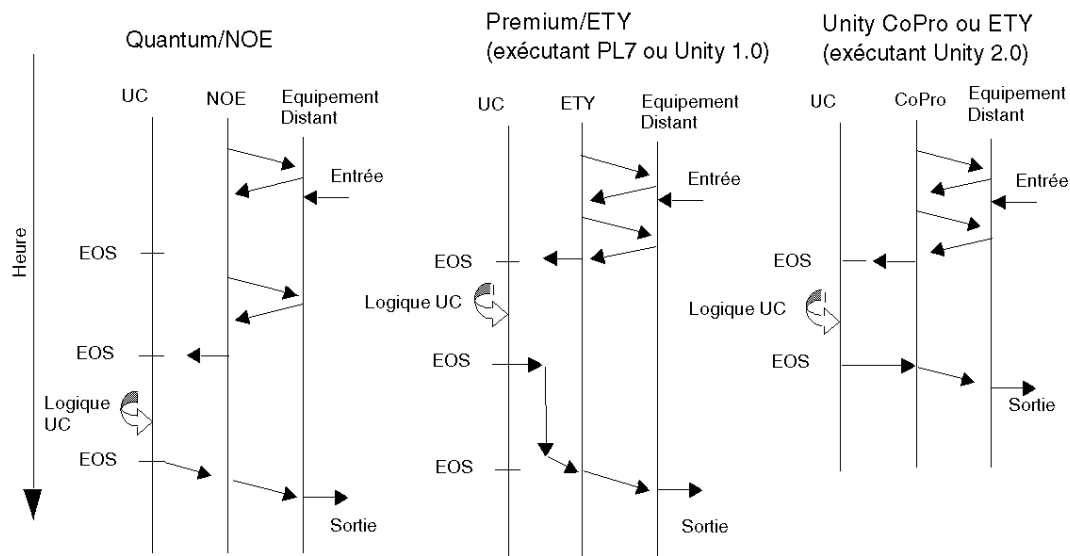
Les périodes de répétition sont limitées par le scrutateur d'E/S. Un module de communication Ethernet Quantum NOE a une fréquence d'horloge de 17 ms. Un module de communication Ethernet Premium ETY ou une UC Unity CoPro avec un port Ethernet intégré (Quantum ou Premium) a une fréquence d'horloge de 10 ms. La fréquence d'horloge limite la résolution du temps dans lequel une requête du scrutateur d'E/S est envoyée à un équipement distant.

Lorsque la fréquence de répétition configurée est de 0 ms, le système envoie des requêtes le plus rapidement possible. Dans un système Quantum NOE, des requêtes sont envoyées après le transfert des données à chaque fin de cycle (EOS). Un système Premium ou Copro envoie des requêtes aussi souvent qu'un équipement distant peut répondre à la requête qui précède.

Lorsque la période de répétition est configurée à une valeur supérieure à 0 ms, elle est arrondie à un multiple de 10 ms sur un système Premium ou Unity Copro ou à 17 ms sur un système Quantum. Par exemple, un système Premium dont la période de répétition est configurée à 35 ms envoie une requête toutes les 40 ms (pourvu que le terminal ait terminé de répondre). Un système Quantum NOE configuré à une période de répétition de 25 ms envoie une requête toutes les 34 ms ou une fois par cycle de l'automate, en prenant la valeur la plus élevée.

Exemple comparatif

Le diagramme suivant compare les périodes de répétition effectives pour les systèmes Quantum, Premium et Unity CoPro sur plusieurs cycles :



- Un automate Quantum doté d'un module de communication Ethernet NOE échange des données avec un équipement distant une fois par cycle de processeur. Ceci limite la période de répétition effective à une valeur supérieure à un cycle de processeur de l'automate.
- Un automate Premium avec un module de communication Ethernet ETY (dans un environnement PL7 ou Unity 1.0) échange des données à la période de répétition configurée (en supposant que l'équipement puisse répondre dans ce délai) et échange les données avec l'UC à chaque cycle EOS. Le cycle de sortie nécessite un cycle de processeur supplémentaire pour transférer les données au module ETY.
- Une UC Unity CoPro avec un port Ethernet intégré ou une UC Premium avec un module ETY dans un environnement Unity transfère les données à la période de répétition configurée (en supposant que l'équipement puisse répondre dans ce délai).

NOTE : Les valeurs des données peuvent être échangées avec l'équipement distant plusieurs fois par cycle de processeur. La dernière valeur lue à partir de l'équipement distant est envoyée à l'UC lors de l'EOS suivant et la valeur écrite sur l'équipement distant est celle de l'UC à l'EOS précédent.

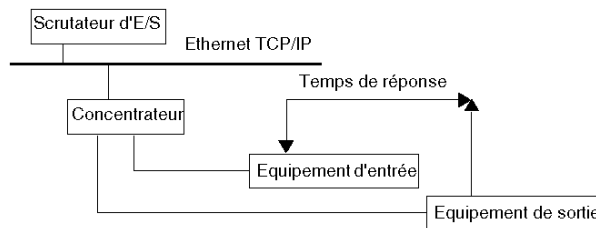
Etats défectueux courants

Etat	Cause	Réponse
Un équipement est introuvable sur le réseau.		Le scrutateur d'E/S émettant les requêtes ARP tente de rechercher l'équipement distant. Des requêtes sont envoyées toutes les 30 s.
Surcharge de socket : un équipement distant refuse d'accepter une connexion du socket TCP.	Cette erreur est courante sur les ponts avec un grand nombre d'entrées dans le scrutateur d'E/S ou dans les équipements de base qui prennent en charge un nombre limité de sockets. Elle se produit lorsqu'un bit de fonctionnement s'éteint selon des intervalles aléatoires.	Si l'équipement distant ne parvient pas à ouvrir le socket TCP, le scrutateur d'E/S tente d'ouvrir un socket chaque seconde. Si le problème persiste, il se peut que vous puissiez le corriger en utilisant la fonction activer/désactiver (<i>voir page 191</i>). Pour libérer des sockets, limitez le nombre d'échanges de données du scrutateur d'E/S fonctionnant sur la même adresse IP.
Un équipement distant refuse FC23.	Si vous utilisez des scrutateurs d'E/S pre-Unity 2.0 I/O ou des terminaux qui ne renvoient pas le code d'erreur correct, le scrutateur d'E/S est défaillant. Il continue d'envoyer FC23 et continue d'être défaillant.	Lorsque cette défaillance se produit, l'équipement renvoie une exception Modbus avec un code d'erreur correspondant au code de fonction non pris en charge. Le scrutateur d'E/S se replie sur une combinaison de FC3 et de FC16.
Une requête ou un paquet de réponses est perdu, ou le socket est endommagé et ne peut transférer les données.		Les transmissions normales du socket TCP se produisent sur la première retransmission par le scrutateur d'E/S ; après trois retransmissions, le socket est réinitialisé et un nouvel ARP est émis. La perte d'un paquet Ethernet peut désactiver le bit de fonctionnement sauf s'il y a suffisamment de temps pour réémettre le paquet et recevoir une réponse avant que la période de temporisation n'ait expiré. Le nombre d'essais concernant un paquet perdu ou corrompu varie selon les différentes versions du produit. Les versions précédentes effectuaient une nouvelle tentative à 800 ms, 600 ms, 1,5 s et 3 s. Les versions plus récentes basent leurs nouvelles tentatives sur les temps de réponse précédents, mais dans un bon système, il est possible d'atteindre environ 50 ms, 800 ms 1,5 s.

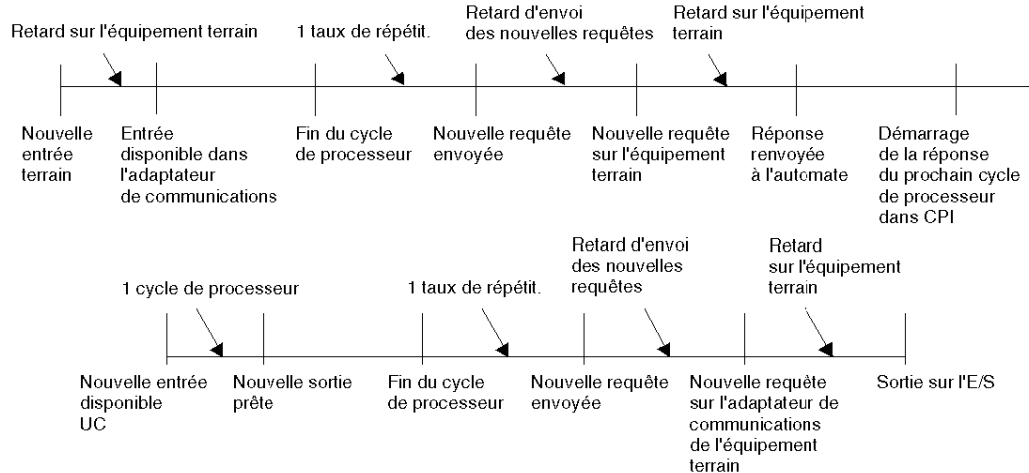
Temps de réponse

Le temps de réponse du scrutateur d'E/S dépend du :

- temps de cycle du processeur
- délai de réponse à la requête de l'équipement scruté
- temps d'activation de l'équipement scruté pour une nouvelle entrée ou une nouvelle sortie



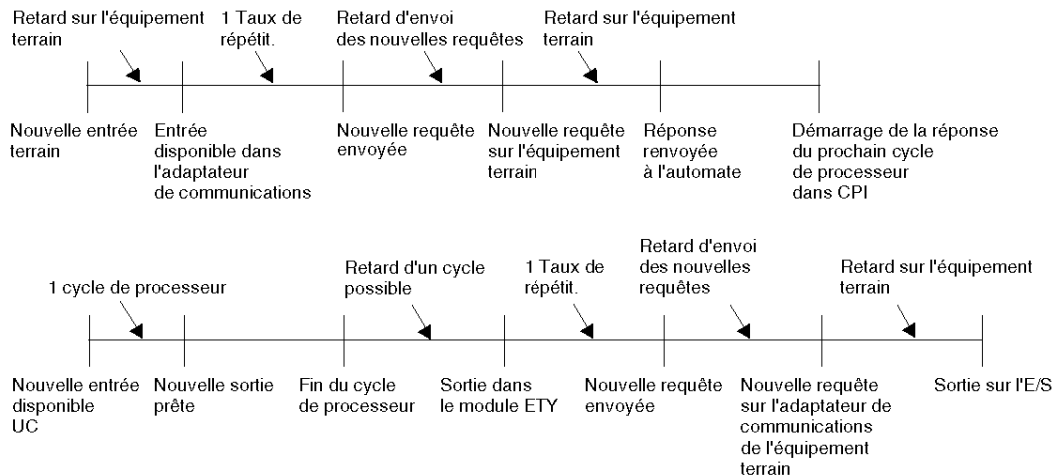
Le diagramme suivant illustre les performances d'un scrutateur d'E/S Quantum, lors de l'aller-retour entre l'entrée et la sortie terrain, en passant par l'UC.



Pour une période de répétition configurée de 0 ms, la formule du temps la moins favorable est la suivante :

- $temps\ total = T_{mod} + 1\ cycle\ de\ processeur + [if\ (T1 > 1\ cycle\ de\ processeur)\ then\ (T1 + 1\ cycle\ de\ processeur)\ Else\ (1\ cycle\ de\ processeur)] + 1\ cycle\ de\ processeur + 0,3\ ms * pas\ de\ requêtes + T_{mod}$
- $T1 = 0,3\ ms * nombre\ de\ requêtes + temps\ de\ réponse\ de\ l'équipement$

Le diagramme suivant illustre les performances d'un scrutateur d'E/S Premium, lors de l'aller-retour entre l'entrée et la sortie terrain en passant par l'UC.



Pour une période de répétition de 0 ms, la formule du temps la moins favorable est la suivante :

- $temps\ total = T_{mod} + T1 + 1\ cycle\ de\ processeur + 1\ cycle\ de\ processeur + 1\ cycle\ de\ processeur\ (pour\ ETY\ seulement) + 0,3\ ms * nombre\ de\ requêtes + T_{mod}$
- $T1 = 0,3\ ms * nombre\ de\ requêtes + temps\ de\ réponse\ de\ l'équipement$

Le diagramme suivant illustre le temps de réponse type du scrutateur d'E/S d'une entrée terrain sur un équipement scruté vers une sortie terrain activée sur un autre équipement scruté du fait de la logique de l'automate déclenchée à partir de la première entrée. Le temps de cycle de processeur est d'environ 50 ms. Le temps de réponse de l'équipement scruté est d'environ 10 ms.

Système d'automate	Nombre d'équipements scrutés		
	1	16	32
Quantum ou Premium avec NOE/ETY (autre que Unity)	110 ms	115 ms	125 ms
UC Unity Quantum ou Premium avec port Ethernet intégré	100 ms	105 ms	115 ms

3.3 Messagerie Modbus

Vue d'ensemble

Cette section décrit le service de messagerie Modbus. Ce service gère le protocole Modbus et permet les transferts de données entre les équipements du réseau.

Contenu de ce sous-chapitre

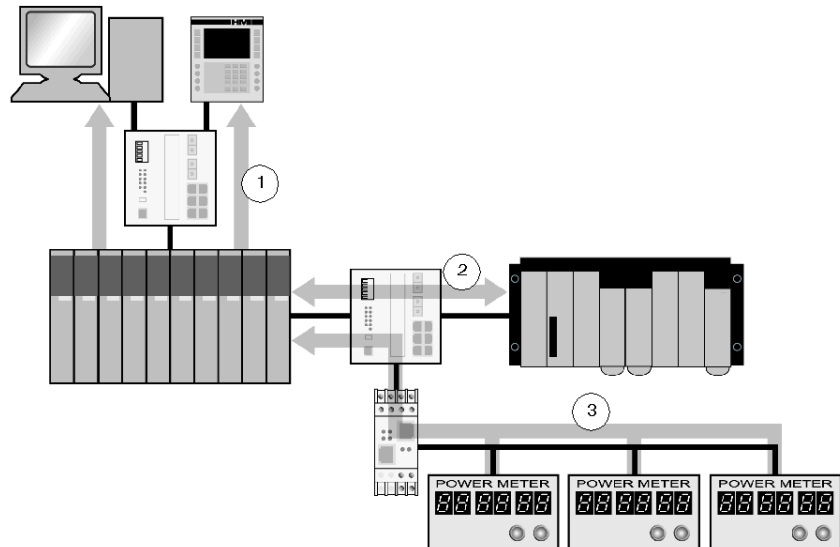
Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Description du service de messagerie Modbus	198
Equipements prenant en charge les services Ethernet Modbus	203
Fonctionnement du client Modbus dans les systèmes Quantum	204
Fonctionnement du client Modbus dans les systèmes Premium	206
Fonctionnement du client Modbus dans les systèmes Momentum	208
Fonctionnement du serveur Modbus dans les systèmes Quantum	209
Fonctionnement du serveur Modbus dans les systèmes Premium	212
Fonctionnement du serveur Modbus dans les systèmes Momentum	214
Serveurs Modbus et limites des sockets	215
Nombre de tentatives et délais d'attente de la messagerie Modbus	216

Description du service de messagerie Modbus

Services de messagerie Modbus

Le service de messagerie Modbus gère le transfert des données ou des commandes entre deux équipements. L'un des équipements est le client et l'autre est le serveur. Le client lance la requête et le serveur y répond. Ces services utilisent le protocole Modbus (ou Modbus sur TCP/IP dans les applications Ethernet) pour assurer le transfert des données entre les équipements.



- 1 Requête de données SCADA et IHM
- 2 Transfert des données de l'automate
- 3 Collecte des données de l'équipement

Norme de communication Modbus

Modbus est la norme de communication industrielle depuis 1979. Elle est désormais combinée à Ethernet TCP/IP pour prendre en charge les solutions Transparent Ready.

Modbus sur TCP/IP est un protocole Ethernet complètement ouvert. Le développement d'une connexion à Modbus TCP/IP ne nécessite pas l'achat d'un composant propriétaire ou d'une licence. Ce protocole se combine aisément à n'importe quel équipement prenant en charge une pile de communication TCP/IP standard. Les spécifications peuvent être obtenues gratuitement sur le site www.modbus.org.

Mise en œuvre d'un équipement Modbus TCP

La couche d'application Modbus est très simple et universellement reconnue. Des milliers de fabricants mettent déjà en œuvre ce protocole. Un grand nombre a déjà développé des connexions Modbus TCP/IP et de nombreux produits sont déjà disponibles. Le protocole Modbus TCP/IP est simple et permet à n'importe quel petit équipement terrain, tel qu'un module d'E/S, de communiquer via Ethernet sans microprocesseur puissant ni mémoire interne très volumineuse.

Modbus TCP/IP

Le même protocole d'application est utilisé pour la liaison série Modbus, Modbus Plus et Modbus TCP. L'interface achemine les messages d'un réseau vers un autre sans changer de protocole. Etant donné que le protocole Modbus est mis en œuvre au-dessus de la couche TCP/IP, vous pouvez également bénéficier de l'acheminement IP qui permet aux équipements de communiquer quelle que soit la distance qui les sépare et quel que soit l'endroit où ils se trouvent dans le monde.

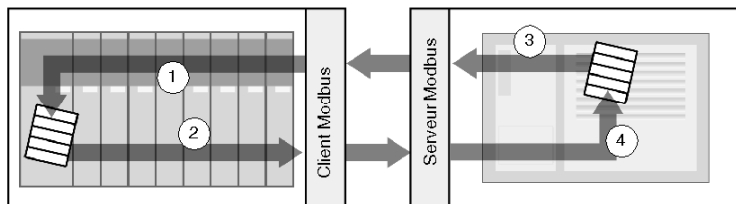
Schneider propose une gamme complète de passerelles permettant l'interconnexion d'un réseau Modbus TCP/IP à des réseaux existants Modbus Plus ou de liaison série Modbus. Pour plus de détails, contactez votre agence commerciale régionale Schneider Electric. L'institut IANA a affecté à Schneider le port TCP 502, réservé au protocole Modbus.

Récapitulatif de la messagerie Modbus

Le transfert d'informations entre un client et un serveur Modbus démarre lorsque le client envoie une requête au serveur pour transférer des informations, exécuter une commande ou exécuter l'une des nombreuses autres fonctions possibles.

Lorsque le serveur a reçu la requête, il exécute la commande ou récupère les données requises dans sa mémoire. Il répond ensuite au client soit en accusant réception de l'exécution de la commande, soit en fournissant les données demandées.

Le temps de réponse système dépend de deux facteurs principaux : le temps nécessaire au client pour envoyer la requête ou recevoir la réponse et la capacité du serveur à répondre dans un délai donné.

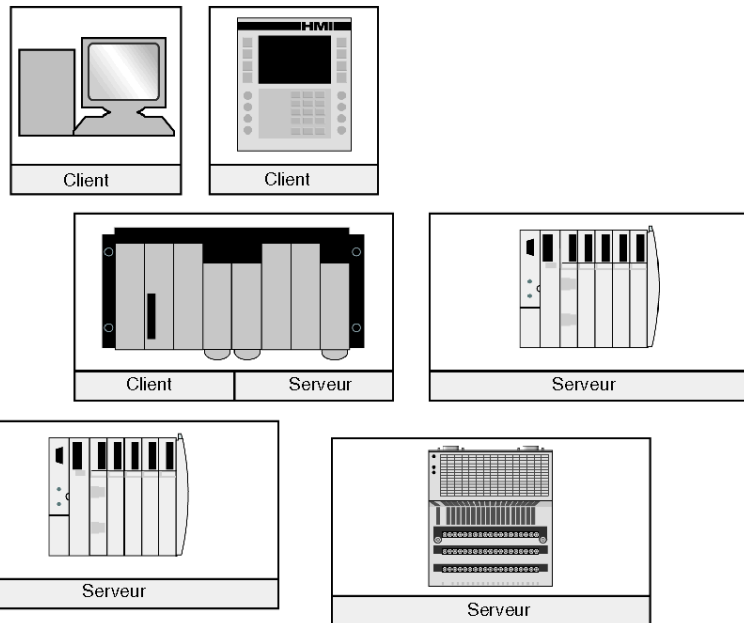


- 1 Données récupérées
- 2 Requête du client
- 3 Réponse du serveur
- 4 Récupération des données

Un équipement peut mettre en œuvre un service client Modbus, un service serveur Modbus, ou les deux, selon ses besoins. Un client peut lancer des requêtes de messagerie Modbus vers un ou plusieurs serveurs. Le serveur répond aux requêtes qu'il reçoit d'un ou de plusieurs clients.

Une application IHM ou SCADA type met en œuvre un service client dans le but d'établir des communications avec les automates et les autres équipements et de collecter des informations. Un équipement d'E/S met en œuvre un service serveur afin que d'autres équipements puissent lire et écrire ses valeurs d'E/S. Cet équipement n'a pas besoin d'établir de communications et n'intègre donc aucun service client.

Un automate propose à la fois les services client et serveur, ce qui lui permet d'établir des communications avec d'autres automates et équipements d'E/S et de répondre aux requêtes provenant d'autres dispositifs (automates, systèmes SCADA, modules IHM et autres équipements).



Ce qu'apporte un service client Modbus

Un équipement mettant en œuvre le service client Modbus peut lancer des requêtes de messagerie Modbus vers un autre équipement qui met en œuvre un serveur Modbus. Avec ces requêtes, le client peut récupérer des données de l'équipement distant ou lui envoyer des commandes.

Ce qu'apporte un service serveur Modbus

Un équipement mettant en œuvre le service serveur Modbus peut répondre aux requêtes lancées par n'importe quel client Modbus. Le service serveur Modbus permet à un équipement de mettre toutes ses données internes et d'E/S à disposition des équipements distants à des fins de lecture et de contrôle.

Codes fonction Modbus

Le protocole Modbus est un ensemble de codes fonction, dans lequel chaque code définit une action spécifique que doit exécuter le serveur. La capacité d'un équipement à exécuter des fonctions de lecture et d'écriture est déterminée par les codes fonction Modbus mis en œuvre par le serveur.

Le protocole Modbus se base sur cinq zones mémoire situées à l'intérieur de l'équipement.

Zone mémoire	Description
0x ou %M	Bits mémoire ou bits de sortie
1x ou %I	Bits d'entrée
3x ou %IW	Mots d'entrée
4x ou %MW	Mots mémoire ou mots de sortie
6x	Zone mémoire étendue

En plus des codes fonction utilisés pour lire et écrire les données au sein de ces zones, il existe des codes pour les statistiques, la programmation, l'identification des équipements et les réponses d'exception. Le serveur Modbus peut mettre à disposition les données dans les limites suivantes :

- Lecture : 125 mots ou registres
- Ecriture : 100 mots ou registres

Quand doit-on utiliser le client

Un client Modbus doit être utilisé lorsque des données doivent être échangées entre deux équipements selon des intervalles irréguliers ou peu fréquents (lorsqu'un événement survient, par exemple). Le client permet le déclenchement d'une requête par le code d'application (dans le cas d'un automate ou d'un système SCADA) ou par un temporisateur interne (système SCADA ou module IHM). L'utilisateur va donc établir des communications uniquement lorsqu'elles sont nécessaires et les ressources seront utilisées de manière plus efficace.

Lorsque les données doivent être échangées à une vitesse fixe courte, le service I/O Scanning (*voir page 183*) doit plutôt être utilisé (si ce service est pris en charge par le client).

Quand doit-on utiliser le serveur

L'accès au serveur Modbus s'effectue depuis un client Modbus ou via un service I/O Scanning et doit servir à transférer des informations, des commandes ou d'autres données requises relatives à l'usine. Le serveur Modbus propose un transfert des données en temps réel ou l'accès aux rapports de données stockés dans sa mémoire. Il répond à toutes les requêtes Modbus qu'il reçoit. Aucune configuration supplémentaire n'est requise.

Lorsqu'un équipement doit échanger des informations sur le statut, des commandes ou des données concernant l'usine avec d'autres équipements, il doit mettre en œuvre un serveur Modbus. Lorsqu'il intègre le service serveur, l'équipement peut répondre aux requêtes envoyées par les clients Modbus et mettre ses E/S internes et ses données à disposition des équipements distants à des fins de lecture et de contrôle. Cet équipement peut être un module d'E/S, un variateur, un dispositif de mesure de puissance, un disjoncteur, un départ-moteur ou un automate.

Les modules d'E/S sont de bons exemples d'équipements mettant en œuvre un service serveur Modbus. En tant que serveurs, les modules d'entrée et les modules de sortie permettent à d'autres équipements de contrôle de respectivement lire et écrire leurs valeurs.

Un système d'automate met en œuvre à la fois les services client et serveur. Le service client permet à l'automate de communiquer avec d'autres automates ou modules d'E/S, tandis que le service serveur lui permet de répondre aux requêtes provenant d'autres dispositifs (automates, systèmes SCADA, modules IHM et autres équipements). Lorsqu'ils n'ont pas besoin de répondre aux requêtes de transfert de données, les équipements n'ont pas l'obligation de proposer un service serveur.

Equipements prenant en charge les services Ethernet Modbus

Equipement		Client Modbus	Serveur Modbus
Unity Pro Quantum	140CPU65150	X	X
	140CPU65160	X	X
	140NOE77101	X	X
	140NOE77111	X	X
	140NWM10000	X	X
Unity Pro Premium	TSXP571634M	X	X
	TSXP572634M	X	X
	TSXP573634M	X	X
	TSXP574634M	X	X
	TSXP575634M	X	X
	TSXETY4103	X	X
	TSXETY110WS	X	X
	TSXETY5103	X	X
	TSXWMY100	X	X
Micro TSX	TSXETZ410	X	X
	TSXETZ510	X	X
Momentum	171CCC96020	X	X
	171CCC96030	X	X
	171CCC98020	X	X
	171CCC98030	X	X
	171ENT11001	-	X
	171ENT11002	-	X
Twido	499TWD01100	X ¹	X ¹
Advantys STB	STBNIP2212	-	X
Altivar ATV38/58	VW3A58310	-	X
Passerelles/ponts Power Logic	EGX200	-	X ¹
	EGX400	-	X ¹
Systèmes de câblage ConneXium	174CEV30020	X ¹	X ¹
	174CEV20030	X ¹	X ¹
	174CEV20040	X ¹	X ¹
¹ L'équipement reçoit et envoie les messages Modbus comme une passerelle.			

Fonctionnement du client Modbus dans les systèmes Quantum

Limites

En utilisant un logiciel de programmation Concept ou Proworx, une application sur un système Quantum peut lancer des communications client Modbus en utilisant les blocs client Modbus suivants :

- MSTR
- READ_REG
- WRITE_REG
- C_READ_REG
- C_WRITE_REG

L'automate Quantum lit et écrit dans la zone de données 4x ou %MW uniquement. Jusqu'à 16 blocs client Modbus peuvent être déclenchés simultanément par un module de communications Ethernet NOE. Si des blocs supplémentaires sont déclenchés, ils sont mis en mémoire tampon jusqu'à ce qu'un ou plusieurs blocs actifs terminent leurs opérations.

Fonctionnement du client Modbus Quantum

Un client Modbus Quantum fonctionne de la manière suivante :

Séquence d'exécution	Événement
1	L'application déclenche le bloc client Modbus.
2	La requête est immédiatement envoyée au module de communications Ethernet NOE.
3	Le module NOE vérifie si un socket TCP est connecté à l'équipement de destination.
4	Si aucun socket TCP n'est connecté, le NOE initialise un socket TCP et le connecte à l'équipement de destination.
5	Le module NOE envoie la requête Modbus.
6	Le message circule sur le réseau et il se produit un retard du réseau.
7	Le serveur Modbus reçoit le message.
8	Le serveur Modbus répond à la requête.
9	Le message circule sur le réseau et il se produit un retard de réseau.
10	Le NOE reçoit la réponse.
11	La prochaine fois que le bloc client Modbus est atteint dans le code, la réponse est recueillie à partir du module NOE et les nouvelles données éventuelles sont mises à la disposition de l'application de l'utilisateur.
12	Le NOE laisse le socket TCP ouvert pour une utilisation future.

NOTE : Le module NOE laisse le socket TCP ouvert jusqu'à ce que l'autre extrémité le ferme ou jusqu'à ce que le module NOE atteigne sa limite de sockets TCP. Si l'un de ces événements se produit, le NOE ferme tous les sockets n'ayant pas de requête en attente.

Les modules NOE plus récents peuvent envoyer plusieurs requêtes sur un simple socket TCP. Certains modules NOE plus anciens ne peuvent prendre en charge qu'un simple socket TCP par requête et ferment le socket TCP à la fin de chaque échange.

Fonctionnement du client Modbus dans les systèmes Premium

Limites

En utilisant Unity Pro ou un logiciel de programmation PL7, une application sur un système Premium peut lancer des communications client Modbus en utilisant les blocs client Modbus suivants :

- WRITE_VAR
- READ_VAR
- SEND_REQ
- DATA_EXCH

L'automate Premium limite le nombre de blocs de communication du client Modbus pouvant être déclenchés simultanément (selon le type d'UC). Cette limite s'applique au nombre total de blocs de requête client Modbus par UC et comprend les blocs déclenchés pour les services de messagerie suivants :

- Client Modbus TCP/IP
- Fipway
- Série Modbus
- Unitelway
- Ethway

Si des blocs client supplémentaires sont déclenchés, un message d'erreur est renvoyé au programme d'application.

Les requêtes du client Modbus sont limitées de la manière suivante :

Client : famille de processeurs	Mécanisme de communications Ethernet	Nombre de requêtes
Unity Pro v2.0 CoPro	Module ETY ou port intégré*	80*
Unity niveau 2 P57-xx	Module ETY	32
Unity niveau 4 TSX574-xx	Module ETY	64
PL7 niveau 2 TSX572-xx	Module ETY	32
PL7 niveau 4 TSX574-xx	Module ETY	64
* Lorsque Unity 2.0 CoPro utilise un port intégré, il peut envoyer 80 requêtes, mais ne peut accepter que huit réponses par cycle.		

Fonctionnement du client Modbus Premium

Le client Modbus fonctionne de la manière suivante :

Séquence d'exécution	Événement
1	L'application déclenche le bloc client Modbus.
2	Le processeur conserve la requête jusqu'à la fin du cycle de processeur en cours.
3	Le module ETY vérifie si un socket TCP est connecté à l'équipement de destination.
4	Si aucun socket TCP n'est connecté, le module ETY initialise un socket TCP et le connecte à l'équipement de destination.
5	Le module ETY envoie la requête Modbus.
6	Le message circule sur le réseau et il se produit un retard de réseau.
7	Le serveur Modbus reçoit le message.
8	Le serveur Modbus répond à la requête.
9	La réponse circule sur le réseau et il se produit un retard de réseau.
10	Le module ETY reçoit la réponse.
11	La réponse est retransmise à l'UC lors de la phase suivante (début du cycle de processus suivant).
12	La prochaine fois que le bloc client Modbus est atteint dans le code, la réponse et les nouvelles données éventuelles sont mises à la disposition de l'application de l'utilisateur.
13	L'ETY laisse le socket TCP ouvert pour une utilisation future.

NOTE : Le module ETY laisse le socket TCP ouvert jusqu'à ce que l'autre extrémité le ferme ou jusqu'à ce que le module ETY atteigne sa limite de sockets TCP. A ce stade, le module ETY ferme tous les sockets n'ayant pas de requête en attente. Le module ETY peut envoyer plusieurs requêtes sur un socket unique.

Fonctionnement du client Modbus dans les systèmes Momentum

Limites

Grâce au logiciel de programmation Unity Pro, Concept ou ProWorx, une application exécutée sur un système Momentum peut lancer des communications client Modbus à l'aide des blocs client Modbus suivants :

- MSTR
- READ_REG
- WRITE_REG
- C_READ_REG
- C_WRITE_REG

L'automate Momentum lit et écrit dans les zones de données 4x ou %MW uniquement. Il est possible de déclencher jusqu'à 16 blocs client Modbus concurrents. Si un bloc supplémentaire est déclenché, il renvoie un code d'erreur à l'application.

Fonctionnement du client Modbus Momentum

Un client Modbus Momentum fonctionne de la manière suivante :

Séquence	Événement
1	L'application déclenche un bloc client Modbus.
2	Le processeur conserve la requête jusqu'à la fin du cycle d'UC en cours.
3	A la fin du cycle d'UC en cours, l'automate Momentum commence à ouvrir un socket vers l'équipement cible et un message SYN est envoyé.
4	Le serveur Modbus renvoie un message SYN ACK.
5	A la fin du cycle d'UC suivant, l'automate Momentum reçoit le message SYN ACK et ouvre le socket.
6	Dès que le socket est ouvert, l'automate Momentum envoie la requête Modbus.
7	Le message est envoyé et il se produit un retard sur le réseau.
8	Le serveur Modbus reçoit le message.
9	Le serveur Modbus répond à la requête.
10	La réponse est renvoyée et il se produit un retard sur le réseau.
11	L'automate Momentum reçoit la réponse.
12	A la fin du cycle d'UC suivant, la réponse est lue dans l'automate Momentum et le socket est fermé.
13	Dès que le code fait appel au bloc client Modbus, la réponse et les nouvelles données sont mises à la disposition de l'application.

Fonctionnement du serveur Modbus dans les systèmes Quantum

Mise en œuvre Quantum

Un serveur Modbus est mis en œuvre dans un module de communications Ethernet NOE ou un port Ethernet intégré dans l'automate Quantum. Les données auxquelles doit accéder le serveur Modbus sont conservées dans la mémoire de l'UC de l'automate. L'interface entre le module NOE ou le port intégré et l'UC définit le fonctionnement du serveur Modbus.

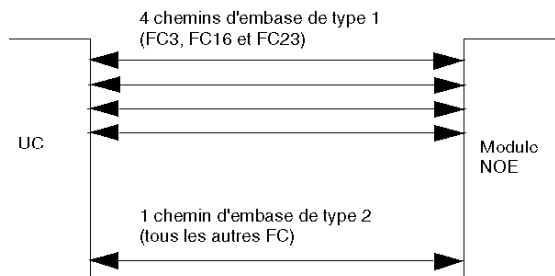
Fonctionnement du serveur Modbus Quantum

Le serveur Modbus des systèmes Quantum fonctionne de la façon suivante :

Séquence d'exécution	Événement
1	Un client Modbus établit un socket TCP vers le module NOE ou le port Ethernet intégré.
2	Le client Modbus envoie une requête sur le socket TCP.
3	Le module NOE ou le port Ethernet intégré reçoit la requête et peut en accuser réception.
4	La requête est placée dans la file d'attente, à l'intérieur du module à transmettre à l'UC. L'UC permet au module NOE/port Ethernet intégré d'accéder à sa mémoire à la fin du cycle de processeur.
5	Dans le cas du module NOE, ce dernier transmet la requête de la file d'attente vers l'UC selon l'une des deux modalités suivantes : ● Si le NOE demande la lecture/écriture du registre Modbus (FC3, FC16 ou FC23), il lit la mémoire de l'automate en utilisant la requête de type 1. ● Si le module NOE demande un autre code de fonction Modbus, il transmet l'ensemble de la requête à l'UC pour le traitement de type 2. Dans le cas du port Ethernet intégré, la requête de la file d'attente est transmise à l'UC.
6	Le module NOE/port Ethernet intégré reçoit immédiatement une réponse à toute requête (sauf les requêtes de programmation) envoyée à l'UC.
7	Le module NOE/port Ethernet intégré renvoie la réponse au client Modbus.
8	Le socket TCP est laissé ouvert.

- Les requêtes de type 1 donnent au module NOE l'accès direct à la mémoire.
- Les requêtes de type 2 transmettent le message Modbus complet à l'UC.

Selon le système, le module NOE ou le port intégré peut répondre à un nombre différent de requêtes à la fin de chaque cycle de processeur. Le diagramme suivant montre les cinq chemins d'embase entre le module NOE et l'UC :



Fonctionnement du serveur Modbus Concept/Proworx

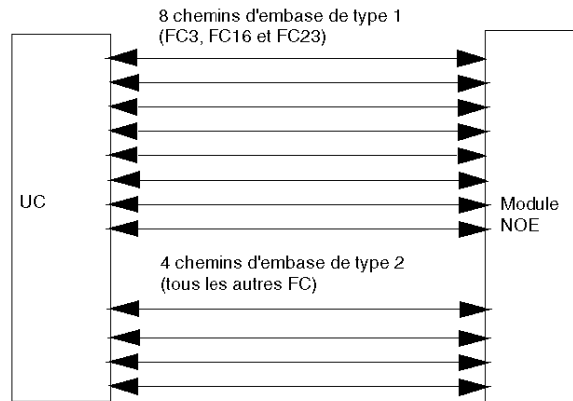
Chaque fois que le module NOE est desservi (une fois par cycle de processeur), il envoie une requête sur chacun des cinq chemins. Les chemins d'embase de type 1 donnent l'accès direct à la mémoire de l'UC. Le module NOE utilise les chemins pour lire/écrire des registres 4x directement sur la mémoire de l'UC pour Modbus FC3, FC16 et FC23.

Les chemins d'embase de type 2 permettent de transmettre le message Modbus à l'UC. Le NOE utilise ce chemin pour transmettre toutes les requêtes du code de fonction à l'UC ; l'UC gère le message Modbus. Les exemples de code de fonction incluent des variables non localisées (FC42), le logiciel de programmation d'automate (FC125, FC43), et des requêtes de lecture/écriture 0x, 1x, 3x. Le chemin de type 2 n'est pas utilisé pour répondre aux requêtes pour des registres 4x (FC3, FC16 et FC23).

Le nombre de chemins d'embase limite les performances du serveur Modbus. Par exemple, si Modbus 10 requêtes FC3 et 5 requêtes FC42 sont mises en file d'attente à l'intérieur du module NOE, un total de 5 cycles de processeur est nécessaire pour terminer le transfert. Au cours des 3 premiers cycles de processeur, 10 requêtes FC3 (4 par cycle de processeur) et 3 requêtes FC42 (1 par cycle de processeur) sont transférées, mais 2 cycles de processeurs supplémentaires sont nécessaires pour transférer les 2 requêtes FC42 restantes.

Performances du serveur Modbus Unity)

Dans un système serveur Modbus Unity, les types et utilisations des chemins restent les mêmes, mais les performances sont améliorées 2 à 4 fois sur le système Concept.



L'Unity 2.0 NOE/embase prend en charge :

- huit requêtes de chemin de type 1 servies par cycle de processeur
- quatre requêtes de chemin de type 2 servies par cycle de processeur (jusqu'à la limite de 20 requêtes)

NOTE : Pour voir l'amélioration, il se peut que vous deviez régler le logiciel SCADA pour vérifier qu'un nombre suffisant de requêtes est envoyé à l'automate.

Fonctionnement du serveur Modbus dans les systèmes Premium

Mise en œuvre Premium

Les systèmes d'automate Premium mettent en œuvre un serveur Modbus dans l'UC de l'automate. Les cartes ETY ou les ports intégrés transmettent les requêtes Modbus à l'UC pour qu'elles y soient traitées. L'UC limite le nombre de requêtes Modbus auxquelles le serveur peut répondre par cycle de processeur. Cette limite inclut les requêtes en provenance de :

- Modbus TCP/IP
- Fipway
- Série Modbus
- Unitelway
- Ethway

Une exception *Modbus occupé* se produit lorsque l'UC reçoit plus de requêtes qu'elle ne peut en gérer au cours d'un cycle processeur. Si cela se produit, une réponse d'exception est renvoyée au client Modbus qui a envoyé la requête.

Le tableau qui suit montre le nombre de requêtes traitées par cycle de processeur pour différents systèmes d'automate Premium.

Automate		Mécanisme de communications Ethernet	Réponse par cycle
Pre-Unity v2.0	Unity Pro v2.0 CoPro	Module ETY* ou port intégré**	20 (estimation)
	Unity niveau 2 P57-xx	Module ETY*	20
	Unity niveau 4 TSX 574-xx	Module ETY*	20
	PL7 niveau 2 TSX572-xx	Module ETY*	8
	PL7 niveau 4 TSX574-xx	Module ETY*	16
Unity Pro v2.0	Unity CoPro	port intégré**	16
		Module ETY*	20
	Unity TSX P57304M	Module ETY*	12
* Le module ETY est limité à 400 transactions/s pour tous les modules.			
** Le port Ethernet intégré est limité à 500 transactions/s sur les systèmes Unity CoPro.			

Fonctionnement du serveur Modbus Premium

Le processus de réponse des systèmes Premium fonctionne de la façon suivante :

Séquence d'exécution	Événement
1	Le client Modbus établit un socket TCP vers le module ETY ou le port Ethernet intégré.
2	Le client Modbus envoie une requête sur le socket TCP.
3	Le module ETY ou le port Ethernet intégré reçoit la requête et peut en accuser réception.
4	La requête est placée dans la file d'attente du module ETY/port Ethernet intégré.
5	Au début du cycle de processeur suivant, le module ETY/port Ethernet intégré transmet la requête à l'UC. A ce moment, tous les modules de communication transmettent les requêtes à l'UC, y compris Fipway, Ethway, et les modules série SCP.
6	L'UC répond au plus grand nombre possible de requêtes (la limite est déterminée par l'UC).
7	S'il existe un nombre plus grand de requêtes reçues que de requêtes pouvant recevoir une réponse, l'UC envoie une réponse d'exception Modbus occupé au module ETY/port Ethernet intégré, qui renvoie la réponse d'exception aux clients.
8	Le module ETY/port Ethernet intégré reçoit des réponses à toutes les requêtes ayant reçu une réponse et renvoie des réponses aux clients.
9	Le socket TCP est laissé ouvert.

Temps de réponse Premium

Le temps de réponse Premium est le délai écoulé entre la réception d'une requête et le début du cycle de processeur suivant.

Fonctionnement du serveur Modbus dans les systèmes Momentum

Mise en œuvre Momentum

L'automate Momentum met en œuvre un serveur Modbus en le considérant comme un élément de l'UC principale. Le nombre de requêtes Modbus auquel peut répondre une UC Momentum est illimité.

Fonctionnement du serveur Modbus Momentum

Le serveur Modbus de l'UC Momentum fonctionne de la manière suivante :

Séquence d'exécution	Événement
1	Le client Modbus établit un socket TCP vers l'UC Momentum, qui peut prendre plusieurs cycles de processeur.
2	A la fin du premier cycle, un SYN est reçu et renvoyé au client.
3	Le client Modbus envoie une requête sur le socket TCP.
4	L'UC reçoit la requête.
5	La requête est traitée à la fin du prochain cycle de processeur.

Serveurs Modbus et limites des sockets

Serveurs Modbus simples

Produit	Temps de réponse
Advantys	4,5 ms
Variateur ATV58	30 ms
Momentum ENT1100/02	1 ms (4,5 ms supplémentaires pour inclure l'embase d'E/S)
Momentum ENT1101	5 à 9 ms

NOTE : Les temps de réponse ci-dessus n'incluent pas les temps de réaction d'E/S.

Limites des sockets TCP des serveurs Modbus

Produit	Limite de socket TCP
Modules Quantum NOE NOE77100/10	32
Modules Quantum NOE NOE77101/11	64 (tous les services Ethernet combinés)
Premium ETY410/510	32 (tous les services Ethernet combinés)
Premium ETY4102/5102	64 (tous les services Ethernet combinés)
UC Momentum	12
Momentum ENT1100/02	4
Momentum ENT1101	4

Nombre de tentatives et délais d'attente de la messagerie Modbus

Client Modbus

Le service du client Modbus prend en charge le nombre de tentatives au niveau de la couche application (*voir page 137*). Le système effectue également des tentatives TCP pour vérifier que les requêtes et les réponses Modbus sont transmises. Le nombre de tentatives et les délais d'attente Modbus dépendent de l'équipement :

Plate-forme	Nombre de tentatives TCP	Délais d'attente du client Modbus
Quantum	5, 25 et 45 s	30 s, pas de nouvelle tentative
Premium	5, 25 et 45 s	défini par l'utilisateur (dans le bloc de communication) sans nouvelles tentatives

Serveur Modbus

Le service du serveur Modbus ne prend pas en charge le nombre de tentatives au niveau de la couche application. Le système implémente les nouvelles tentatives TCP pour s'assurer que les requêtes et les réponses Modbus sont transmises. Le nombre de tentatives dépend de l'équipement :

Plate-forme	Nombre de tentatives TCP
Unity 2.0 Quantum	50 ms, 800 ms et 1,5 s
Unity 2.0 Premium	50 ms, 800 ms et 1,5 s
Quantum	800 ms et 1,5 s
Premium	800 ms et 1,5 s

3.4 Service Global Data

Vue d'ensemble

Le service Global Data assure le transfert d'informations en temps réel d'un équipement source vers un autre équipement du réseau qui souscrit à ces informations.

Contenu de ce sous-chapitre

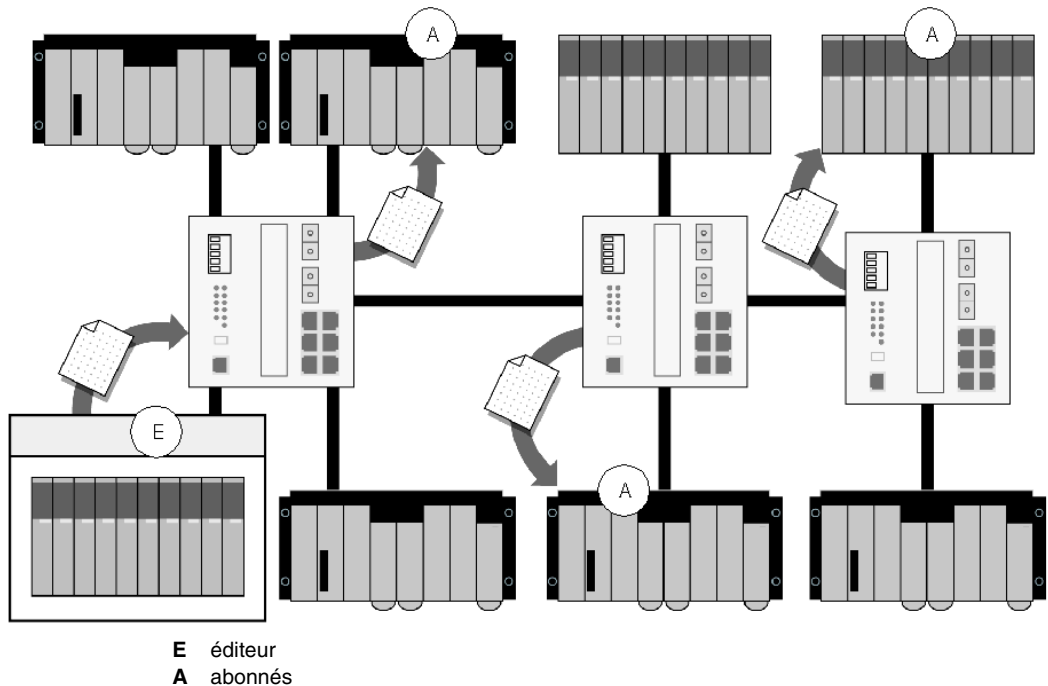
Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Service Global Data	218
Considérations relatives à Global Data	222

Service Global Data

Récapitulatif

Sur Ethernet, le service Global Data permet à un équipement de *publier* des informations en temps réel sur le réseau. Tout équipement connecté au réseau peut choisir de recevoir ces informations. Les équipements qui doivent échanger des informations sont organisés en groupes de distribution. Chaque équipement d'un groupe peut publier un bloc de données dans le groupe entier et sélectionner les blocs de données publiées auxquels il souhaite souscrire (qu'il souhaite recevoir).



Normes Global Data

Le service Global Data est mis en œuvre grâce au service standard NDDS (Network Data Distribution Service). Ce service s'appuie sur le protocole RTPS (Real-Time Publish Subscribe) tel qu'il est défini par RTI (Real Time Innovations). Ce protocole a été adopté comme norme par l'OMG (Object Management Group), le groupe responsable du standard COBRA. Le service Global Data est chargé de distribuer les données sur un réseau IP grâce à la technologie de multidiffusion.

La combinaison des services ci-dessus distribue les données globales à l'aide de la technologie de multidiffusion IP/UDP.

Opérations réalisées par l'éditeur et l'abonné

L'opération Global Data implique deux types de participants : un ou plusieurs éditeurs et un ou plusieurs abonnés. Un éditeur place des données sur le réseau. Il envoie un groupe de données globales au groupe de distribution à une vitesse configurée dans l'équipement de publication.

Le groupe de distribution est un groupe logique d'équipements abonnés, appartenant éventuellement à plusieurs réseaux. Vous pouvez intégrer un équipement abonné dans un groupe de distribution en lui attribuant une adresse IP de multidiffusion. Cette adresse IP est différente de l'adresse IP normale utilisée pour Modbus, le scrutateur d'E/S, le Web, etc. Tous les équipements du groupe de distribution utilisent cette adresse IP de multidiffusion (*voir page 148*).

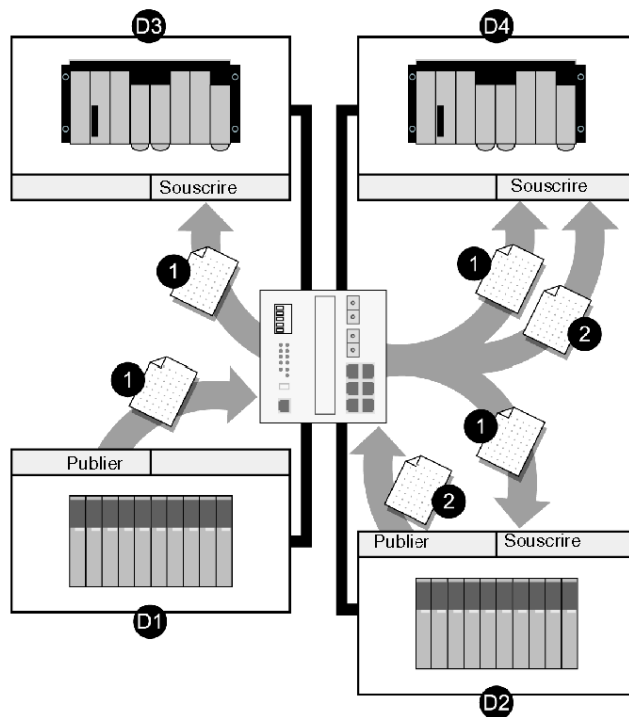
L'abonné reçoit une copie de toutes les données publiées dans le groupe de distribution, ne sélectionne que les blocs de données auxquels il souscrit, et transmet ces données à l'application de l'utilisateur.

La gestion des erreurs doit être assurée côté abonné car l'éditeur n'envoie pas les données à chaque abonné. L'éditeur place des données sur le réseau. Il n'a aucun contrôle sur les abonnés et ne reçoit aucune réponse lorsqu'un abonné réceptionne les données. Il doit surveiller le temps entre chaque réception des nouvelles données provenant chacun éditeur. Si le temps entre deux mises à jour successives de données envoyées par un éditeur est supérieur au délai de temporisation configuré, le service envoie une erreur à l'application utilisateur sur l'éditeur. Ce dernier doit surveiller les erreurs et effectuer une action si aucune donnée n'est reçue.

Ce processus est différent de celui des communications Modbus, dans lesquelles une commande est envoyée à un autre équipement pour effectuer une action. Dans le cas de Modbus, l'équipement émetteur de la commande doit savoir si l'envoi aboutit. Grâce à Global Data, l'éditeur rend simplement les informations disponibles et délègue à l'abonné la réception et la manipulation des informations.

Si, pour une raison quelconque, un équipement abonné ne reçoit pas une copie des nouvelles données publiées auxquelles il a souscrit, il reçoit une mise à jour de ces données lors du cycle de publication suivant. Le service Global Data publie les informations d'état rapidement, et la publication suivante envoie les toutes dernières données de souscription, et non une copie des données précédentes.

La figure ci-dessous représente un groupe de distribution constitué de quatre équipements (D1 à D4). Deux d'entre eux publient des données (D1 et D2) et trois sont des abonnés (D2, D3 et D4). L'équipement 2 publie des données et en reçoit. Le flux de données décrit comment les équipements 1, 2 et 3 souscrivent aux données publiées par l'équipement 1 et l'équipement 4 souscrit aux données publiées par les équipements 1 et 2.



Limites

Le service Global Data présente les limites suivantes relatives à la communication :

- Un groupe de distribution peut contenir jusqu'à 64 membres, chacun pouvant être un éditeur, un abonné, ou les deux.
- La restriction actuelle est que chaque module Ethernet ne peut être membre que d'un groupe. Ainsi, pour qu'un système soit membre de plusieurs groupes, il doit disposer de plusieurs modules de communication Ethernet.
- Un éditeur peut publier un bloc de données contenant jusqu'à 512 mots.
- Un abonné peut recevoir du groupe un nombre illimité de blocs de données publiées, même si certains automates restreignent le volume total des données reçues par le service.

Quand utiliser Global Data

Le service Global Data est utilisé lorsqu'un équipement souhaite rendre les informations qu'il contient disponibles à plusieurs équipements entre 10 ms et 30 s. Ce service permet à un équipement de publier les données de l'équipement et l'état de l'usine dans de nombreux autres équipements. Il n'est pas recommandé pour l'émission de commandes, car l'éditeur n'envoie pas les données à un équipement et le transfert de données ne donne pas lieu à un accusé de réception.

Le système est conçu pour qu'un équipement publie son état et que d'autres équipements réagissent à cet état. Par exemple, un lecteur publie sa vitesse et les autres lecteurs du système adaptent la leur en fonction de cette donnée.

Equipements Global Data

Les équipements ci-dessous utilisent Global Data avec une publication maximale de 512 mots et une souscription maximale de 2 048 mots :

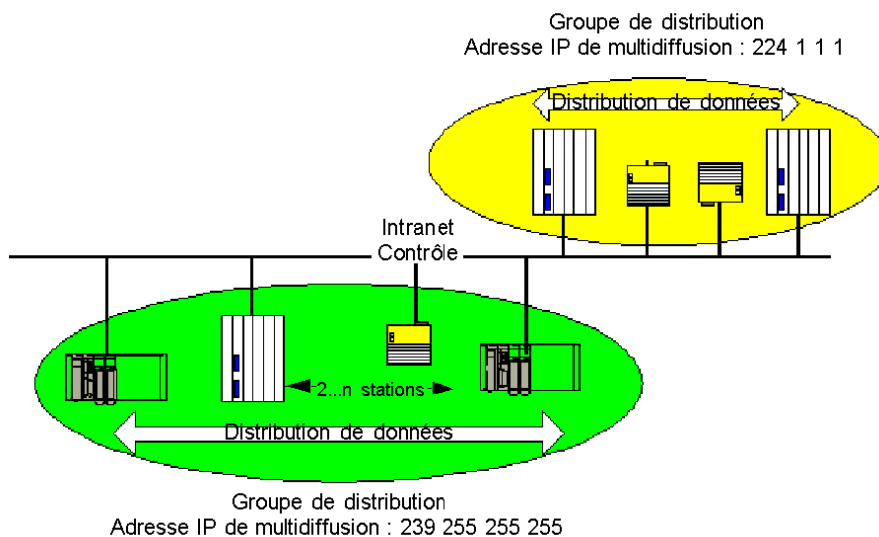
- ETY4102/5102 et ETY4013/5103
- Port Ethernet CoPro Premium et Quantum
- NOE77101/11

Considérations relatives à Global Data

Technologie de multidiffusion

Le service Global Data est mis en œuvre en utilisant la technologie de multidiffusion (voir page 147). La technologie de multidiffusion est différente des technologies de diffusion générale et de diffusion unique. La diffusion générale envoie des informations d'un équipement à tous les équipements du réseau. La diffusion unique envoie des données d'un équipement à un autre. La multidiffusion permet à un équipement d'envoyer un bloc unique (paquet) de données à un groupe de distribution (voir page 219) prédéfini.

Les données publiées qui sont envoyées à une adresse IP de multidiffusion spécifique ne sont transférées par des commutateurs et des routeurs qu'aux équipements du groupe de distribution qui souscrivent à cette adresse IP de multidiffusion. Le filtrage de multidiffusion (voir page 149) empêche les données d'aller vers chaque équipement du réseau et permet au groupe de distribution de fonctionner efficacement sur un réseau Ethernet sans perturber les autres équipements du réseau.



Le service Global Data met actuellement en œuvre GMRP pour établir le filtrage de multidiffusion. GMRP est le protocole utilisé par l'équipement cible pour notifier aux commutateurs et aux routeurs qu'il veut recevoir les données en provenance d'une adresse IP particulière de multidiffusion. Cette adresse IP appartient exclusivement à un groupe de distribution.

Synchronisation d'application

La publication des données est synchronisée au début du cycle d'UC, lorsque le taux de publication configuré a été atteint. Les données souscrites sont recopiées dans la mémoire de l'application de l'équipement abonné à la fin du cycle d'UC après la réception des données.

Temps de réponse

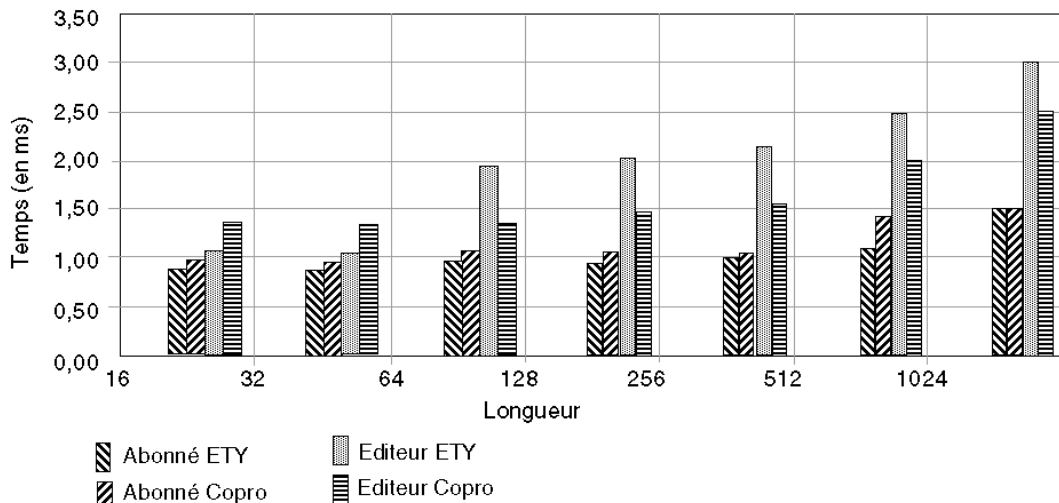
Le temps de réponse Global Data est mesuré à partir d'un changement de statut dans l'éditeur à l'heure où ce changement est connu au niveau de l'abonné :

heure de publication + 1 cycle UC sur l'éditeur + heure de publication du service + heure du réseau + heure de publication de l'abonné + 1 cycle UC sur l'abonné

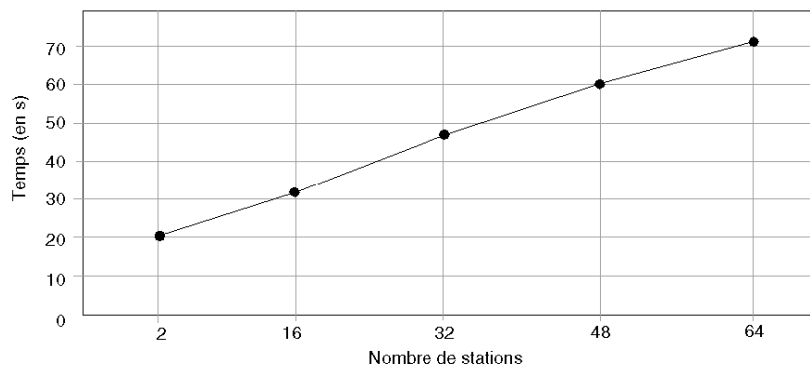
où *heure de publication du service* et *heure de publication de l'abonné* sont généralement de 1 à 2 ms chacune.

NOTE : Les systèmes ETY doivent inclure un cycle UC supplémentaire sur l'abonné.

Le diagramme suivant montre les heures de démarrage système pour un module de communications Premium ETY Ethernet et un module Unity Copro. Les temps de réponse des deux équipements sont mesurés avec chaque équipement utilisé comme abonné et comme éditeur.



Le diagramme suivant montre le temps maximal requis pour atteindre un état stable (mesuré en secondes).



3.5 Remplacement d'équipements défectueux

Vue d'ensemble

Lorsque le service FDR est pris en charge dans un équipement terrain, vous pouvez le remplacer facilement et de façon fiable en cas de panne. Lorsque l'équipement terrain est installé, il est reconfiguré automatiquement avec les paramètres d'exploitation et l'adresse IP de l'équipement en panne.

Contenu de ce sous-chapitre

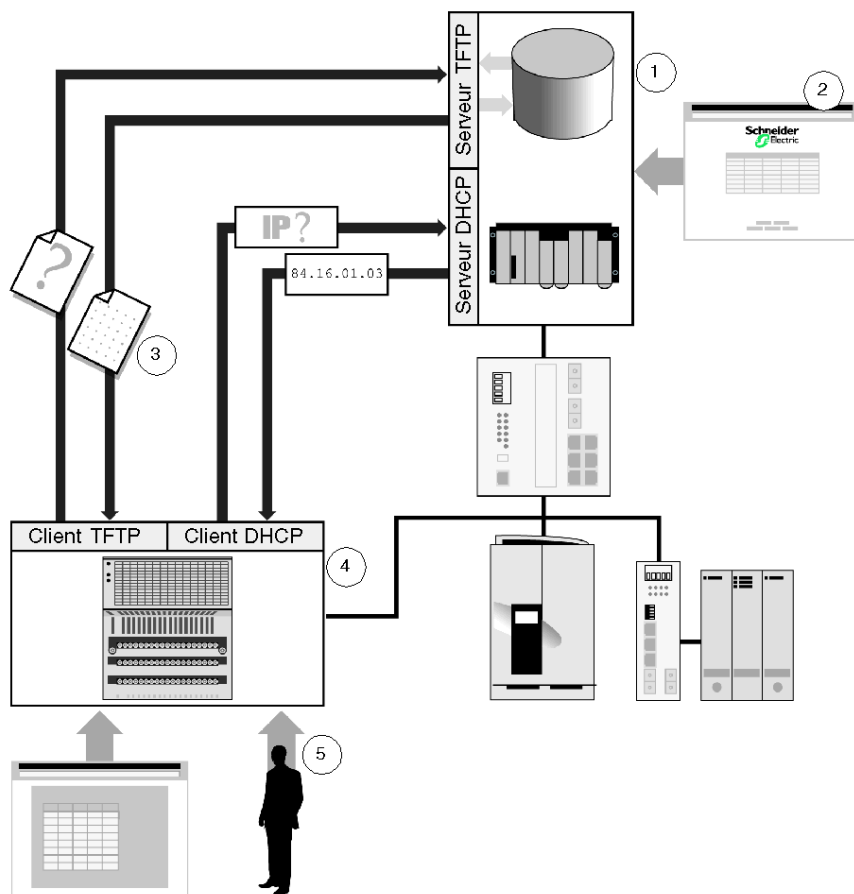
Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Service FDR (Faulty Device Replacement, Remplacement d'équipements défectueux)	226
Equipements prenant en charge les services FDR	229

Service FDR (Faulty Device Replacement, Remplacement d'équipements défectueux)

Récapitulatif

Le service FDR (Faulty Device Replacement, Remplacement d'équipements défectueux) utilise un serveur FDR central pour stocker les paramètres du réseau et les paramètres de fonctionnement des équipements présents sur le réseau. En cas de panne d'un équipement, le serveur configure automatiquement l'équipement de remplacement et lui attribue les mêmes paramètres que ceux de l'équipement défectueux. Avec le service FDR, le personnel d'entretien n'a plus besoin de conserver les enregistrements de configuration à porter de main et le risque d'erreur humaine au moment de la saisie de la nouvelle configuration est réduit.



- 1 Serveur FDR
- 2 Configuration du serveur
- 3 Fichier des paramètres de fonctionnement transféré au client FDR
- 4 Client FDR (équipement de remplacement)
- 5 Affectation des noms de rôle

Composants FDR

Un service FDR comprend un serveur et un client FDR. Le serveur est un équipement passif ; il stocke simplement tous les paramètres des équipements présents sur le réseau. Pour configurer le serveur, créez une liste des équipements connectés au réseau (chacun étant identifié par un *nom de rôle*) et de leurs paramètres IP. Une fois le service FDR activé, le serveur répond aux requêtes lancées par les clients FDR.

Le client FDR est un équipement réseau qui stocke ses paramètres sur le serveur FDR pour faciliter son remplacement. A chaque client est affecté un nom de rôle que l'identifie de façon unique par rapport aux autres équipements du réseau. Une fois connecté au réseau, l'équipement envoie une copie de ses paramètres de fonctionnement au serveur. Les paramètres réels dépendent du type d'équipement client FDR, mais doivent toujours être suffisants pour permettre à un équipement de remplacement d'être configuré pour fonctionner exactement comme le client original. Lorsque le serveur a reçu une copie des paramètres, le client vérifie périodiquement si le serveur dispose d'une série de paramètres actualisée. Une mise à jour est envoyée au serveur en cas de changement des paramètres de fonctionnement du client. Selon la mise en œuvre du client, cette mise à jour peut être ou non automatique.

La panne d'un client déclenche les événements suivants :

Séquence	Événement
1	Votre personnel d'entretien doit affecter le même nom de rôle à l'équipement de remplacement.
2	Votre personnel d'entretien place le nouvel équipement sur le réseau.
3	L'équipement envoie automatiquement une requête au serveur pour demander la série de paramètres IP qui est utilisée par un équipement portant ce nom de rôle.
4	L'équipement reçoit les paramètres IP, puis se connecte au serveur FDR et télécharge une copie de ses paramètres de fonctionnement.
5	Lorsque les paramètres ont été téléchargés, l'équipement les met en œuvre et le fonctionnement reprend.

Les paramètres réels peuvent inclure une vérification de la cohérence de l'équipement destinée à s'assurer que l'équipement de remplacement est du même type que l'original. Le client peut ensuite choisir de fonctionner même si l'équipement de remplacement est différent de l'équipement original, mais toujours compatible avec ce dernier.

Quand doit-on utiliser le service FDR

Le service FDR doit être utilisé pour tous les équipements qui le prennent en charge sur un réseau d'automatisme. Les usines doivent être mises à niveau à mesure que Schneider Electric ajoute le service FDR dans ses nouveaux équipements. Pour l'instant, le service se concentre sur les équipements d'E/S, et non sur les systèmes automates ou IHM. Dans un système à redondance d'UC, il est impossible d'utiliser le serveur FDR. Un seul serveur FDR est autorisé sur un sous-réseau (*voir page 144*). Si vous atteignez le nombre maximum de clients FDR sur un réseau, fractionnez ce dernier et affectez un nouveau serveur FDR au réseau nouvellement établi.

Equipements prenant en charge les services FDR

Equipement		Client FDR	Serveur FDR
Quantum	140CPU65150	-	X
	140CPU65160	-	X
	140NOE77101	-	X
	140NOE77111	-	X
Premium	TSXP571634M	-	X
	TSXP572634M	-	X
	TSXP573634M	-	X
	TSXP574634M	-	X
	TSXP575634M	-	X
	TSXETY4103	-	X
	TSXETY5103	-	X
Micro TSX	TSXETZ410	X	-
	TSXETZ510	X	-
Momentum	171ENT11001	X	-
Advantys STB	STBNIP2212	X	-
Altivar ATV38/58	VW3A58310	X	-

3.6 Synchronisation horaire

Vue d'ensemble

Cette section décrit le service de synchronisation horaire et la manière dont il fournit l'heure aux équipements du réseau.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Service de synchronisation horaire	231
Fonctionnement du service de synchronisation horaire	233
Applications de synchronisation horaire	234
Équipements Schneider - mise en œuvre du service de synchronisation horaire	238

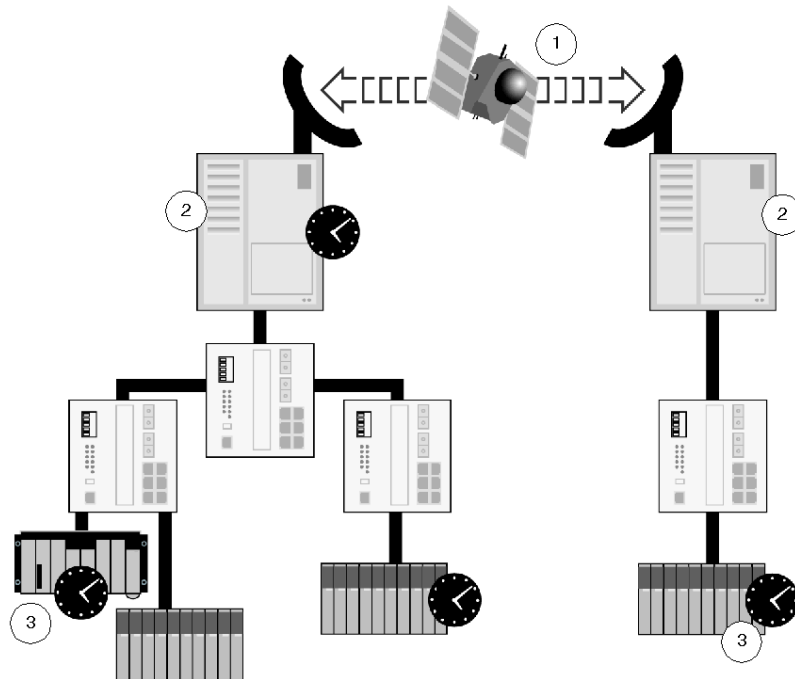
Service de synchronisation horaire

Récapitulatif de la synchronisation horaire

La synchronisation horaire est un service qui fournit et gère une heure précise pour les équipements du réseau. En général, la précision de l'heure est de l'ordre de 1 à 2 ms. Lorsque l'heure des équipements a été synchronisée, le service peut être utilisé pour :

- synchroniser une action ;
- horodater la survenue des événements (enregistrement de la chronologie des événements) ;
- gérer l'ordre des opérations d'une usine.

La synchronisation horaire s'effectue en envoyant des mises à jour horaires périodiques à tous les équipements configurés pour ce service.



- 1 Heure satellite GPS
- 2 Serveurs de synchronisation NTP
- 3 Heure locale

Description de la synchronisation horaire

La synchronisation horaire utilise le protocole SNTP pour fournir l'heure du serveur à tous les clients qui mettent en œuvre ce service. Le serveur de synchronisation central peut fonctionner indépendamment ou être connecté à un récepteur GPS, un récepteur DCF ou une horloge distante (via NTP). Le service NTP se base sur l'heure de Greenwich et les fuseaux horaires locaux, et est géré par les clients. Plusieurs serveurs de synchronisation peuvent fonctionner sur le réseau pour fournir la redondance au cas où le serveur primaire tomberait en panne.

Pour maintenir une heure précise, les clients demandent l'heure au serveur selon des intervalles configurés. Ces clients peuvent régler les temps de réponse du réseau pour le transfert de l'heure. Lorsque le client a reçu l'heure, une horloge interne la conserve localement. Lors de la prochaine mise à jour configurée, le client demande l'heure au serveur et synchronise son horloge locale. La précision de l'heure du client dépend de celle de l'horloge locale, de la fréquence des mises à jour et de la précision du serveur de synchronisation.

De nombreux équipements peuvent être utilisés comme serveurs de synchronisation (par exemple, un PC Windows ou Linux avec une précision de 1 à 30 ms, un serveur de synchronisation dédié d'une précision supérieure à 1 ms). Le serveur de synchronisation utilise une horloge locale pour conserver son heure lorsqu'il reçoit des mises à jour d'une source distante (récepteur GPS ou DCF, par exemple).

Pendant la synchronisation horaire, tous les clients demandent l'heure au serveur de synchronisation. L'horloge interne de chaque client est synchronisée avec l'heure du serveur de synchronisation, permettant ainsi d'enregistrer dans l'usine l'ensemble des alarmes et des horodatages de modification des fichiers et des programmes sur la base d'une source horaire identique. La synchronisation horaire permet de suivre l'ordre des modifications dans l'usine, sans qu'il soit nécessaire de définir manuellement l'heure pour chaque équipement.

Enregistrement de la chronologie des événements

L'enregistrement de la chronologie des événements permet de reconstruire ou d'examiner avec une grande précision l'ordre des événements dans une ou plusieurs usines. Cette application est basée sur l'horodatage précis des événements au niveau de leur source.

Synchronisation des actions

Avec la synchronisation des actions, plusieurs équipements d'une usine exécutent une opération au même moment. Cette synchronisation peut être utile pour démarrer des variateurs le long d'un convoyeur ou pour transférer des produits depuis une zone de l'usine vers une autre.

Fonctionnement du service de synchronisation horaire

Fonctionnement détaillé du service

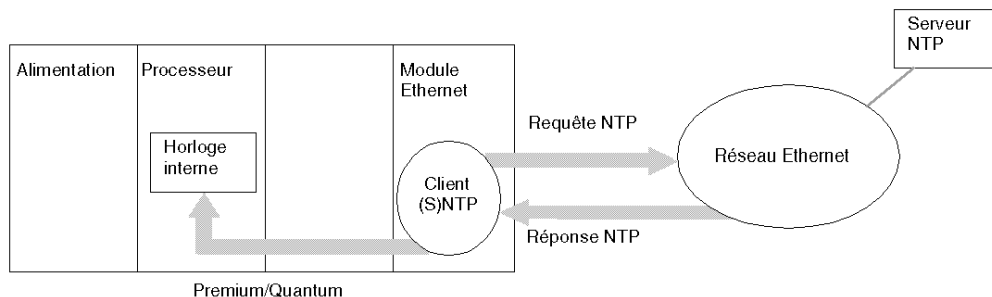
Le service de synchronisation horaire utilise le protocole SNTP pour fournir l'heure du serveur central à tous les clients qui la demandent, selon les intervalles configurés. Grâce à l'horodatage des requêtes et des réponses en chaque point de l'échange, les clients peuvent tenir compte des retards provoqués par le réseau. Les charges et les retards du réseau n'ont généralement pas d'incidence sur la précision du signal horaire. En revanche, on suppose que le retard est uniforme, de sorte que lorsqu'il survient sur le paquet de la requête mais pas sur le paquet reçu, il peut provoquer une légère imprécision de l'heure du client.

Lorsque le client a reçu l'heure, son horloge interne la conserve localement. Lors de la prochaine mise à jour configurée, le client demande l'heure au serveur et synchronise de nouveau son horloge locale. La précision de l'heure du client dépend de celle de son horloge locale et de la fréquence des mises à jour. Plus les mises à jour sont fréquentes, plus le décalage est réduit et plus l'heure du client est précise.

La précision du service est également déterminée par celle du serveur de synchronisation. Un serveur de synchronisation peut être un PC Windows ou Linux, ou bien un serveur de synchronisation dédié doté d'une horloge atomique. Le serveur de synchronisation utilise son horloge locale pour conserver son heure lorsqu'il reçoit des mises à jour d'une source distante (récepteur GPS ou DCF, par exemple). La précision de l'horloge interne et le temps de réponse aux requêtes NTP peuvent avoir une incidence sur la précision globale du système. Un PC Windows agissant en tant que serveur NTP limite en général la précision du système à $\sim \pm 30$ ms, tandis qu'un serveur NTP dédié doté d'un récepteur GPS a une précision supérieure à 1 ms.

Ce service est plus performant que les anciens systèmes de synchronisation horaire car il ne requiert qu'une simple connexion. Avec les anciens systèmes, chaque équipement devait être équipé d'un récepteur GPS ou DCF, ce qui se traduisait par des coûts plus élevés et un positionnement difficile des antennes.

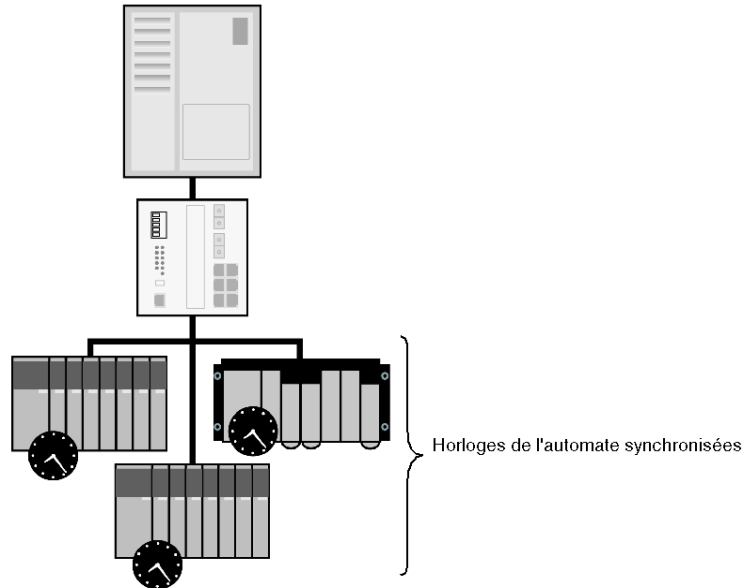
Lorsqu'une UC agissant en tant que client demande une mise à jour de l'heure, le module Ethernet obtient cette information auprès du serveur et met à jour l'horloge interne de l'UC. Cette horloge interne fonctionne désormais comme l'horloge locale de l'automate jusqu'à la prochaine mise à jour. Il est possible d'accéder à cette horloge à tout moment dans la logique utilisateur, via un bloc fonction élémentaire spécifique.



Applications de synchronisation horaire

Fonctions utilisant la synchronisation horaire

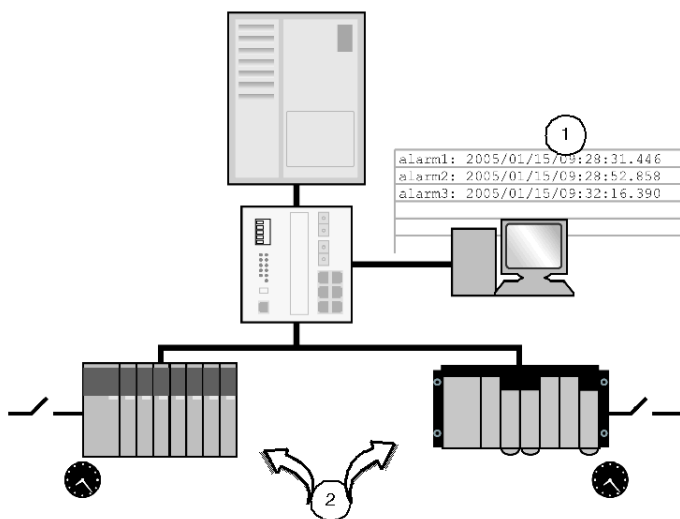
La synchronisation horaire donne à tous les équipements du réseau la même référence horaire. Ce service prend en charge, sur la base d'une heure identique, l'horodatage des événements, les alarmes et les modifications de programme ou de fichier dans l'usine.



Enregistrement de la chronologie des événements

Pour horodater des événements, l'automate doit être capable de détecter un événement lorsqu'il se produit au niveau du module d'E/S. Pour ce faire, choisissez un module avec des paramètres de filtrage et des temps de réponse minimum. Si possible, associez le module d'entrée à une tâche d'événement dans l'UC (fonction prise en charge sur les UC avancées). L'événement qui se produit sur site est détecté par le module et appelle la tâche d'événement, interrompant ainsi le programme et permettant au code d'application d'horodater l'entrée.

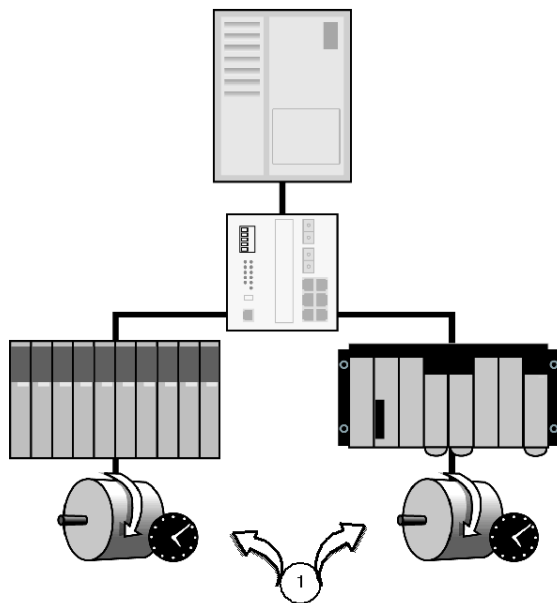
Si l'UC ne prend pas en charge la mise en œuvre des tâches d'événement, la *tâche rapide* doit être utilisée. Configurez la tâche rapide de manière à ce qu'elle soit exécutée aussi souvent que possible. Contrairement à la tâche d'événement, la tâche rapide interrompt l'exécution du programme principal pour rechercher des événements. La fréquence d'exécution de la tâche rapide doit être configurée de telle sorte qu'elle n'ait pas d'impact majeur sur la durée d'exécution du programme principal. Le module d'E/S contenant l'événement en entrée doit être associé à la tâche rapide ; les premières actions de la tâche rapide doivent consister à vérifier l'entrée du module d'E/S et à horodater cette entrée si elle représente un événement enregistrable.



- 1 Comparaison des heures des événements dans l'usine pour déterminer l'ordre des événements
- 2 Horodatage local des événements

Synchronisation des actions

Le service de synchronisation horaire peut synchroniser l'activation d'événements dans une ou plusieurs usines. Utilisez la tâche rapide pour vous assurer que l'heure courante est définie de façon identique à celle à laquelle l'événement doit se produire. Si l'heure est correcte, la sortie doit être activée. La précision est altérée par la fréquence de la tâche rapide, par la longueur de son exécution (car la sortie n'est pas activée avant la fin de la tâche rapide), ainsi que par le temps d'activation des E/S. Le module d'E/S contenant la sortie de l'événement doit être associé à la tâche rapide.



1 Actions synchronisées dans l'usine

Comparaison avec les systèmes classiques d'enregistrement des événements

Les principales différences entre un service de synchronisation horaire et un système classique d'enregistrement de la chronologie des événements sont le coût et la précision. Un système classique affiche une précision d'1 ms, mais s'avère plus coûteux qu'un système d'automate mettant en œuvre le service de synchronisation horaire.

Toute différence au niveau de la précision est due aux modules d'E/S utilisés. Un système classique d'enregistrement de la chronologie des événements utilise des modules d'E/S dédiés avec des systèmes spéciaux de filtrage. Le module d'E/S procède à l'horodatage de l'entrée dès que cette dernière survient et commence à la filtrer. Si l'entrée est déterminée comme étant bruyante, l'événement est supprimé des enregistrements.

Le service de synchronisation horaire repose sur des modules automatés d'E/S normaux qui filtrent l'entrée avant de la transmettre à l'UC comme un événement et de l'enregistrer via un horodatage. Cette méthode de filtrage avant l'enregistrement se traduit par une précision moindre, mais elle réduit les coûts car aucun module spécial d'E/S n'est requis.

L'avantage financier vient du fait que l'heure est fournie via un réseau Ethernet existant. Dans un système classique, un récepteur GPS ou DCF doit être connecté directement à chaque module d'E/S. Un système faisant appel à plusieurs récepteurs est bien plus coûteux qu'un simple récepteur connecté à un serveur de synchronisation central NTP. Qui plus est, le premier système nécessite de positionner des antennes pour les équipements à l'extérieur de l'usine (les récepteurs GPS exigent une vue dégagée du ciel) et cette opération est difficile. En revanche, la configuration Ethernet ne nécessite qu'une simple antenne extérieure et utilise le réseau Ethernet existant de l'usine.

Equipements Schneider - mise en œuvre du service de synchronisation horaire

Les modules TSXETY5103 et 140NOE77111 sont les seuls modules Ethernet prenant en charge le protocole NTP. Comme l'indique le tableau suivant, la synchronisation de l'horloge (résolution) diffère selon l'UC utilisé avec ces modules.

Module Unity et processeur utilisés		Fonctionnement classique prévu du service horaire		
Modules Ethernet	Modules Ethernet avec processeur Unity	Synchronisation de l'horloge ¹	Synchronisation des événements	Horodatage ²
TSXETY5103*	TSXP570244M TSXP571x4M TSXP572x4M TSXP573x4M	+/-1 ms typique +/-10 ms maximum	= précision de la synchronisation de l'horloge + temps de la tâche rapide + temps d'E/S	= précision de la synchronisation de l'horloge + temps d'E/S
	TSXP574x4M TSXP575x4M	+/-1 ms typique +/-5 ms maximum		
140NOE 77111**	140CPU31110 140CPU43412U 140CPU53414U	+/-1 ms typique +/-10 ms maximum		
	140CPU65150 140CPU65160 140CPU67160	+/-1 ms typique +/-5 ms maximum		
¹ Décalage entre l'heure de l'entrée terrain et l'heure du serveur central.				
² En supposant que l'entrée est connectée au module d'interruption.				
* Les modules TSXETY5103 doivent être de la version 3.1 ou supérieure et sont compatibles avec Unity version 2.0 ou supérieure.				
** Les modules 140NOE77111 doivent être de la version 3.5 ou supérieure et sont compatibles avec Unity version 2.0 ou supérieure.				

3.7 Service de notification par message électronique

Vue d'ensemble

Cette section décrit le service de notification par message électronique et la manière dont il fournit aux utilisateurs des données de traitement, des rapports de production, des alarmes et des notifications d'événements.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Service de notification par message électronique	240
Fonctionnement du service de notification par message électronique	242
Equipements prenant en charge la notification par message électronique	244

Service de notification par message électronique

Résumé

Le service de notification par message électronique permet aux applications d'automate de signaler les conditions surveillées par l'automate, via un client de messagerie exécuté au sein d'un module de communication Ethernet. L'automate peut créer, de façon automatique et dynamique, des messages électroniques courts pour alerter les utilisateurs spécifiés concernant les :

- alarmes,
- événements,
- rapports de production,
- rappels de maintenance,
- mises à jour du statut de l'usine,
- autres informations relatives à l'usine.

Les destinataires peuvent être situés au niveau local ou distant.

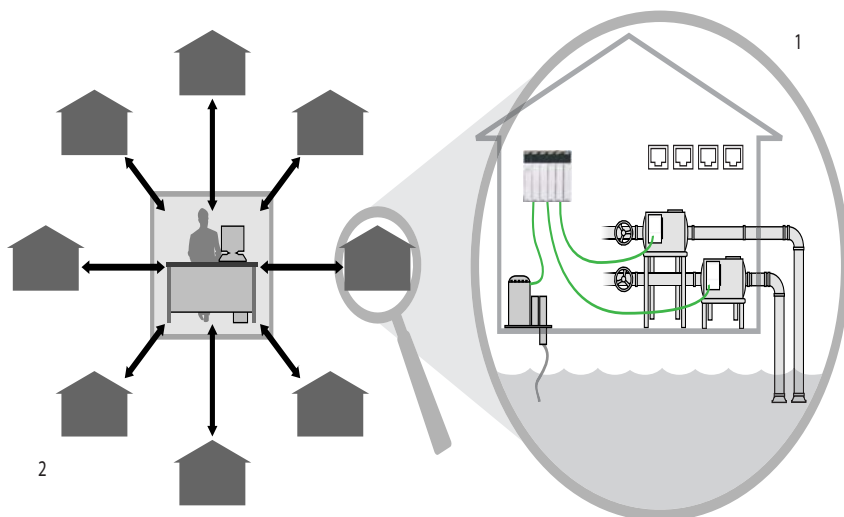
Ce service permet de créer des en-têtes de messages électroniques prédéfinis (incluant les noms et adresses électroniques des destinataires, ainsi que l'objet du message) à utiliser avec différents corps de messages électroniques. Certains équipements vous permettent d'ajouter des valeurs obtenues de façon dynamique à partir des informations les plus récentes de l'application de l'automate ou de l'état de la machine. D'autres n'autorisent que les messages prédéfinis. Il est possible de créer plusieurs messages électroniques pour décrire différents événements ou alarmes, notamment plusieurs variables système. Cette option peut être modifiée par un administrateur autorisé.

NOTE : Les messages doivent être traités via un système de messagerie électronique, ce qui explique que parfois, l'heure d'envoi du message et l'heure de sa réception diffèrent. Par conséquent, ce service ne doit être utilisé que pour une notification non critique.

Exemple d'application

De nombreux bâtiments industriels sont raccordés à plusieurs stations de pompage distantes pour leur alimentation en eau. Ces stations contiennent des pompes, des vannes et des filtres qui requièrent une maintenance préventive régulière basée sur le nombre d'heures de fonctionnement. Les dates de maintenance peuvent changer d'un mois sur l'autre selon l'utilisation qui est faite des pompes, des filtres ou des vannes. La notification par message électronique à l'équipe de maintenance lorsque les limites de maintenance sont atteintes évite de se déplacer pour aller vérifier une station de pompage distante.

Par exemple, l'un des filtres de pompage a été utilisé pendant 1 000 heures sur une période de 3 mois, sans nettoyage ni remplacement. Il requiert maintenant une maintenance préventive. Le système étant configuré pour déclencher une demande de maintenance toutes les 1 000 heures de fonctionnement, une alarme est envoyée par le module Ethernet au serveur de messagerie pour signaler à l'équipe de maintenance qu'elle doit nettoyer ou remplacer le filtre dans la station de pompage. Lorsque le serveur de messagerie a traité le message et l'a envoyé au réseau de l'entreprise, l'équipe de maintenance reçoit la notification par message électronique. Si le serveur de messagerie est configuré pour envoyer des messages à des pageurs ou à des téléphones mobiles, une notification supplémentaire peut être envoyée à l'équipe de maintenance par ces moyens de communication.

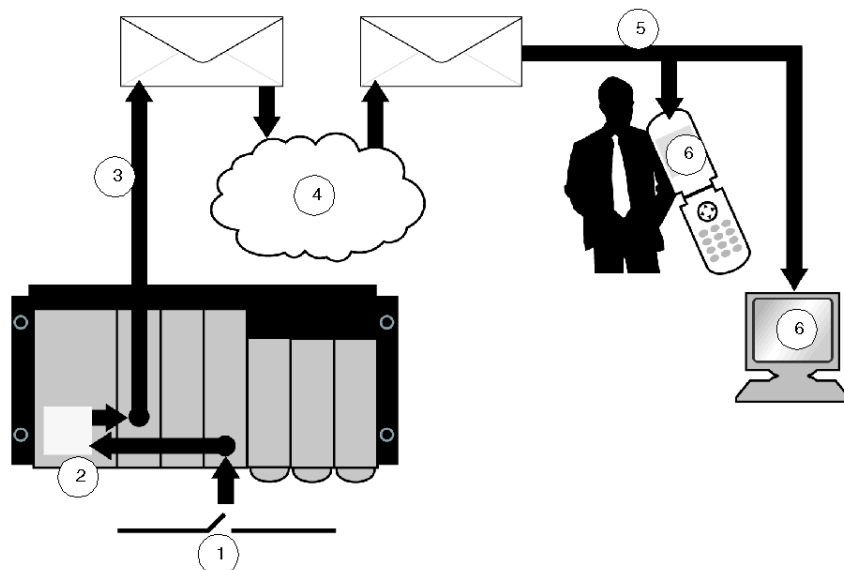


- 1 Envoi de la notification par message électronique concernant les heures de fonctionnement de la pompe
- 2 Plusieurs sites indiquent l'opération de maintenance au sous-traitant via un message électronique

Fonctionnement du service de notification par message électronique

Fonctionnement du service

Le service de notification par message électronique est mis en œuvre à l'intérieur d'un module de communication Ethernet qui sert de client de messagerie. Lorsqu'une alarme ou un événement préconfiguré est déclenché dans l'automate, le module Ethernet utilise le protocole SMTP (sur le port TCP numéro 25) pour communiquer avec un serveur de messagerie. Ce serveur est connecté au réseau de l'usine ou à Internet, permettant ainsi au message électronique d'atteindre ses destinataires. Il est également possible d'envoyer des messages électroniques ou des SMS (Short Message Service, Service de message court) à des téléphones mobiles, lorsque le serveur de messagerie du client prend en charge ces fonctions.



- 1 Événement en entrée
- 2 Message électronique déclenché
- 3 Message électronique envoyé au serveur de messagerie
- 4 Internet ou système de messagerie
- 5 Serveur de messagerie local
- 6 Message électronique affiché

Bien que les notifications soient envoyées automatiquement après le déclenchement d'un événement ou d'une alarme, le destinataire devra peut-être observer un temps d'attente significatif avant de recevoir le message. Le message est traité par un serveur de messagerie, envoyé par Internet ou un système de messagerie d'entreprise, traité de nouveau par un serveur de messagerie, puis parvient au destinataire par l'intermédiaire de son compte de messagerie. Une notification envoyée à un téléphone mobile n'est reçue que lorsque le téléphone est allumé et se trouve dans la zone de couverture. C'est la raison pour laquelle ce service ne doit être utilisé que pour les notifications non critiques, telles que les rappels de maintenance ou les rapports de production.

Sécurité

Un mot de passe de connexion facultatif, authentifié par le serveur de messagerie SMTP pour vérifier si le client est autorisé à envoyer des messages électroniques, peut protéger chaque message électronique. Pour configurer la protection par mot de passe, vous pouvez utiliser un sous-ensemble de l'extension de service SMTP pour l'authentification (RFC 2554). Cette extension permet au client de s'authentifier avant d'envoyer des messages. En outre, la méthode SASL (qui permet d'ajouter un système d'authentification aux protocoles nécessitant une connexion) inclut une commande pour identifier et authentifier un utilisateur auprès d'un serveur et éventuellement pour négocier la protection des interactions ultérieures via le protocole. Cette négociation se traduit par l'insertion d'une couche de sécurité entre le protocole et la connexion. Lorsqu'elle est activée, le nom de connexion et le mot de passe sont cryptés. Afin de renforcer la sécurité, l'installation de messagerie du site peut changer le numéro du port TCP (25 par défaut).

Exigences supplémentaires du service

Le service de notification ne fournit qu'un client de messagerie dans le module Ethernet. Le client envoie des notifications par message électronique. Pour que les destinataires puissent recevoir ces messages, le site dans lequel le module Ethernet est installé doit posséder un serveur de messagerie, tel que Lotus Notes, Microsoft Exchange ou Linux SendMail. Le client se connecte au serveur de messagerie pour envoyer le message à ses destinataires.

Equipements prenant en charge la notification par message électronique

Equipement		Fonction de sécurité	Nombre maximal d'en-têtes	Variables dans le corps du message	Contenu du corps du message dynamique
Premium	TSXP571634M (v3.1 ou ultérieure)	X	3	X	X
	TSXP572634M (v3.1 ou ultérieure)	X	3	X	X
	TSXP573634M (v3.1 ou ultérieure)	X	3	X	X
	TSXP574634M (v2.0 ou ultérieure)	X	3	X	X
	TSXP575634M (v2.0 ou ultérieure)	X	3	X	X
	TSXETY4103 (v3.1 ou ultérieure)	X	3	X	X
	TSXETY5103 (v3.1 ou ultérieure)	X	3	X	X
	TSXWMY100	-	100	X	-
Quantum	140CPU65150 (v2.0 ou ultérieure)	X	3	X	X
	140CPU65160 (v2.0 ou ultérieure)	X	3	X	X
	140NOE77101 (v3.5 ou ultérieure)	X	3	X	X
	140NOE77111 (v3.5 ou ultérieure)	X	3	X	X
	140NWM10000	-	100	X	-

3.8 Serveur Web standard

Vue d'ensemble

Cette section décrit un service utilisant un navigateur Web standard pour diagnostiquer et configurer des équipements Transparent Ready.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Services du serveur Web	246
Fonctionnement du serveur Web	248
Équipements prenant en charge les services de serveur Web standard	252

Services du serveur Web

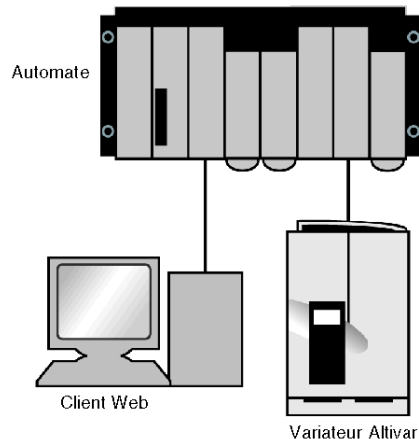
Récapitulatif

Des diagnostics intégrés permettent d'exécuter des fonctions de diagnostic et de maintenance. Ils peuvent être exécutés localement ou à distance par l'intermédiaire d'un simple navigateur Internet. Ce service utilise un serveur Web intégré et un serveur de données en temps réel. Toutes les données sont présentées au format HTML et sont accessibles au moyen de n'importe quel navigateur Internet. Ce service est très utile pour surveiller l'état des équipements du réseau et accéder aux informations relatives au fonctionnement et à la configuration.

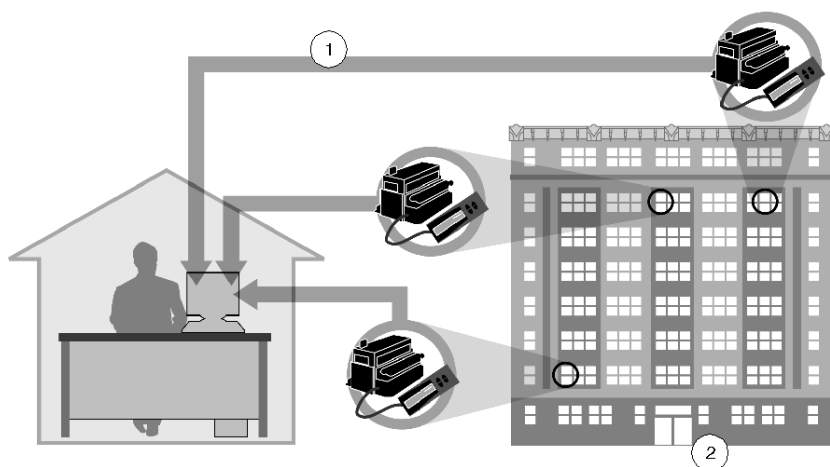
Le serveur Web intégré est un serveur de données d'automate en temps réel. Toutes les données de l'équipement, de diagnostic et de configuration sont affichées au format HTML en utilisant n'importe quel navigateur Internet et une machine virtuelle Java (JVM) pour prendre en charge le code Java intégré. Aucune programmation n'est nécessaire au niveau de l'équipement Transparent Ready ou du PC exécutant le navigateur Web.

Service Web et pages Web

Certains automates permettent la configuration distante via des pages Web. Par exemple, les variateurs Altivar donnent accès aux informations de vitesse actuelles et vous permettent de configurer les taux d'accélération par l'intermédiaire de leurs pages Web. Le client peut ensuite accéder aux pages Web du variateur Altivar.



Une autre application surveille l'utilisation de l'alimentation dans des immeubles d'habitation. Si des contrôleurs de circuit Power Logic sont installés sur différents disjoncteurs dans l'immeuble, un administrateur peut surveiller à distance l'utilisation de l'alimentation de chaque locataire en accédant simplement à la page Web du contrôleur de circuit Power Logic à l'aide d'un navigateur Web. Le fait de ne pas devoir se rendre physiquement auprès de chaque dispositif de mesure économise une quantité considérable de temps et de ressources.



- 1 accès distant aux dispositifs de mesure de puissance sur le réseau Ethernet de l'immeuble
- 2 immeuble de bureaux configuré pour une mesure de puissance séparée pour chaque locataire

Fonctionnement du serveur Web

Récapitulatif

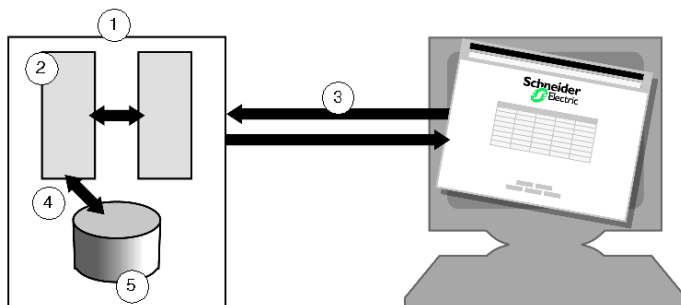
Lorsqu'un client HTTP accède au serveur Web, l'application reçoit la requête et récupère les données requises sur la mémoire de l'équipement. Les informations sont renvoyées au client sous la forme d'une page Web. Le serveur Web est un service passif ; il fonctionne uniquement lorsque des informations lui sont demandées. Les pages Web sont au format HTML ; elles sont stockées sur le serveur Web en même temps que d'autres fichiers source de données comme PDF, JPG, etc. Certains serveurs Web peuvent afficher des données en temps réel, mais une machine virtuelle Java JVM doit être installée pour permettre au client d'afficher ces pages Web.

Lorsque vous tentez d'accéder à une page Web, le navigateur Web émet une requête auprès du serveur. Une fois que le serveur a traité la requête, il renvoie les pages HTML au client. On distingue deux types de pages Web :

- des pages statiques, qui peuvent contenir ou non des données en temps réel. Si vous souhaitez actualiser des données en temps réel, vous devez préalablement recharger les pages Web, ce qui implique l'envoi d'une autre requête.
- des pages dynamiques, qui contiennent des données en temps réel. Ces pages Web contiennent des applets Java qui sont exécutées sur la JVM du client, récupèrent les données en temps réel sur le serveur Web et affichent les données dans le navigateur Web.

Avec les pages statiques, telles que celles issues d'une passerelle EGX ou d'un écran de configuration NOE, le client doit actualiser la demande de page pour mettre les données à jour. Le serveur Web accède à la page HTML, obtient les données en temps réel, met à jour le fichier HTML, puis renvoie les informations au destinataire. Le client peut demander des mises à jour le cas échéant.

Avec les pages dynamiques, comme les statistiques Ethernet sur un module NOE, les mises à jour de données sont fournies par les applets Java. Le client qui demande les données doit être équipé d'une JVM en cours d'exécution. Lorsque vous accédez aux fichiers HTML, la partie statique du fichier HTML est téléchargée en même temps que les applets Java. Les applets Java exécutées dans la JVM du client émettent une requête Modbus pour que le dispositif obtienne les données en temps réel.



- 1 serveur http
- 2 page Web
- 3 requête d'une page Web
- 4 valeurs courantes des données dynamiques placées dans la page Web
- 5 mémoire de l'équipement

Pages Web courantes

Les pages Web les plus courantes sont les suivantes :

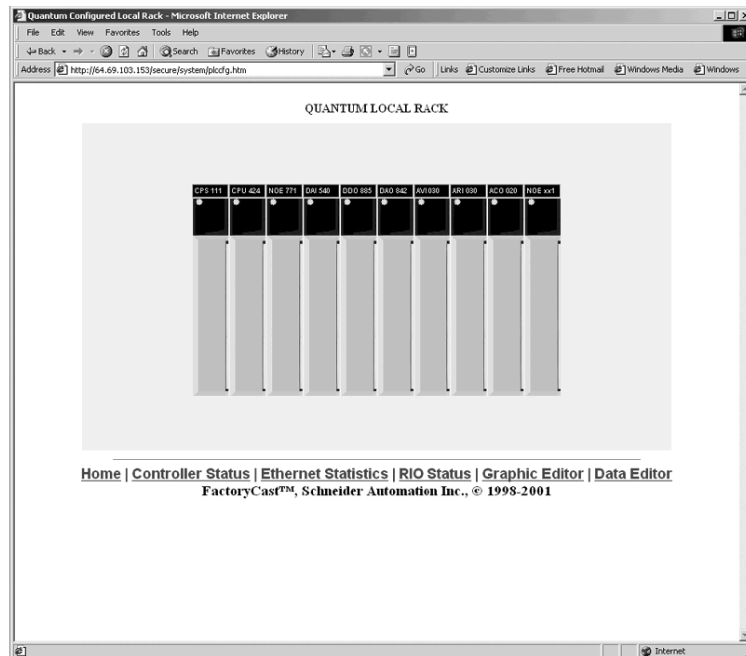
- visualisateurs du rack
- éditeurs de données
- affichages des statistiques Ethernet
- affichages des propriétés de l'équipement
- menus
- écrans de configuration de l'équipement
- affichages des diagnostics de l'équipement

Visualisateurs du rack

Un visualisateur du rack est pris en charge dans les modules TCP/IP Ethernet pour les plates-formes et les équipements suivants :

- TSX Micro
- Premium
- Quantum
- Momentum
- Advantys STB
- FactoryCast

Une page Web de visualisateur de rack typique ressemble à ceci :

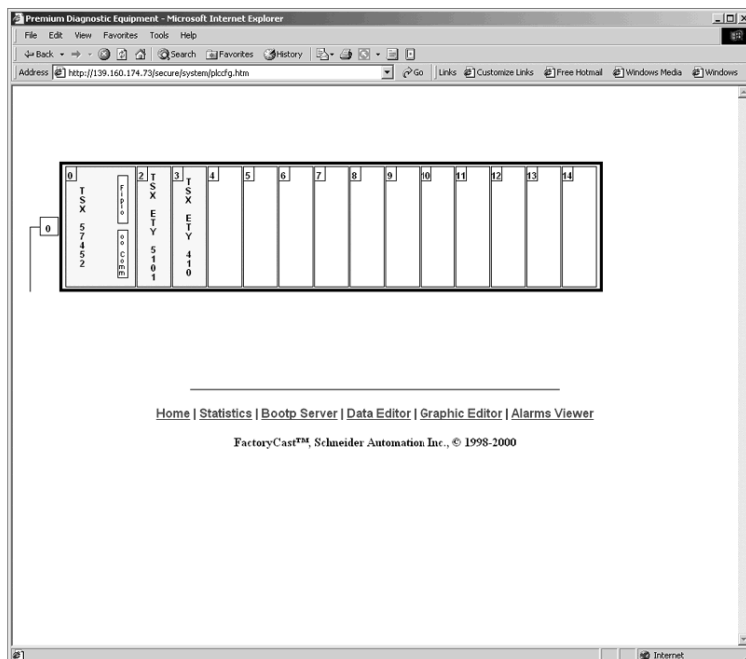


Editeurs de données

La fonction d'éditeur de données peut être utilisée pour créer des tableaux de variables animées pour l'accès en lecture/écriture en temps réel aux listes des données d'automate. Les variables à afficher peuvent être saisies et affichées symboliquement (S_Pump 234) ou à l'aide de leur adresse (%MW99).

Ces variables prennent en charge l'accès en écriture uniquement si cette option a été activée à l'aide du logiciel de configuration FactoryCast. Un deuxième mot de passe doit être saisi et validé lors de l'écriture d'une valeur dans une variable. Vous pouvez créer différentes tables d'animations contenant des variables d'application spécifiques à contrôler et modifier, et les enregistrer dans le module TCP/IP Ethernet.

L'illustration suivante présente un éditeur de données :



Statistiques Ethernet : Les statistiques Ethernet incluent les paramètres IP, le nombre de paquets transmis et reçus et toutes les erreurs au niveau de la couche Ethernet.

Propriétés de l'équipement : Les propriétés de l'équipement incluent la version courante du produit, le système d'exploitation et la version du microprogramme ou du noyau.

Menu : Les menus affichent les listes des pages disponibles sur un équipement.

Configuration de l'équipement : La configuration de l'équipement correspond aux configurations des services sur cet équipement.

Diagnostics de l'équipement : Les diagnostics de l'équipement correspondent aux diagnostics des services sur cet équipement.

Equipements prenant en charge les services de serveur Web standard

Produit		Référence
Quantum	Processeur	140CPU65150
		140CPU65160
	Modules	140NOE771001
		140NOE 77111
		140NWM10000
Premium	Processeur	TSXP572623M
		TSXP572823M
		TSXP573623M
		TSXP574823M
		TSXP571634M
		TSXP572634M
		TSXP573634M
		TSXP574634M
		TSXP575634M
	Module	TSXETZ4103
		TSXETY110WS
		TSXETY5103
		TSXWMY100
Micro TSX	Modules	TSXETZ410
		TSXETZ510
Momentum	Processeurs M1E	171CCC96020
		171CCC96030
		171 CCC 980 20
		171 CCC 980 30
	Modules	170 ENT 110 01
		170 ENT 110 02
Advantys STB		STBNIP2212
Altivar ATV 38/58		VW3 A58310
Passerelle Power Logic		EGX200
		EGX400

3.9 Serveur Web FactoryCast

Vue d'ensemble

Cette section explique comment utiliser le serveur Web FactoryCast pour contrôler et surveiller les opérations d'usine.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Serveur Web FactoryCast	254
Fonctionnement du serveur Web FactoryCast	256
Equipements prenant en charge les services de serveur Web FactoryCast	258

Serveur Web FactoryCast

Récapitulatif

Un serveur Web FactoryCast est une extension du serveur Web standard qui permet d'établir des diagnostics et de contrôler une usine via des pages Web personnalisées. Les fonctions disponibles sont les suivantes :

- gestion des alarmes d'équipement et d'usine avec acquittement total ou partiel (pages prêtes à l'emploi pour la fonction de visualisateur d'alarme) ;
- diagnostics graphiques d'usine (vues graphiques personnalisées, générées par l'utilisateur, avec la fonction d'édition de données graphiques) ;
- contrôle graphique d'usine via des pages Web animées, créées par l'utilisateur et stockées dans le module FactoryCast.

Les pages Web personnalisées sont transférées au module par le logiciel de configuration FactoryCast.

Hébergement et affichage de pages Web utilisateur

Les modules Web FactoryCast disposent d'une zone mémoire qui héberge les pages Web générées par les utilisateurs. Ces pages Web peuvent être créées grâce à des outils d'édition HTML standard comme Microsoft FrontPage et Macromedia Dreamweaver. Les applets Java liées à des variables d'automate permettent d'améliorer ces pages en affichant des représentations graphiques de l'état d'une usine. Ces objets animés sont fournis dans l'éditeur de données graphiques fourni avec FactoryCast.

Ces pages Web permettent d'effectuer les opérations suivantes :

- afficher et modifier des variables en temps réel ;
- créer des liens hypertexte vers d'autres serveurs Web externes.

L'éditeur de données graphiques vous permet de créer des écrans graphiques à plusieurs fins :

- affichage, surveillance et diagnostics ;
- génération de rapports de production en temps réel ;
- manuels de maintenance ;
- guides d'opérateur.

Logiciel de configuration des serveurs Web FactoryCast

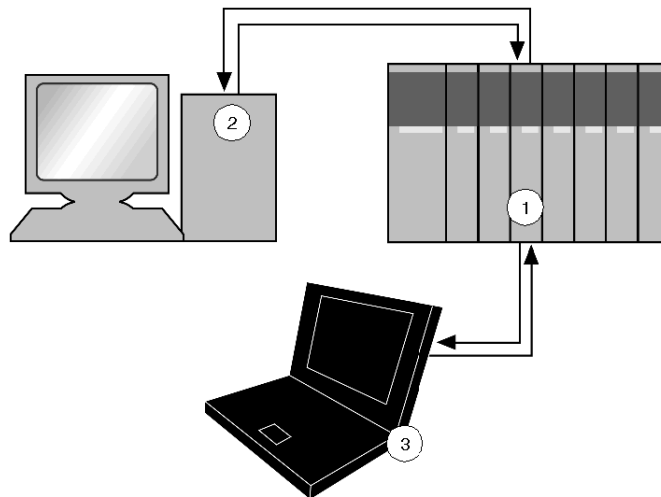
Le logiciel de configuration MS Windows des serveurs Web FactoryCast est fourni sur CD-ROM avec chaque module FactoryCast. Utilisez ce logiciel pour configurer et administrer le serveur Web intégré à ces modules. Il vous permet d'effectuer les opérations suivantes :

- gérer la sécurité d'accès ;
- définir les noms d'utilisateur et mots de passe permettant d'accéder aux pages Web ;
- définir l'accès aux variables modifiables ;
- enregistrer/restaurer un site Web ;
- transférer des pages Web créées localement vers ou à partir du module FactoryCast.

Utilisations du serveur Web FactoryCast

En configurant les diagnostics d'usine, vous créez des informations importantes qui sont immédiatement disponibles et vous les présentez dans le format de votre choix. Vous pouvez créer des pages Web qui contiennent des manuels, des procédures d'exploitation et des documents de référence utiles comme des dessins CAO.

Si les fichiers deviennent trop volumineux, vous pouvez les stocker sur plusieurs serveurs Web et ne conserver que les liens vers ces fichiers sur l'équipement FactoryCast. L'illustration suivante montre comment un serveur Web FactoryCast accède à des documents :



- 1 Module FactoryCast stockant des liens vers un serveur Web central.
- 2 Serveur Web central où les documents sont stockés.
- 3 Un client Web peut accéder aux documents souhaités, grâce au module FactoryCast.

Fonctionnement du serveur Web FactoryCast

Visualisateur d'alarme

Le visualisateur d'alarme est un système d'alarme prêt à l'emploi composé d'une page d'alarme protégée par mot de passe (visible dans un navigateur Web) et de blocs fonction à l'intérieur de l'équipement (utilisés pour ajouter des alarmes au système d'alarme). Le tampon de diagnostic de l'équipement est la source des alarmes sur la page Web. Ce système peut être utilisé :

- pour traiter les alarmes de l'équipement (affichage, accusé de réception et suppression) que le système est capable de gérer automatiquement ;
- par l'application de l'utilisateur qui se sert de blocs fonction élémentaires (EFB) pour le diagnostic.

Le visualisateur d'alarme est une page Web contenant les informations suivantes pour chaque alarme :

- son état,
- le type d'EFB associé,
- sa zone géographique,
- les dates et heures de l'occurrence/la correction d'une panne.

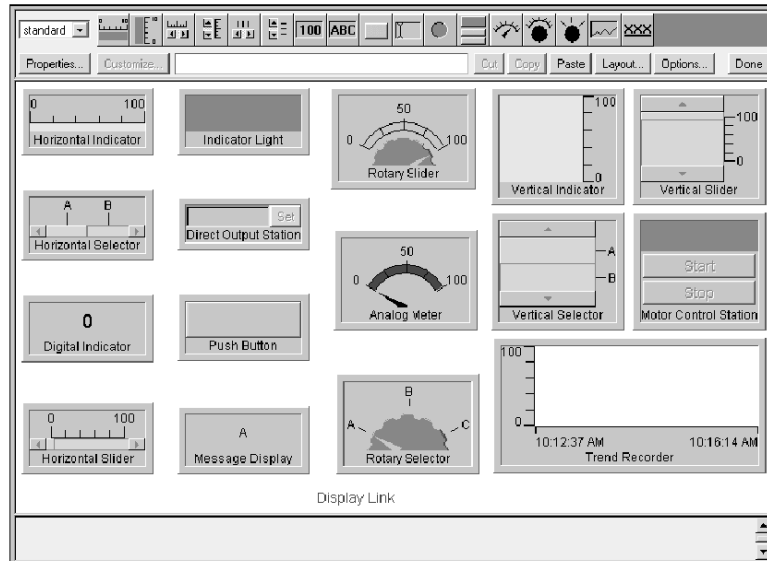
Editeur de données graphiques

L'éditeur de données graphiques permet de créer des écrans personnalisés affichant des données animées de l'usine. Ces vues sont créées dans un outil de type Web (accessible à partir de l'équipement FactoryCast) en utilisant une bibliothèque d'objets graphiques. Il est possible de personnaliser les objets à l'aide de couleurs, de variables d'automate à afficher, d'étiquettes, etc. Les objets graphiques suivants sont fournis :

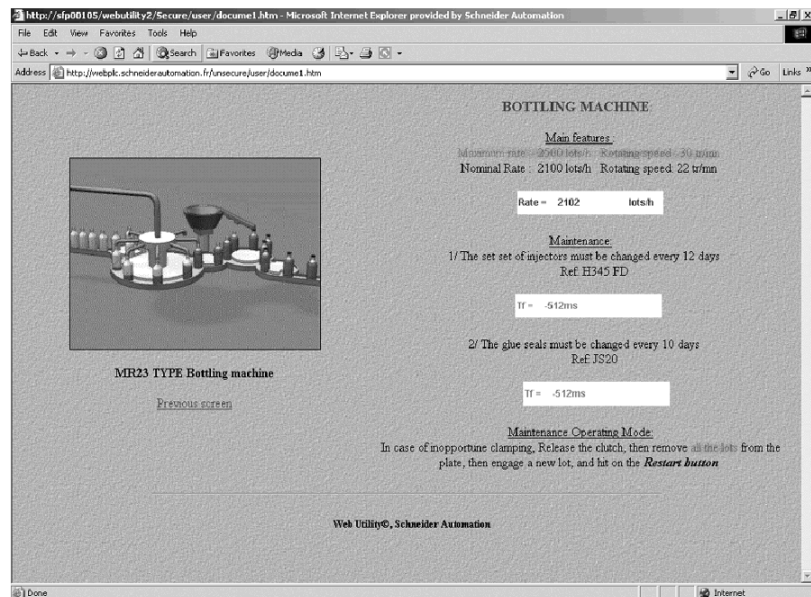
- Indicateurs analogiques et numériques
- Graphiques à barres horizontales et verticales
- Zones d'affichage des messages et de saisie des valeurs
- Zones pour boutons de commande
- Fonctions d'affichage des tendances

Une fois créés, les écrans peuvent être stockés dans l'équipement FactoryCast pour être utilisés ultérieurement ou être réutilisés dans des pages Web personnalisées.

L'illustration suivante présente certains des objets qu'il est possible d'inclure dans un écran graphique :



Un écran graphique terminé peut ressembler à ceci :



Equipements prenant en charge les services de serveur Web FactoryCast

Equipement	
Quantum	140NOE77111
	140NWM10000
Premium	TSXETY110WS
	TSXETY5103
	TSXWMY100
Micro	TSXETZ510

3.10 **Serveur Web FactoryCast HMI**

Vue d'ensemble

Cette section décrit le service Web FactoryCast HMI et explique comment l'utiliser pour le diagnostic et le contrôle de l'usine en temps réel.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Services Web FactoryCast HMI	260
Equipements prenant en charge le service Web HMI FactoryCast	265

Services Web FactoryCast HMI

Récapitulatif

Le serveur Web FactoryCast HMI étend les fonctions FactoryCast (*voir page 254*) en exécutant les fonctions Web IHM suivantes :

- Gestion de base de données IHM en temps réel (propre au module et indépendante du processeur de l'automate)
- Calculs arithmétiques et logiques pour le prétraitement des données sur l'IHM
- Transmission des messages électroniques déclenchés par un événement spécifique (par message électronique)
- Connexion au serveur SQL ainsi qu'aux bases de données relationnelles MySQL et Oracle pour archiver les données de suivi ou de consignation

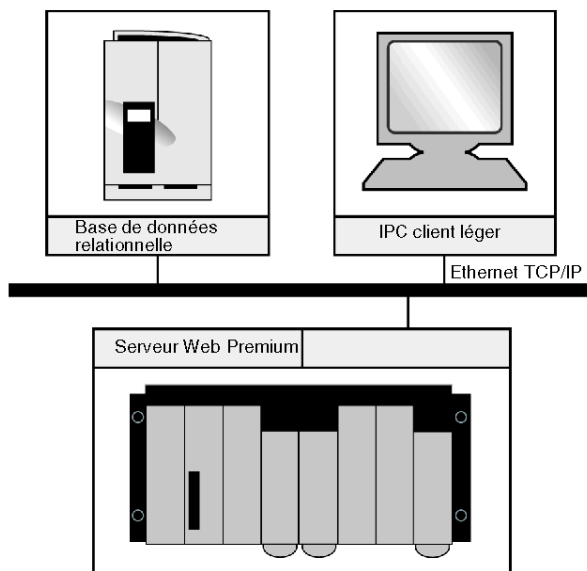
FactoryCast HMI est un serveur Web actif qui exécute des fonctions IHM intégrées dans un module automate. Le serveur Web actif évite la communication via l'interrogation pour mettre à jour la base de données IHM/SCADA.

Le logiciel FactoryCast HMI configure les services sur le module. Il suffit de configurer les paramètres de chaque service ; aucune programmation véritable n'est nécessaire. Le logiciel offre un mode de simulation pour tester l'application sans module FactoryCast HMI ni connexion physique à un automate, ce qui simplifie la mise au point.

Fonctionnement du service Web FactoryCast HMI

Bien que d'autres équipements Ethernet dotés d'un serveur Web intégré puissent fournir des données en temps réel, ils ne peuvent fournir des informations historiques ou exécuter des services Web, sauf si un client est connecté. Les équipements FactoryCast HMI intègrent une JVM. Un équipement FactoryCast HMI peut fournir des informations historiques de tendance et exécuter d'autres services Web tels que la consignment dans la base de données et l'envoi de messages électroniques.

L'illustration suivante présente le flux des données du service Web FactoryCast HMI :



Architecture

Les serveurs Web FactoryCast HMI peuvent être intégrés dans :

- des installations nécessitant des solutions IHM souples et économiques,
- des architectures hybrides qui complètent les systèmes SCADA conventionnels,
- des architectures au sein desquelles des liaisons directes sont requises entre les systèmes d'automatisation et les niveaux de gestion des informations (liaisons informatiques).

Solution Web IHM souple

Les équipements FactoryCast HMI remplacent les solutions IHM ou SCADA conventionnelles dans les architectures nécessitant un module IHM multistation souple. Un équipement FactoryCast HMI fournit une fonction de contrôle à distance temporaire sur Internet ou sur les réseaux d'entreprise. Les architectures types peuvent être constituées :

- de plusieurs automates sur un réseau Ethernet avec des modules serveur Web FactoryCast HMI,
- d'un ou de plusieurs clients avec une interface client léger équipée d'un simple navigateur Internet,
- d'une base de données relationnelle dans laquelle FactoryCast HMI peut archiver les données directement à partir du système d'automatisation.

Les modules FactoryCast HMI lisent les données de l'automate et exécutent les services IHM (messagerie électronique, calculs interprétés, connexions à des bases de données relationnelles, mise à jour de pages Web) à la source dans l'automate, sans affecter le programme de l'automate ni la durée du cycle du processeur.

Cette solution offre :

- une application IHM fiable exécutée à la source dans un automate,
- une interface multistation intégrée et un accès distant facile et économique à configurer (terminal client léger),
- une application IHM facile à gérer car elle réside dans un emplacement unique sur le serveur,
- une notification par message électronique pour assurer la maintenance préventive,
- un archivage des données directement à partir de la source de données.

Architecture hybrides

FactoryCast HMI complète les systèmes SCADA conventionnels. Le logiciel SCADA Vijeo Look ou Monitor Pro permet de centraliser les informations afin d'effectuer la supervision globale à partir d'un site central.

La combinaison d'une solution FactoryCast HMI et d'une solution SCADA conventionnelle permet :

- la simplification de l'application SCADA en situant une partie du traitement SCADA au niveau de la source,
- une disponibilité accrue pour suivre les données du fait de la connexion directe entre les modules FactoryCast HMI et les bases de données relationnelles,
- un diagnostic distant puissant prêt à l'emploi.

Liaisons directes et niveaux de gestion des informations

Dans les architectures hybrides, FactoryCast HMI évite les équipements intermédiaires (passerelles), dont l'installation et la gestion sont coûteuses. Il établit une liaison directe entre les niveaux d'automatisation et les niveaux globaux de gestion des informations (MES, ERP, etc.). L'automate archive les informations directement depuis le système d'automatisation dans des bases de données relationnelles, permettant ainsi à un système d'automatisation collaboratif de partager les données en temps réel. Cette solution se traduit par :

- des architectures simplifiées,
- des coûts réduits d'installation, de développement et de maintenance,
- une fiabilité accrue des données (du fait que les données sont collectées à la source),
- une plus grande disponibilité au niveau de l'archivage des données.

Base de données des balises IHM

Avec une architecture interne similaire à celle d'un système IHM/SCADA, les modules FactoryCast HMI gèrent leur propre base de données de variables en temps réel, indépendamment du programme de l'automate. Cette base de données de variables exécute différentes fonctions, notamment le traitement interne, l'archivage, les alarmes et la messagerie électronique. Ces variables sont mises à jour par le service d'acquisition de données du système d'automatisation. Ce service devient opérationnel lorsque les paramètres suivants ont été définis dans le logiciel FactoryCast HMI :

- Importation directe des bases de données de variables/symboles de l'automate (sans entrées en double)
- Définition de la fréquence d'acquisition (fréquence de mise à jour de la variable)

NOTE : Une application FactoryCast HMI exécutée dans un module Premium FactoryCast HMI configuré permet également d'accéder aux variables de l'automate distant dans l'architecture via un réseau transparent (protocoles transparents X-Way/Uni-TE).

Caractéristiques du service Web

Les services Web FactoryCast HMI acceptent :

- un maximum de 1 000 variables d'E/S provenant des automates par application,
- un maximum de 100 variables internes par application,
- une fréquence d'acquisition minimale de 500 ms.

Connexions aux bases de données relationnelles

Le module FactoryCast HMI peut être connecté directement aux bases de données relationnelles distantes suivantes :

- SQL Server
- MySQL
- Oracle

Cette connexion permet l'archivage de toutes les données internes ou de traitement, l'objectif étant de consigner et suivre ces données. Les données peuvent être archivées (écrites) périodiquement et/ou pour un événement spécifique. Ces variables peuvent être issues d'automates (bits d'E/S, bits internes, mots internes et registres) ou être locales dans le module.

La fonction de roulement de FactoryCast HMI sert à vérifier la taille des tables en gérant le nombre maximal d'enregistrements. Il s'agit d'une fonction circulaire d'archivage de données qui supprime automatiquement les données les plus anciennes. La fonction de roulement est accessible en définissant des paramètres dans le logiciel FactoryCast HMI.

Caractéristiques de la base de données

Les caractéristiques de la base de données sont les suivantes :

- Nombre de bases de données pouvant être connectées : 3
- Nombre de tables pouvant être écrites par base de données : 10 (maximum)
- Nombre de colonnes par table : 50 (maximum)
- Type de base de données prise en charge : Oracle, SQL Server et MySQL
- Création automatique de table : le serveur FactoryCast HMI crée automatiquement une table dans la base de données.

Fonctions de calcul

Le serveur FactoryCast HMI peut effectuer diverses opérations arithmétiques et logiques sur une combinaison de variables à partir de la base de données IHM, indépendamment du processeur de l'automate. Certains de ces calculs incluent la mise à l'échelle, le formatage et le traitement logique pour le déclenchement d'événement.

La fonction de calcul utilise un ensemble de feuilles de calcul avec des formules définies dans les cellules. Les feuilles de calcul sont interprétées et traitées par le serveur. Le résultat de chaque formule est associé à une nouvelle variable interne. Un déclenchement défini par l'utilisateur lance le traitement de chaque feuille de calcul.

Equipements prenant en charge le service Web HMI FactoryCast

Equipement	
Quantum	140NWM10000
Premium	TSXWMY100

3.11 Autres services

Vue d'ensemble

Cette section décrit d'autres services de prise en charge disponibles avec certains équipements Transparent Ready. Ces services sont des mises en œuvre des services d'infrastructure informatique standard pouvant être utilisés pour la maintenance et la surveillance du système.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Service FTP	267
Service SNMP	269
Service TFTP	271
Service Telnet	272
Autres services pris en charge par les équipements Quantum	274
Autres services pris en charge par les équipements Premium	275
Autres services pris en charge par les équipements TSX Micro	277
Autres services pris en charge par les équipements Momentum	277
Autres services pris en charge par les équipements Advantys STB	278
Autres services pris en charge par les passerelles/ponts Power Logic	278
Autres services pris en charge par les systèmes de câblage ConneXium	279

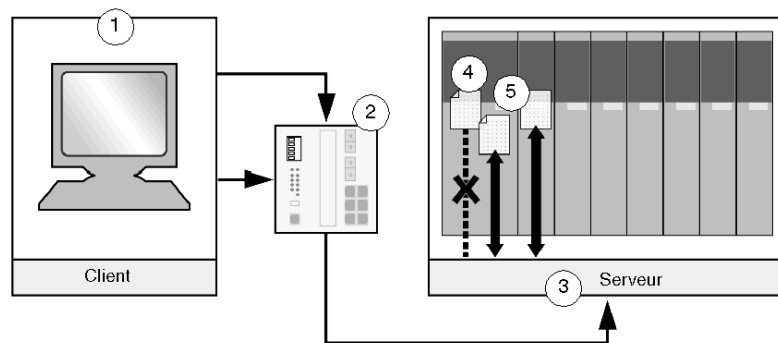
Service FTP

Récapitulatif du service FTP

FTP est un protocole client-serveur utilisé par de nombreux systèmes pour transférer des fichiers entre équipements. De nombreux équipements, comme les équipements Transparent Ready, mettent en œuvre le protocole FTP pour transférer des informations afin de charger un nouveau microprogramme, des pages Web personnalisées, etc.

FTP transporte et échange toutes les informations à l'aide de TCP. Par défaut, FTP utilise le numéro de port TCP 20 pour le transport des données et le numéro de port TCP 21 pour le contrôle. Le client initie une connexion FTP en se connectant au port de contrôle du serveur. Le serveur répond en reconnectant le port de données au client. Une fois les connexions établies, le transfert de fichiers peut avoir lieu.

Dans les équipements Transparent Ready, le protocole FTP peut être utilisé à différentes fins selon l'équipement. Par exemple, seuls le microprogramme et les pages Web personnalisées sont accessibles sur les UC Transparent Ready par le biais du serveur FTP. Il est impossible d'accéder aux fichiers programmes des UC.



- 1 un PC client FTP
- 2 un commutateur Ethernet
- 3 un automate avec des connexions au serveur FTP
- 4 un programme automate sans chemin d'accès au serveur FTP
- 5 Fichiers de pages Web HTML

Sécurité FTP

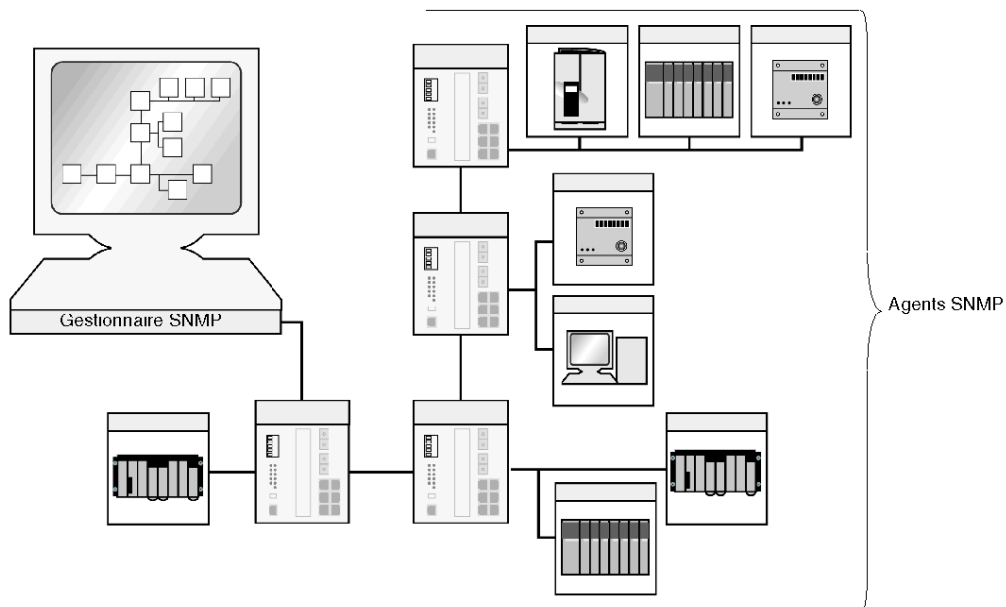
Le client doit fournir un nom d'utilisateur et un mot de passe pour lire ou écrire des fichiers sur le serveur. Cependant, la transmission de ces informations d'authentification s'effectue en texte simple ; il est donc possible de les obtenir en examinant le contenu des messages entre le client et le serveur.

La transmission des fichiers sur ou en dehors d'un réseau est une préoccupation majeure lorsque des pare-feux sont mis en place pour contrôler l'accès et le flux d'informations. Ce type de communication est donc bloqué sauf si le port FTP est ouvert dans le pare-feu. Pour plus d'informations sur l'ouverture des ports sur les pare-feux, reportez-vous à la documentation du pare-feu (*voir page 165*) ou contactez le service informatique de votre entreprise.

Service SNMP

Récapitulatif

Grâce au service SNMP, vous pouvez surveiller l'état du réseau et des équipements connectés au réseau. Ce service prend en charge la gestion de nombreux équipements de réseau divers à l'aide d'un système unique. Ce dernier comprend le système de gestion de réseau, le protocole SNMP et l'agent SNMP dans chaque équipement de réseau.



Le protocole SNMP est utilisé pour échanger des informations de gestion du réseau entre le gestionnaire de réseau ou le système de gestion (tel que HP Openview, IBM Netview, etc.) et les agents SNMP.

Fonctionnement du service SNMP

Les informations disponibles dans un équipement sont répertoriées dans une structure de données appelée *base d'informations de gestion* (MIB). Une base MIB contient des définitions de données des attributs de chaque objet géré par le réseau de manière à ce que le système de gestion puisse rassembler et combiner les informations à partir d'équipements multiples. Le service SNMP surveille l'état du réseau, modifie les configurations des équipements et génère des alarmes sur la base des défaillances de ces derniers.

De nombreuses MIB standard ont été développées (MIB-II, MIB du commutateur, etc.). Les équipements mettent en œuvre ces MIB pour offrir des informations standard à n'importe quel système de gestion de réseau. Selon la complexité de l'équipement, les fabricants peuvent choisir d'implémenter des MIB privées qui fournissent des informations supplémentaires concernant leur équipement.

Le protocole SNMP transporte et échange toutes les informations à l'aide du protocole UDP. La petite taille et la simplicité des paquets du protocole UDP réduisent la charge du réseau. En revanche, la surveillance prolongée peut augmenter la charge du réseau.

Sécurité SNMP

Depuis l'introduction du protocole SNMP, la protection des informations de gestion du réseau est devenue un enjeu de plus en plus important. Dans SNMPv1, les requêtes et les réponses sont envoyées en texte clair, exposant ainsi les variables aux pirates informatiques. Les auteurs des MIB ont découvert que certaines définitions de type de données nécessitaient plus de précision. SNMPv2 a choisi la solution d'améliorer l'authentification de l'origine du message, tout en protégeant ces messages contre leur divulgation, et de placer des contrôles d'accès sur la base de données MIB. Certains aspects sécuritaires restent néanmoins vulnérables. L'architecture SNMPv3 complète les spécifications SNMPv1 et v2 initiales avec des fonctionnalités de sécurité et d'administration supplémentaires.

Service TFTP

Récapitulatif du service TFTP

TFTP est un protocole client/serveur simple, utilisable en lieu et place du protocole FTP pour transférer des fichiers. Il utilise le numéro de port UDP 69 et est mis en œuvre au-dessus de la couche de transport UDP. Avec TFTP, la plupart des fonctions standard du protocole FTP sont supprimées. Il ne peut effectuer que des opérations de lecture et d'écriture sur un serveur distant, il ne peut pas dresser de listes de répertoires, et il n'offre aucune assurance au niveau de la sécurité et de l'authentification des utilisateurs. TFTP peut être mis en œuvre sur des équipements simples.

Pendant une connexion TFTP, les fichiers sont transférés entre le client et le serveur. Le destinataire confirme si la réception du fichier s'est effectuée sans erreur. Le protocole n'autorise toutefois pas la retransmission d'une partie erronée d'un fichier. C'est le fichier dans son intégralité qui doit être retransmis. Cela peut occasionner un retard dans la transmission. Toutefois, la probabilité d'erreurs dans le fichier suite à la transmission ou une perte de la transmission est relativement faible.

De la même manière que le service FTP des équipements Transparent Ready (*voir page 267*), l'utilisation de TFTP varie selon les équipements. Par exemple, sur un pont Modbus série-Modbus Ethernet, le microprogramme est transféré par TFTP, mais pas le fichier de configuration de l'équipement. Pour se connecter au serveur, un client est requis (WSFTP ou TFTP Windows, par exemple).

Service Telnet

Récapitulatif du service Telnet

Le protocole Telnet propose une session de communication textuelle interactive ou une interface utilisateur entre un client et un hôte. Les interfaces Telnet permettent d'effectuer des tâches comme la configuration d'équipements, les diagnostics et l'échange de fichiers.

Le protocole Telnet s'exécute sur la couche transport TCP via le port 23. Une session Telnet peut générer une quantité importante de trafic réseau, car chaque touche peut être envoyée comme un paquet TCP distinct.

Voici des exemples d'un écran de configuration et d'un écran de diagnostic du commutateur ConneXium Ethernet (499NES27100) :

System Parameter

148.218.112.101

Schneider Automation Ethernet Switch 10/100 Mbps

IP Address

: [148.218.112.101]

Subnet Mask

: [255.255.255.0]

Default Gateway

: [0.0.0.0]

VLAN ID (0=all)

: [0]

IP Configuration

: <LOCAL>

MAC Address

: 00:79:63:00:02:77

System Name

: Switch_Role_Name

Note:

Set IP-Configuration <LOCAL> to use manual settings.
APPLY changes the state if the objects immediately and
saves the state to Non Volatile Memory.

MAIN MENU APPLY

Enter Agent IP address in decimal dot format (e.g., 148.218.19.69)


```
Port Configuration/Statistics                                     148.218.112.101

                               Schneider Automation Ethernet Switch 10/100 Mbps

Port: 01      Port Name: [      ]
State: <Enable> Set Speed:  <autonegotiate>
Link: Up      Actual Speed: 100MFDX      Type: 10/100 TP

Port Statistics
Transmitted Packets: 277234
Received Packets: 1231027
Received Bytes: 154371683
Received Broadcasts: 917923
Received Multicasts: 183637
Received Fragments: 0
Detected CRCErrors: 0
Detected Collisions: 0

MAIN MENU  APPLY  REFRESH

Type in port number and press enter
```

Sécurité de Telnet

Le protocole Telnet demande un nom d'utilisateur et un mot de passe que le client doit saisir pour accéder à la session Telnet. Dans certains cas, les serveurs Telnet gèrent différents noms d'utilisateur/mots de passe permettant d'accéder à différentes options de configuration d'équipement. Cependant, la transmission de ces informations d'authentification s'effectue en texte simple. Il est donc possible de les obtenir en examinant le contenu du message.

Autres services pris en charge par les équipements Quantum

SNMP

Equipement	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
140CPU65150	X	-	-	X	X
140CPU65160	X	-	-	X	X
140NOE77101	X	-	-	X	X
140NOE77111	X	-	-	X	X
140NWM10000	X	-	-	X	X

FTP

Equipement	Micrologiciel	Fichiers Web	Sécurité	Support FDR
140CPU65150	X	X	X	X
140CPU65160	X	X	X	X
140NOE77101	X	X	X	X
140NOE77111	X	X	X	X
140NWM10000	X	X	X	-

TFTP

Equipement	Support FDR
140CPU65150	X
140CPU65160	X
140NOE77101	X
140NOE77111	X
140NWM10000	X

Telnet

Equipement	Configuration	Diagnostic ¹	Sécurité	Niveaux de sécurité
140CPU65150	-	X	X	X ²
140CPU65160	-	X	X	X ²
140NOE77101	-	X	X	X ²
140NOE77111	-	X	X	X ²
140NWM10000	-	X	X	X ²

¹ Pour utilisation en usine seulement

² Mots de passe multiples

Autres services pris en charge par les équipements Premium

SNMP

Equipement	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
TSXP571634M	X	-	-	X	X
TSXP572634M	X	-	-	X	X
TSXP573634M	X	-	-	X	X
TSXP574634M	X	-	-	X	X
TSXP575634M	X	-	-	X	X
TSXETY4103	X	-	-	X	X
TSXETY110WS	X	-	-	X	X
TSXETY5103	X	-	-	X	X
TSXWMY100	X	-	-	X	X

FTP

Equipement	Micrologiciel	Fichiers Web	Sécurité	Support FDR
TSXP571634M	X	X	X	X
TSXP572634M	X	X	X	X
TSXP573634M	X	X	X	X
TSXP574634M	X	X	X	X
TSXP575634M	X	X	X	X
TSXETY4103	X	X	X	X
TSXETY110WS	X	X	X	-
TSXETY5103	X	X	X	X
TSXWMY100	X	X	X	-

TFTP

Equipement	Support FDR
TSXP571634M	X
TSXP572634M	X
TSXP573634M	X
TSXP574634M	X
TSXP575634M	X
TSXETY4103	X
TSXETY110WS	X
TSXETY5103	X
TSXWMY100	X

Telnet

Equipement	Configuration	Diagnostic ¹	Sécurité	Niveaux de sécurité
TSXP571634M	-	X	X	X ²
TSXP572634M	-	X	X	X ²
TSXP573634M	-	X	X	X ²
TSXP574634M	-	X	X	X ²
TSXP575634M	-	X	X	X ²
TSXETY4103	-	X	X	X ²
TSXETY110WS	-	X	X	X ²
TSXETY5103	-	X	X	X ²
TSXWMY100	-	X	X	X ²
¹ Pour utilisation en usine seulement				
² Mots de passe multiples				

Autres services pris en charge par les équipements TSX Micro

FTP

Equipement	Micrologiciel	Fichiers Web	Sécurité	Support FDR
TSXETZ410	X	X	X	X
TSXETZ510	X	X	X	X

Autres services pris en charge par les équipements Momentum

SNMP

Equipement	MIB-II	TFprivate-MIB
170ENT11001	X	X

FTP

Equipement	Configuration	Fichiers Web	Sécurité
170ENT11001	X	X	X

Telnet

Equipement	Configuration	Diagnostic	Sécurité
171CCC96020	-	X	X
171CCC96030	-	X	X
171CCC98020	-	X	X
171CCC98030	-	X	X
170ENT11001	X	X	X

Autres services pris en charge par les équipements Advantys STB

SNMP

Equipement	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
STBNIP2212	X	-	-	X	X

FTP

Equipement	Configuration	Fichiers Web	Sécurité
STBNIP2212	X	X	X

Autres services pris en charge par les passerelles/ponts Power Logic

SNMP

Equipement	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
EGX 200	X	-	-	X	-
EGX 400	X	-	-	X	-

FTP

Equipement	Configuration	Fichiers Web	Sécurité
EGX 200	-	X	X
EGX 400	X	X	X

Autres services pris en charge par les systèmes de câblage ConneXium

SNMP

Equipement	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
499NES17100	X	-	-	X	X
499NOS17100	X	-	-	X	X
174CEV30020	X	-	-	X	-
174CEV20030	X	-	-	X	-
174CEV20040	X	-	-	X	-

FTP

Equipement	Configuration	Fichiers Web	Sécurité
174CEV20040	X	X	X

TFTP

Equipement	Configuration	Support FDR
499NES17100	-	-
174CEV30020	X	X
174CEV20030	X	X

Telnet

Equipement	Configuration	Diagnostic	Sécurité
174CEV30020	X	X	X
174CEV20030	X	X	X

3.12 OPC Factory Server

Vue d'ensemble

Cette section décrit le serveur OFS (OPC Factory Server) et fournit des exemples sur le mode de mise en œuvre de ces serveurs dans des systèmes Transparent Ready.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
OPC Factory Server	281
Services OFS	285
Performances OFS	288
Architecture d'exécution pour Unity/OFS/SCADA : un exemple simple	292
Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA non fréquemment modifiés	294
Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA nécessitant des modifications fréquentes	296
Architecture Build-time/Runtime pour système avec multiples connexions SCADA	298

OPC Factory Server

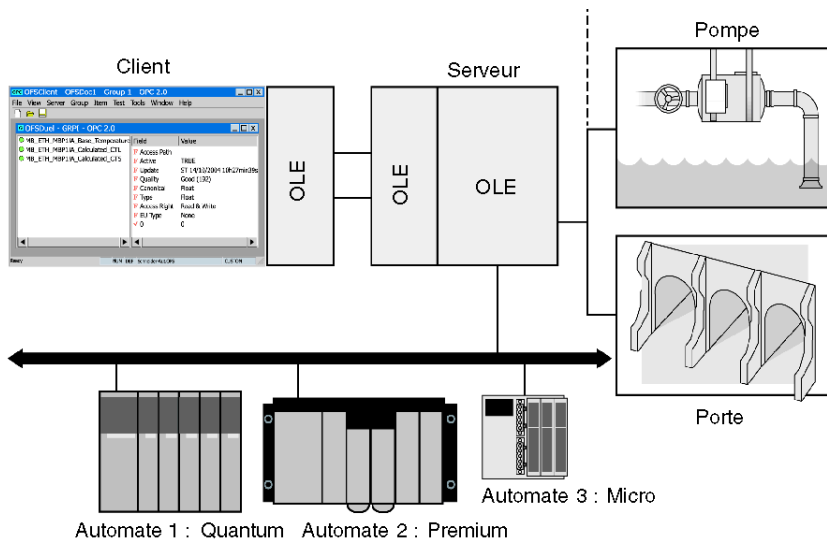
Récapitulatif

L'accès aux données OPC permet de déplacer des données en temps réel depuis des automates, des DCS et d'autres équipements de contrôle vers des clients d'affichage, tels que des panneaux IHM. La spécification OPC définit un ensemble standard d'objets, d'interfaces et de méthodes qui assure l'interopérabilité au niveau des applications de contrôle des processus et d'automatisation de la fabrication. Elle reposait à l'origine sur le modèle objet composant OLE de Microsoft et sur les technologies des modèles objet composant distribués.

OPC Factory Server (OFS) est un serveur de données multi-automate capable d'envoyer des données à des clients OPC et de communiquer avec des automates Compact, Micro, Momentum, Premium, Quantum, TSX Série 7 et TSX S1000. Le serveur OFS met à la disposition des applications clientes un groupe de services (appelé *méthodes*) pour accéder aux variables des systèmes de contrôle. OFS est un serveur OPC d'accès aux données des automates conforme aux normes OPC 1.0A et OPC 2.0. Il fonctionne avec n'importe quel client compatible OPC et avec deux types de logiciels OPC :

- le logiciel de supervision : le serveur OFS joue le rôle d'un pilote en assurant les communications avec tous les équipements Transparent Ready ;
- le logiciel de supervision personnalisé, via l'interface d'automatisation OLE ou l'interface personnalisée OLE.

L'illustration suivante présente une interface OFS :



Le serveur OFS assure l'interface entre les automates Schneider Electric et une ou plusieurs applications clientes dans lesquelles il est possible d'afficher et/ou de modifier certaines valeurs des équipements.

Fonctionnalités du serveur OFS

Le serveur OFS prend en charge :

- plusieurs équipements,
- plusieurs protocoles de communication,
- plusieurs clients,
- l'accès aux équipements et aux variables par le biais d'adresses ou de symboles,
- l'accès au serveur en mode local ou distant,
- un mécanisme de notification qui permet de transmettre des valeurs au client uniquement lorsque celles-ci changent d'état,
- la détection automatique de la taille des requêtes réseau en fonction du type d'équipement,
- la disponibilité des services via les interfaces d'automatisation OLE et personnalisée OLE,
- la compatibilité avec les normes OPC Data Access, versions 1.0A et 2.0.

Modes d'échange de données

Le serveur OFS gère deux modes d'échange des données avec l'automate :

- mode classique par défaut (interrogation),
- mode *Push data*, dans lequel les données sont envoyées sur l'initiative de l'automate.

Le mode Push data est recommandé lorsque les changements d'état sont rares.

Services OFS

Le serveur OFS offre les services suivants :

- lecture et écriture de variables dans un ou plusieurs automates présents sur un ou plusieurs réseaux,
- outil de configuration convivial qui décrit les paramètres nécessaires pour que le serveur fonctionne efficacement,
- outil permettant la modification en ligne des paramètres pour accroître la souplesse d'utilisation,
- possibilité d'utiliser une liste de symboles pour l'application de l'automate,
- interface de navigation qui présente graphiquement les équipements accessibles et leurs symboles,
- liste des éléments spécifiques dépendant d'un équipement, qui permet l'exécution de fonctions telles que le contrôle d'état, le démarrage/l'arrêt de l'automate et la supervision des alarmes.

Communication avec l'automate

Le serveur OFS fonctionne avec les gammes d'automates Quantum, Premium, Micro, Momentum, Compact, Série 7 et S1000 sur les réseaux suivants :

- Liaison série Modbus (RTU)
- TCP/IP (adressage IP ou X-Way)
- Modbus Plus
- Uni-Telway
- Fipway
- Ethway
- ISAway
- PCIway
- USB

Le serveur OFS est compatible avec l'automate Nano sur un réseau Uni-Telway, avec les restrictions suivantes :

- opérations de lecture uniquement,
- accès à un mot unique ou à x bits parmi 16 bits consécutifs.

Le tableau suivant présente la compatibilité OFS 3.1 avec les équipements de la gamme Schneider Electric SA et les différents réseaux :

Réseau	Premium	Micro	Série 7	Série 1000
Ethway	TSXETY110 (Ethway)		TSXETH107 TSXETH200	ETH030
TCP/IP	TSXETY110 (TCP/IP) TSXETY410 (TCP/IP) Voie intégrée TSXETY510 (TCP/IP)	TSXETZ410 TSXETZ510		
Uni-Telway	Voie intégrée TSXFPP20	Voie intégrée TSX FPP20	TSX SCM22	
Fipway	TSXFPP20	PCMCIA TSXFPP20	TSXP7455 TSXFPP20	
ISAway	Bus ISA			
PCIway	Bus PCI			
Modbus	TSXSCP11		TSXSCM22	Cartes JB
Modbus Plus	TSXMBP100	TSXMBP100		
USB	Voie intégrée			

	Quantum	Momentum	Compact
TCP/IP	140NOE771 Voie intégrée	171CCC96030 171CCC98030	
Modbus	Voie intégrée	171CCC760 171CCC780	Voie intégrée
Modbus Plus	Voie intégrée		Voie intégrée
USB	Voie intégrée		

Définition du groupe d'éléments

Les services OFS sont tous basés sur le concept de groupe d'éléments. Un élément est une variable d'automate à laquelle il est possible d'accéder par une adresse ou par un symbole. Les groupes OFS possèdent les caractéristiques suivantes :

- Il est possible de définir plusieurs groupes.
- Un groupe peut inclure plusieurs équipements. Chaque élément d'un groupe peut avoir une adresse d'équipement différente.
- Un groupe inclut différents dispositifs et supports de communication. Chaque élément peut faire référence à un pilote de communication différent. Si un équipement est accessible par le biais de plusieurs supports de communication, il est possible de combiner des variables adressées via différents supports au sein d'un même groupe.
- Les éléments qui constituent un groupe peuvent être différents. Il est possible de combiner tous les types d'objets gérés par le serveur OFS, par exemple des mots, des mots doubles et des virgules flottantes, dans un même groupe.
- Tous les éléments du groupe ont la même vitesse de mise à jour et le même pourcentage de bande morte.

Services OFS

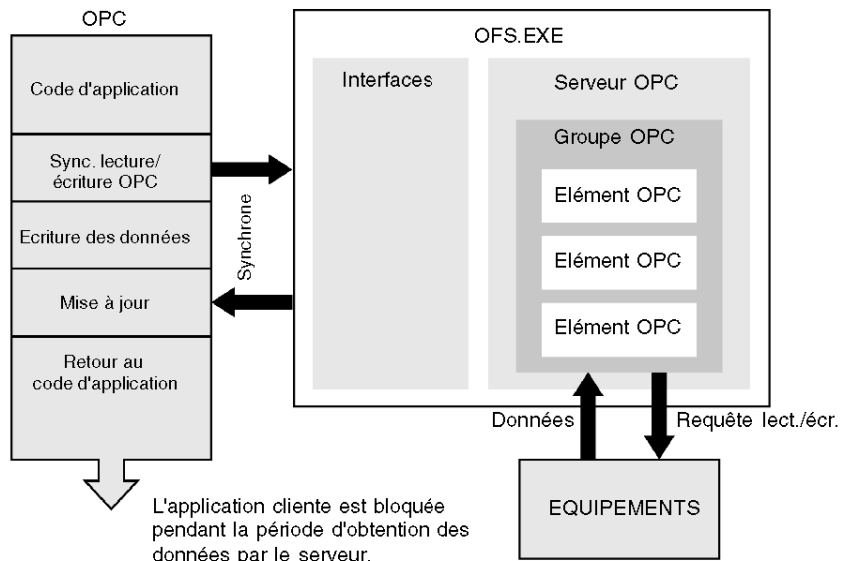
Services synchrones

Les services synchrones permettent de :

- lire et écrire partiellement ou complètement un groupe d'éléments ;
- scruter périodiquement les variables (interrogation en lecture) qui doivent être traitées par l'application cliente.

Le terme *synchrone* signifie que l'application cliente qui appelle un service en lecture ou en écriture est bloquée tant qu'elle n'a pas obtenu de résultat. L'instruction qui suit un appel de lecture ou d'écriture synchrone dans le code de l'application cliente est exécutée uniquement une fois que toutes les requêtes de communication correspondant à l'appel en question ont été traitées. Pendant une opération de lecture synchrone, OFS ne garantit pas que l'accès à toutes les variables d'un groupe se fera dans le même cycle de processeur si le groupe est transcrit sur plusieurs requêtes de communications. Un mécanisme OFS assure le nombre de requêtes nécessaire pour accéder à l'ensemble d'un groupe d'éléments (pour les groupes synchrones uniquement).

Les conditions qui permettent aux éléments d'un groupe d'être cohérents les uns avec les autres (lus ou écrits dans le même cycle de processeur) sont décrites dans le guide d'OPC Factory Server.



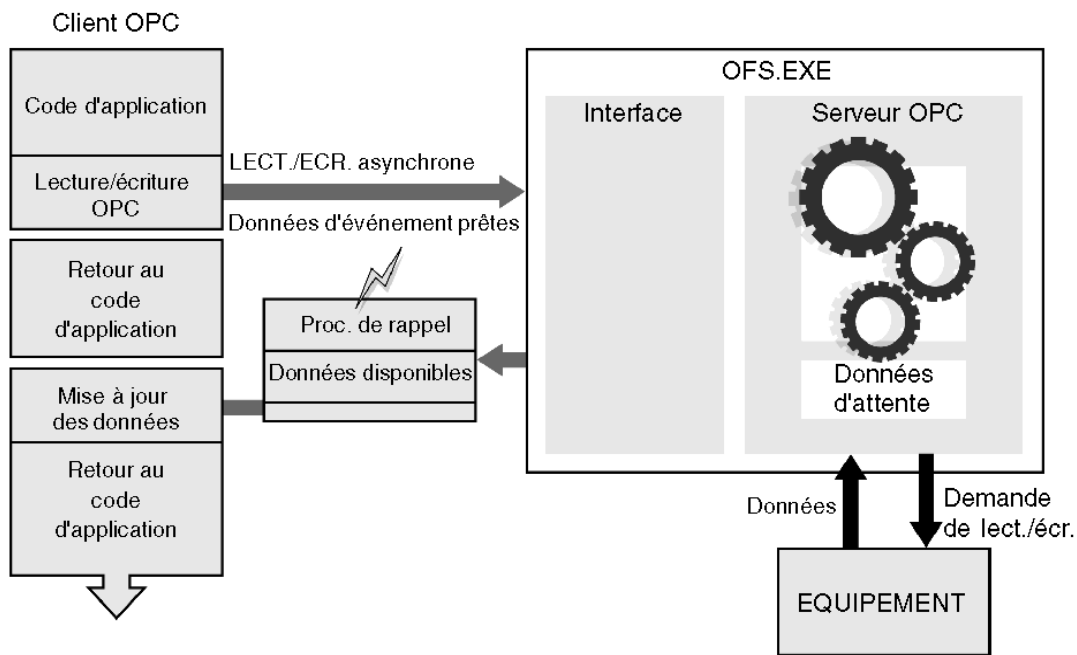
Services asynchrones

En mode asynchrone, toute requête de commande asynchrone reçoit une réponse immédiate. La commande demandée est soit refusée (réponse de code incorrect) soit en cours (réponse de code correct) ; elle n'est pas terminée.

La fin et le résultat de la commande sont annoncés via le mécanisme de notification. Celui-ci doit être activé avant de démarrer une commande asynchrone.

Les commandes Lecture, Ecriture, Actualiser et Annuler permettent de lire et écrire partiellement ou totalement un groupe d'éléments. L'application cliente doit scruter périodiquement l'évolution des variables (interrogation en lecture). Elle n'est pas bloquée pendant le temps nécessaire à l'obtention des données. Le mécanisme de notification activé annonce ensuite les résultats au client.

La synchronisation avec l'automate est identique au processus décrit pour les services synchrones.



Services de notification

OFS effectue une interrogation en lecture et une notification des changements dans les valeurs de variable. L'application cliente a besoin d'une fonction de réveil programmée intégrée. L'OFS doit appeler le réveil lorsque les valeurs des éléments changent dans les groupes examinés périodiquement.

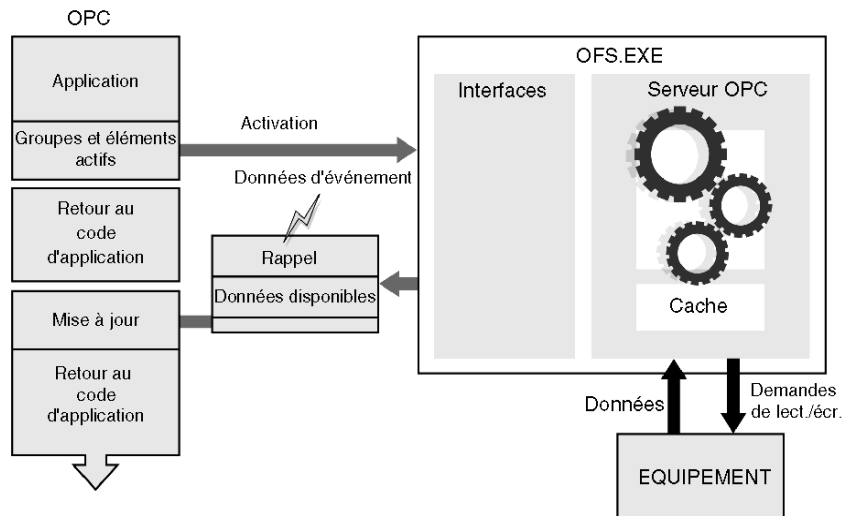
La fonction de réveil doit être unique dans l'application cliente. Elle reçoit toutes les notifications du serveur OFS, puis les redistribue vers les fonctions de traitement spécifiques de chaque groupe scruté périodiquement.

NOTE : Pour les logiciels de supervision prêts à être exécutés, la fonction de réveil doit être pré-programmée. Dans le cas contraire, n'utilisez pas le mécanisme de notification. La norme OPC OnDataChange définit le nom de cette fonction de réveil. Le serveur OFS notifie par groupe et non par élément individuel. Pour un groupe donné, le serveur OFS envoie à la fonction de réveil de l'application cliente une liste des éléments dont la valeur a changé. Dans le cas d'un élément de type table, le serveur OFS transmet l'ensemble de la table même si seul un sous-ensemble d'éléments a vu ses valeurs modifiées.

NOTE : Dans la fonction de réveil, les processus requérant un temps de traitement considérable par le processeur (par exemple, un affichage trop complexe) ne doivent pas être effectués. Ces types de processus peuvent nuire aux performances du système d'exploitation.

Les questions suivantes se rapportent au service de notification :

- L'affectation d'une période de scrutation à un groupe vous permet de scruter les variables d'automate à des périodes différentes. Vous pouvez par exemple afficher l'heure de l'automate chaque seconde et la température chaque minute.
- Affectez une bande morte à un groupe afin que les notifications soient filtrées lorsque les valeurs de variable de groupe changent. La notification survient si la modification des variables est supérieure à un certain pourcentage de leur valeur antérieure après la période de scrutation du groupe. Par exemple, l'application cliente est informée uniquement si la température varie de plus de 10 %.



NOTE : La bande morte est appliquée uniquement aux variables en virgule flottante ou en nombre entier afin que vous puissiez contrôler (ou limiter) le flux des notifications envoyées à l'application cliente et ainsi éviter de surcharger le système.

Performances OFS

Récapitulatif

La section suivante décrit les caractéristiques statiques du serveur OFS et définit certaines règles de génération et d'optimisation de requêtes réseau. L'objectif de ces règles est de minimiser autant que possible le nombre de requêtes.

Taille maximale d'une requête

Le tableau suivant spécifie le nombre maximal d'octets de données pouvant être compactés en une requête unique. Tous les éléments de données sollicités dans une même requête proviennent du même cycle d'automate et sont donc de taille homogène. Les octets de données indiqués dans le tableau peuvent être utilisés pour calculer le nombre d'éléments de même type pouvant être lus ou écrits dans une requête de communications d'automate. Un mot peut prendre jusqu'à 2 octets, un double mot 4 octets et un mot en virgule flottante 4 octets également.

Comptez 8 bits par octets sauf si vous effectuez la lecture avec un automate PL7 sur un réseau XWAY, auquel cas chaque octet compte 4 bits uniquement.

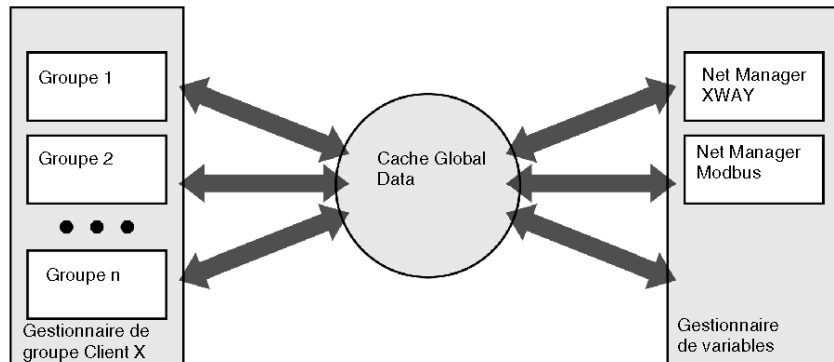
Par exemple, sur un automate PL7 s'exécutant sur XIP, 248%MB, 62%MD, 124%MW ou 992%M peuvent être lus et 244%MB, 61%MD, 122%MW ou 1960%M écrits dans une requête unique.

Le tableau suivant indique le nombre maximal d'octets de données pouvant être compactés dans une requête d'équipement Unity Pro.

Support de communication	Lecture	Ecriture
XIP	249	235
Voie intégrée XIP	256	242
TCP/IP	1022	1008
PCIway	224	210
USB	1022	1008
USB X-Way (USBX)	1020	1006
Fipway	123	109
Uni-Telway	241	227
Ethway	249	235
Modbus Plus	250	236
Modbus RTU	249	235

Utilisation des groupes

Le fait de séparer les éléments dans des groupes différents peut influencer sur la construction de requêtes réseau. Pour chaque équipement, les éléments sont répartis dans des ensembles indépendants si nécessaire. Néanmoins, ces ensembles ne sont pas déterminés par les groupes eux-mêmes, mais par la vitesse de mise jour minimale de groupe.



Les groupes n'influent pas sur la génération de requêtes réseau. En déclarant les éléments dans deux groupes différents avec la même vitesse de mise à jour, vous générez le même nombre de requêtes que si vous les déclariez dans un groupe unique.

Les requêtes sont générées par lots constitués d'éléments appartenant à des groupes avec la même période. Elles ne sont pas générées à l'intérieur d'un groupe.

Optimisation des requêtes

Chaque ensemble d'éléments est optimisé individuellement en fonction d'un équipement et d'une fréquence. Les algorithmes d'optimisation agissent en deux phases :

- **Le compactage** : regroupement des éléments de même type (avec des adresses semblables ou consécutives) dans des tables. Pour l'écriture, le regroupement est réalisé uniquement si les éléments sont strictement consécutifs. Obtenez une liste d'éléments à partir des éléments initiaux pour les envoyer à l'automate à des fins de lecture ou d'écriture. Sur les automates de la série 7, le compactage n'est pas réalisé sur les bits unitaires ; pour les tables de bits, il est effectué uniquement si le nombre de bits est un multiple de 8.
- **La concaténation** : construction des requêtes en optimisant les possibilités du protocole. Certains protocoles vous permettent de définir l'accès à différents types d'objets dans la même requête. Le serveur OFS ajuste automatiquement la taille des requêtes au maximum autorisé.

Les équipements Unity utilisent à la fois le compactage et la concaténation pour l'optimisation.

Les variables localisées ou non localisées dans le générateur de requêtes en lecture Modbus proposent une technique de mélange (*longueur du décalage du bloc de lecture*). Le générateur de requête en lecture peut mélanger n'importe quel type de variable dans une même requête ; une variable correspond à un identificateur à 6 octets. Le module NOE ne peut envoyer qu'une requête par cycle de processeur pour les variables non localisées et 4 requêtes par cycle de processeur pour les registres.

Par exemple, l'envoi d'une variable booléenne, de deux variables de nombre entier en virgule flottante et d'une structure avec cinq nombres entiers égalerait ou dépasserait une requête :

%MW2, %MW3, %MW40, %mX5, %MX8 => 1 requête avec 3 éléments
(MW2 ... 3, MW40, MWX5 ... 8)

Performances dynamiques

Les performances dynamiques du serveur OFS peuvent être mesurées grâce à plusieurs caractéristiques :

- Temps de réponse de la configuration
- Temps de réponse en lecture/écriture
- Volume des données échangées
- Sensibilité aux erreurs

Elles peuvent également être mesurées selon deux axes :

- Communication de l'OFS avec les équipements
- Communication de l'OFS avec les clients OPC

Dans certains cas, vous devez configurer différents paramètres d'OFS pour obtenir de meilleures performances : par exemple, si l'accès aux équipements se fait via différents types de réseau et si un réseau aux performances moindres est utilisé quelque part sur le chemin réseau. L'un des paramètres d'ajustement de serveur qui influe sur les performances de la communication de l'OFS avec les équipements est la fonction multivoie.

Reportez-vous au manuel d'OPC Factory Server pour plus d'informations sur la fenêtre de diagnostic, qui indique l'état du serveur et des communications.

Fonction multivoie

La plupart des protocoles de communication utilisés par l'OFS sont semi-duplex ; après l'envoi d'une requête, le serveur attend la réponse avant d'envoyer la requête suivante. Il existe une exception avec XWAY pour Unity ou les automates PL7. Avec les réseaux semi-duplex, la seule manière d'accélérer la communication consiste à ouvrir plusieurs voies entre l'émetteur et le récepteur. Vous pouvez ouvrir entre 1 et 16 voies pour chaque équipement et configurer ce nombre statiquement à l'aide de l'outil de configuration d'OFS ou dynamiquement avec le paramètre #MaxChannel spécifique.

La valeur qui offre les performances optimales dépend de l'automate sollicité (par ex. le nombre de requêtes qu'il peut traiter par cycle) et de la carte de communication utilisée (principalement sur les automates Concept). Pour obtenir ces données, reportez-vous à la documentation relative à l'automate et à la carte de communication.

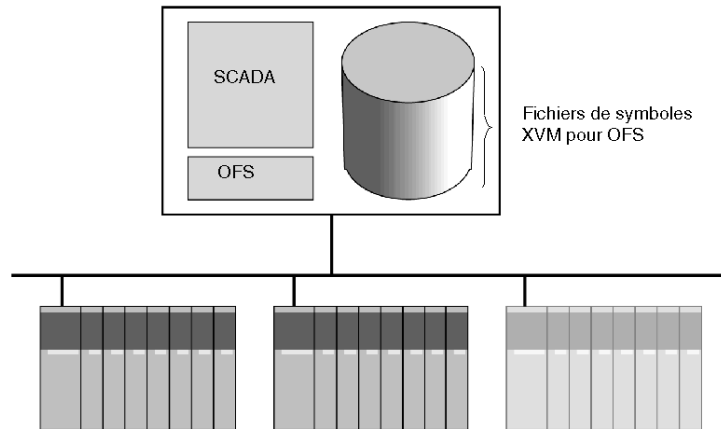
NOTE : La fonction multivoie n'est pas déterminante pour Unity Pro ou pour les automates PL7 utilisant un réseau XWAY (full duplex) et des pilotes série Modbus (voie simple uniquement) sur n'importe quel type d'automate.

Sur les réseaux semi-duplex, un paramètre peut être utilisé pour envoyer plusieurs requêtes simultanément à un équipement : plus la valeur est élevée, plus les performances de la communication avec l'équipement sont bonnes.

Architecture d'exécution pour Unity/OFS/SCADA : un exemple simple

Exemple d'architecture

L'exemple d'exécution suivant se rapporte à des architectures simples dans lesquelles l'application de l'automate n'a pas besoin de modifications en ligne.



VijeoLook constitue le meilleur choix pour ce type d'architecture. Seul un ordinateur est utilisé pour exécuter les logiciels SCADA et OFS, et le nombre maximal d'automates sur un système comme celui-ci est de cinq.

Options du système d'exécution

Sur Ethernet TCP/IP uniquement, vous pouvez affecter le fichier de symboles XVM sur un ordinateur différent de celui qui exécute les logiciels SCADA et OFS. Cette option vous permet de centraliser vos ressources sur un ordinateur autorisant les sauvegardes. Elle s'avère particulièrement utile lorsque le système est intégré dans une architecture plus vaste.

Caractéristiques clés du système

- Le système d'exécution requiert un fichier de symboles XVM Unity Pro compatible avec le serveur OFS. Ce fichier de symboles est exporté en mode Compilation par Unity Pro et doit être copié sur l'ordinateur utilisé pour exécuter le système. Un fichier de symboles est requis pour chaque application d'automate.
- Le système de fichiers SCADA + OFS + XVM est exécuté sur un seul ordinateur.
- OFS accède aux données de l'automate en temps réel. Toute différence détectée entre l'application exécutée et le fichier de symboles local sur l'ordinateur déclenche la vérification des signatures. Conformément au QoS pour OFS, la communication s'arrête ou bascule vers un service de mauvaise qualité. Vous devez donc mettre manuellement à jour l'ordinateur avec le fichier de symboles approprié pour que le fichier de symboles soit cohérent avec l'application exécutée dans l'automate.

Versions des produits

Produit	Version	Commentaires
Unity Pro M, L, XL	2.0	
VijeoLook	2.6	Inclut la version correcte d'OFS

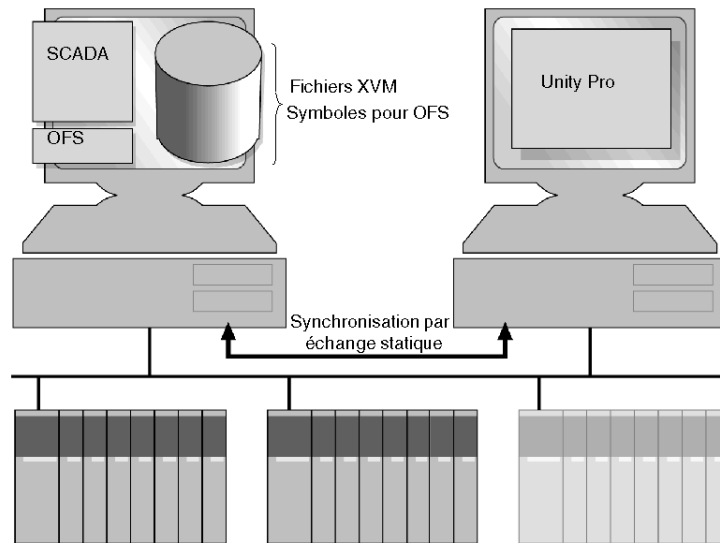
Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA non fréquemment modifiés

Exemple d'architecture

L'exemple de système build-time/runtime suivant gère des architectures :

- qui ne requièrent pas de modifications fréquentes de leur application ;
- qui ont une faible contrainte de synchronisation entre le système SCADA et l'application exécutée pendant les modifications.

La synchronisation entre la base de données Unity Pro et le système OFS est gérée manuellement, avec un échange statique du fichier de symboles.



En définissant VijeoLook comme système SCADA, jusqu'à 5 automates peuvent être pris en charge. Pour les configurations plus étendues, utilisez Monitor Pro. Un ordinateur est utilisé pour exécuter les logiciels SCADA et OFS et un autre pour exécuter Unity Pro sur les applications d'automate.

Option Build-time/Runtime

Sur TCP/IP Ethernet uniquement, vous pouvez stocker le fichier de symboles XVM sur un ordinateur différent de celui qui exécute les logiciels SCADA et OFS. Cette option vous permet de centraliser vos ressources sur un ordinateur autorisant les sauvegardes. Elle s'avère particulièrement utile lorsque le système est intégré dans une architecture plus vaste.

Caractéristiques clés du système

- Le système d'exécution requiert un fichier de symboles XVM Unity Pro compatible avec le serveur OFS. Ce fichier de symboles est exporté en mode Compilation par Unity Pro et doit être copié sur l'ordinateur utilisé pour exécuter le système. Un fichier de symboles est requis par application d'automate.
- Le système de fichiers SCADA + OFS + XVM est exécuté sur un seul ordinateur.
- Unity Pro est exécuté sur un ordinateur séparé pour les modifications d'application. Il n'est pas nécessaire que cet ordinateur soit connecté en permanence au réseau ; il peut être seulement connecté pour effectuer les modifications en ligne ou copier le fichier XVM sur le système OFS.
- OFS accède aux données de l'automate en temps réel. Toute différence détectée entre l'application exécutée et le fichier de symbole local sur l'ordinateur déclenche la vérification des signatures. Conformément au QoS pour OFS, la communication s'arrête ou bascule vers un service de mauvaise qualité. Vous devez donc mettre manuellement à jour l'ordinateur avec le fichier de symboles approprié pour que le fichier de symboles soit cohérent avec l'application exécutée dans l'automate.

Cette mise à jour peut être lancée par l'application SCADA via un mode de commande spécifique du serveur OFS. L'application continue de s'exécuter. Seule la communication OFS est interrompue pendant la mise à jour du fichier de symboles.

Versions des produits

Produit	Version	Commentaires
Unity Pro M, L, XL	v2.0	
VijeoLook	v2.6	Inclut la version correcte de OFS
MonitorPro	v7.2	Accès aux variables structurées non inclus

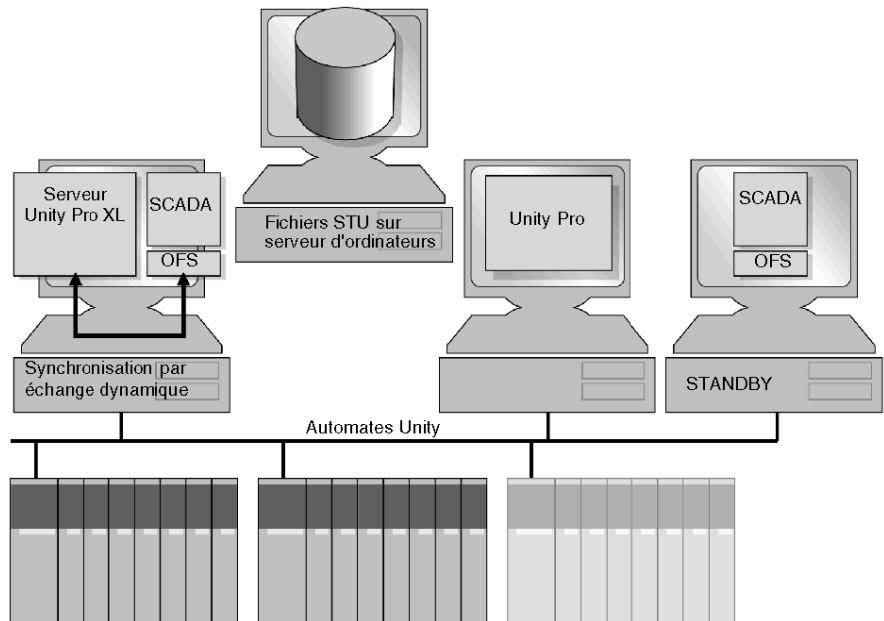
Architecture Build-time/Runtime pour les systèmes Unity/OFS/SCADA nécessitant des modifications fréquentes

Exemple d'architecture

L'exemple de système build-time/runtime suivant gère des architectures qui nécessitent :

- des modifications d'application fréquentes ;
- un niveau de service supérieur pour permettre la synchronisation entre le système SCADA et l'application exécutée pendant les modifications.

La synchronisation est gérée par le biais d'échanges dynamiques entre les systèmes OFS et Unity Pro XL. Aucune opération manuelle n'est requise pour mettre à jour le fichier de symboles pour OFS.



Un ordinateur est utilisé pour les systèmes SCADA, OFS et Unity Pro XL en mode serveur. Un deuxième ordinateur est utilisé pour exécuter Unity Pro et lancer les modifications d'application, ainsi qu'un troisième pour atteindre la redondance avec Monitor Pro. Le serveur d'ordinateurs dédié aux fichiers d'application STU assure la cohérence de l'accès depuis le système OFS/Unity Pro XL et Unity Pro vers la même application.

Options Build-time/Runtime

L'architecture décrite ci-dessus est recommandée pour un système de redondance (normal/standby) avec Monitor Pro.

Pour les architectures ne nécessitant pas de redondance, le fichier d'application STU peut être stocké sur l'ordinateur exécutant les systèmes OFS/SCADA et Unity Pro XL.

Caractéristiques clés du système

- Unity Pro XL est indispensable pour les modes de fonctionnement de OFS : c'est le seul logiciel capable d'exécuter le mode serveur requis pour la mise à jour dynamique des symboles. Unity Pro XL doit donc être installé. OFS lance Unity Pro XL et ouvre l'application en arrière-plan.
- Le système SCADA + OFS + Unity Pro XL est exécuté sur un seul ordinateur.
- Unity Pro s'exécute sur un ordinateur séparé pour les modifications d'application. Il n'est pas nécessaire que cet ordinateur soit connecté en permanence au réseau, mais seulement pour les modifications en ligne.
- Lorsqu'un serveur d'ordinateurs est utilisé pour les fichiers d'application STU, OFS et Unity Pro utilisent la même application pour les modifications et la synchronisation.
- OFS accède aux données de l'automate en temps réel. Il détecte toute différence entre l'application exécutée et le fichier de symbole local sur l'ordinateur (vérification des signatures). Conformément au QoS pour OFS, la communication s'arrête ou bascule vers un service de mauvaise qualité.
- OFS/Unity Pro XL met à jour les symboles en accédant au fichier STU. En fonction des paramètres OFS, cette mise à jour peut être automatique ou déclenchée par l'application SCADA via un mode de commande spécifique de OFS. L'application continue de s'exécuter. Seule la communication OFS est interrompue pendant la mise à jour du fichier de symboles.
- Lorsque Unity Pro est utilisé pour gérer les modifications en ligne, le fichier d'application STU effectue la synchronisation de OFS/Unity Pro XL avec la bonne version de l'application.

Versions des produits

Produit	Version	Commentaires
Unity Pro M, L, XL	v2.0	Pour les modifications d'application
VijeoLook	v2.6	Inclut la version correcte de OFS
MonitorPro	v7.2	Accès aux variables structurées non inclus

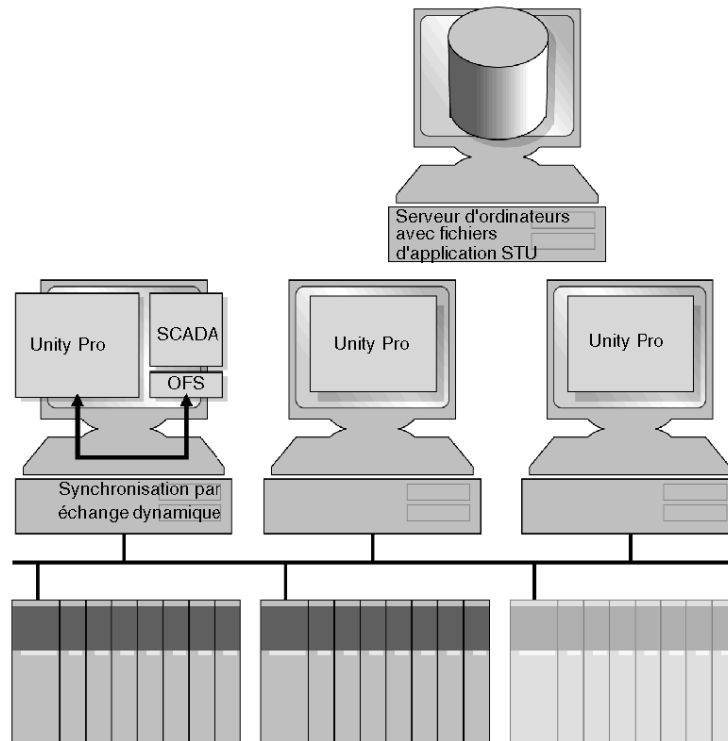
Architecture Build-time/Runtime pour système avec multiples connexions SCADA

Exemple d'architecture

L'exemple de système build-time/runtime suivant gère des architectures nécessitant :

- des modifications d'application fréquentes ;
- un niveau de service supérieur pour permettre la synchronisation entre le système SCADA et l'application exécutée pendant les modifications.

Cette architecture prend également en charge plusieurs SCADA connectés sur un serveur OFS centralisé. La synchronisation est gérée par le biais d'échanges dynamiques entre les systèmes OFS et Unity Pro XL. Aucune opération manuelle n'est requise pour mettre à jour le fichier de symboles pour OFS.



Un ordinateur est utilisé pour exécuter les systèmes OFS et Unity Pro XL en mode serveur. Un ou plusieurs ordinateurs sont dédiés au système SCADA. Un autre ordinateur est utilisé pour exécuter Unity Pro et lancer les modifications d'application.

Le serveur d'ordinateurs dédié aux fichiers d'application STU assure la cohérence d'accès, de sorte que toutes les stations qui exécutent Unity Pro accèdent aux mêmes informations d'application actualisées.

Option du système

Le fichier d'application STU peut être stocké sur l'ordinateur qui exécute les systèmes OFS/SCADA et Unity Pro XL.

Caractéristiques clés du système

- Unity Pro XL est indispensable pour les modes de fonctionnement de OFS. C'est la seule architecture prenant en charge l'exécution en mode serveur, requise pour la mise à jour dynamique des symboles. Unity Pro XL doit donc être installé. OFS lance Unity Pro XL et ouvre l'application en arrière-plan.
- Le système OFS + Unity Pro XL est exécuté sur un seul ordinateur.
- Le système SCADA est exécuté sur un ordinateur dédié et communique avec OFS (DCOM) pour assurer l'accès en temps réel à l'automate.
- Unity Pro s'exécute sur un ordinateur séparé pour les modifications d'application. Il n'est pas nécessaire que cet ordinateur soit connecté en permanence au réseau, mais seulement pour les modifications en ligne.
- Le serveur d'ordinateurs dédié aux fichiers d'application STU assure la cohérence d'accès, de sorte que toutes les stations OFS et Unity Pro utilisent les mêmes données d'application pour les modifications et la synchronisation.
- OFS accède aux données à partir de l'automate en temps réel. Il détecte toute différence entre l'application exécutée et le fichier de symbole local sur l'ordinateur (vérification des signatures). Conformément au QoS pour OFS, la communication s'arrête ou bascule vers un service de mauvaise qualité.
- OFS/Unity Pro XL met à jour les symboles en accédant au fichier STU. En fonction des paramètres OFS, cette mise à jour peut être automatique ou déclenchée par l'application SCADA via un mode de commande spécifique de OFS. L'application continue de s'exécuter. Seule la communication OFS est interrompue pendant la mise à jour du fichier de symboles.
- Pour toute modification en ligne effectuée à partir de Unity Pro, le fichier d'application STU doit être sauvegardé de façon à synchroniser OFS/Unity Pro XL avec la bonne version de l'application.

Versions des produits

Produit	Version	Commentaires
Unity Pro M, L, XL	2.0	Pour les modifications d'application
Unity Pro XL	v2.0	Pour le mode serveur de l'ordinateur
VijeoLook	v2.6	Inclut la version correcte de OFS
Monitor Pro	v7.2	Accès aux variables structurées non inclus

3.13 SCADA/IHM

Vue d'ensemble

Cette section décrit le fonctionnement et la conception d'un système SCADA ou IHM. Elle se concentre sur l'utilisation du protocole de communications Modbus TCP/IP entre le système SCADA et les terminaux. Les informations ne sont pas spécifiques à un système SCADA ou un module IHM ; les concepts décrits s'appliquent à la plupart des progiciels disponibles sur le marché, mais les termes et les techniques peuvent varier d'un progiciel à l'autre.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
SCADA/IHM	301
Communications entre un serveur d'E/S et un équipement terrain	303
Communications SCADA vers des équipements terrain : Utilisation des sockets et des requêtes	308
Communications client entre un serveur d'E/S et un affichage	312
Détails sur la mise en œuvre des produits Schneider	313

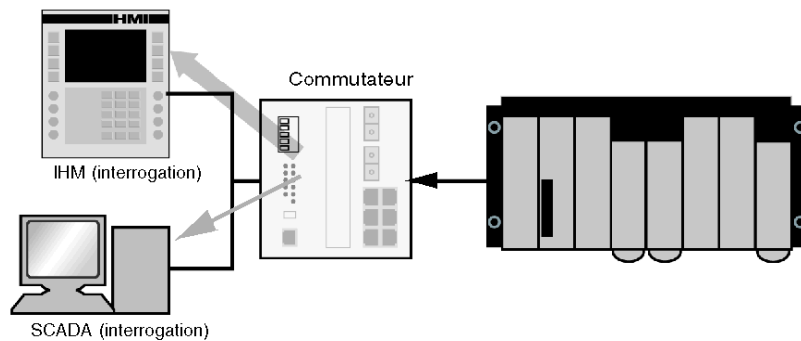
SCADA/IHM

Modèles SCADA/IHM

Les systèmes SCADA et IHM sont représentés par deux modèles : autonome et client/serveur.

Modèle autonome

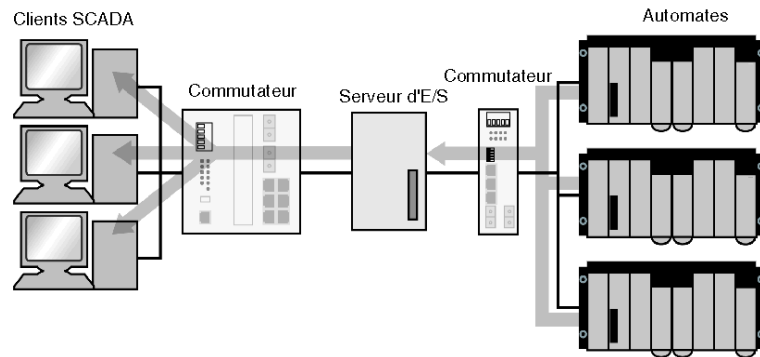
Le modèle SCADA/IHM autonome utilise le même ordinateur ou terminal pour interroger et afficher des données à partir des équipements sur le terrain. Chaque terminal d'affichage supplémentaire interroge ses propres données à partir des équipements terrain. L'illustration suivante présente une IHM et un PC avec SCADA interrogeant un automate pour obtenir des données



Modèle client/serveur

Le modèle client/serveur utilise un serveur d'E/S distinct et des clients d'affichage. Le serveur d'E/S interroge des données à partir des équipements terrain et les clients affichent ces données. Chaque client obtient les données à partir du serveur d'E/S, pas des équipements terrain. Le serveur d'E/S combine toutes les requêtes en provenance des équipements d'affichage et rassemble les données des équipements terrain dans le système SCADA. La charge sur le réseau et les équipements terrain devient plus faible, et le temps de réponse système s'améliore. Dans certains systèmes, le serveur d'E/S peut être le même équipement physique que l'équipement d'affichage.

NOTE : Plusieurs serveurs d'E/S peuvent être utilisés pour activer la redondance. L'illustration suivante montre que les requêtes en provenance du client SCADA sont obtenues à partir des automates par le serveur d'E/S.



Un système SCADA peut inclure d'autres serveurs de type tendance, alarmes, etc. Ces serveurs ne sont pas inclus dans la description parce qu'ils utilisent le serveur d'E/S pour communiquer avec les équipements terrain.

Les données utilisées par le système SCADA sont appelées *étiquettes*. Les étiquettes peuvent être utilisées pour l'affichage, les tendances, les alarmes, les rapports, etc.

Communications dans le système SCADA

Deux étapes de communications constituent le chemin SCADA-équipement :

- entre le client d'affichage et le serveur d'E/S
- entre le serveur d'E/S et l'automate (ou système autonome)

Vous pouvez utiliser plusieurs serveurs d'E/S pour activer la redondance.

Communications entre un serveur d'E/S et un équipement terrain

Récapitulatif

La manière dont un système SCADA rassemble des données à partir de l'équipement terrain peut considérablement affecter la charge du réseau et de l'équipement, ainsi que les temps de réponse globaux du système. Les communications entre le serveur d'E/S et les équipements terrain peuvent suivre plusieurs modèles courants. La plupart des systèmes SCADA utilisent une combinaison de :

- rapports d'exception de données en provenance des équipements terrain ;
- interrogation du serveur d'E/S sur l'état de l'équipement, en fonction des groupes et des périodes définis par l'utilisateur ;
- écritures d'exception du serveur d'E/S en réponse à des commandes de l'opérateur ;
- lectures/écritures basées sur le temps du serveur d'E/S pour les étiquettes utilisées dans le code d'application.

Rapport d'exception

Le rapport d'exception constitue la méthode la plus efficace mais aussi la moins courante pour transférer des données entre un équipement terrain et le système SCADA. L'équipement terrain doit avoir connaissance des étiquettes utilisées par le système SCADA et doit les surveiller en cas de modification dans l'équipement terrain. Lorsque la valeur d'une étiquette change, l'équipement terrain écrit la nouvelle valeur dans le système SCADA. Pour que cette méthode fonctionne, les équipements terrain doivent être en mesure d'initier des communications avec le système SCADA (par le biais d'un client de messagerie Modbus) et ce dernier doit être en mesure de recevoir le transfert des données (par le biais d'un serveur de messagerie Modbus). Le rapport d'exception est utilisé pour signaler l'état des équipements terrain en termes d'affichage, de tendances et d'alarmes.

Le rapport d'exception est efficace parce que les mêmes valeurs inchangées ne sont pas retransférées à l'infini (comme c'est le cas dans un système interrogé). Ce système de rapport d'exception permet à l'équipement de fermer le socket TCP lorsque les valeurs des données sont inchangées, libérant ainsi le socket TCP pour d'autres utilisations tout en réduisant la charge de l'équipement.

Problèmes liés au rapport d'exception

Les systèmes SCADA interrogent normalement les données à partir des équipements terrain pour surveiller l'état de chaque équipement. Le système SCADA peut détecter une défaillance des communications et vous en informer. Si le système SCADA n'interroge pas l'équipement terrain (comme c'est le cas dans un système de rapport d'exception), il ne peut pas détecter ou signaler une défaillance des communications. Pour lui permettre de détecter une défaillance des communications, le système SCADA a le choix entre :

- attendre des commandes en écriture en provenance de l'équipement terrain toutes les n secondes ;
- interroger l'équipement terrain de temps en temps pour vérifier s'il est en ligne.

Un autre problème peut se poser si une réponse en écriture en provenance de l'équipement terrain se perd ou qu'une valeur change alors que le système SCADA est dans l'incapacité de recevoir le message. Dans ce cas, le système SCADA affiche l'ancienne valeur, mais n'affiche pas d'erreur de communications. Pour corriger ceci, l'équipement terrain transfère périodiquement la valeur d'étiquette.

Surveillance de l'équipement terrain

Il n'est pas pratique pour un équipement terrain de surveiller individuellement un grand nombre de variables afin de déterminer si un rapport d'exception s'avère nécessaire. La plupart des systèmes utilisent un checksum sur un groupe de variables. Une écriture de sauvegarde doit toujours être mise en œuvre au cas où le checksum échoue. Par exemple, des variables multiples peuvent changer sans affecter le résultat du checksum. L'équipement terrain peut réduire la charge de l'équipement et du réseau en appliquant une hystérésis sur les variables et en envoyant un rapport d'exception uniquement si une variable change selon une quantité prédéterminée.

Variante sur le rapport d'exception

Si vous utilisez un système SCADA qui ne met pas en œuvre un serveur de messagerie Modbus ou un équipement terrain qui ne met pas en œuvre un client de messagerie Modbus, le système SCADA interroge uniquement le checksum ou un bit unique pour indiquer qu'une ou plusieurs étiquettes d'un bloc de données ont changé. Lorsqu'une modification est détectée, le système SCADA interroge le jeu de données entier pour obtenir les nouvelles valeurs. Ce système n'est normalement pas pris en charge nativement dans le système SCADA. Vous devez le coder en utilisant une certaine forme de logique utilisateur dans le système SCADA.

Pour interroger l'état du terrain, le logiciel SCADA lit les données de chaque équipement terrain. Normalement, le logiciel SCADA détermine la manière dont les données sont interrogées sur la base de :

- groupes définis par utilisateur ;
- groupes créés par SCADA.

Si vous configurez les groupes, vous devez prendre en compte :

- la manière dont les variables sont groupées et leurs adresses correspondantes dans les équipements terrain ;
- la fréquence d'interrogation des groupes en comparaison avec la vitesse des réponses qu'ils reçoivent ;
- le moment auquel les groupes sont interrogés : continuellement ou ponctuellement ;
- la manière dont l'interrogation des groupes est liée.

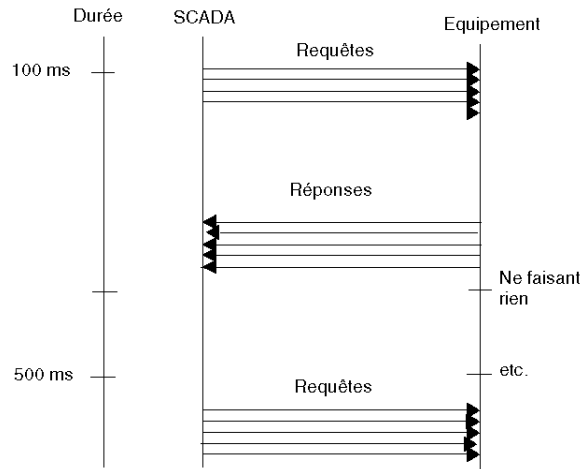
Les groupes de variables doivent être configurés de manière à être interrogés à une vitesse égale ou inférieure à celle à laquelle l'équipement terrain peut répondre. Pour calculer cette vitesse, consultez la section sur l'évaluation des performances (*voir page 352*) du système. N'oubliez pas de prendre en compte tous les autres équipements, y compris d'autres systèmes SCADA, qui communiquent avec l'équipement terrain.

Lors de la création des groupes, essayez de regrouper les étiquettes de manière à pouvoir activer et désactiver l'interrogation des groupes. Les variables sont interrogées uniquement si nécessaire. Vous pouvez coder ce comportement ou utiliser une fonction automatique du système SCADA. Dans chaque cas, les variables d'alarme doivent être placées dans un groupe et les variables de tendance dans un ou plusieurs groupes distincts des variables d'affichage. Le groupe contenant les variables d'affichage doit être interrogé uniquement lorsque les étiquettes sont actives sur un écran.

Lorsque des systèmes SCADA utilisent un serveur OPC pour lire des données à partir d'un équipement terrain, chaque serveur d'E/S peut créer des groupes distincts (même si chaque serveur d'E/S interroge les mêmes variables). Le système SCADA peut tenter d'ajouter/supprimer des variables à partir des groupes du serveur OPC. Ce processus est inefficace à cause des retards. L'alternative préférée consiste à ce que le système SCADA crée un plus grand nombre de groupes avec moins de variables dans chaque groupe et active/désactive les groupes ou variables dans les groupes. Cependant, les serveurs OPC ne présentent pas tous les mêmes capacités à activer/désactiver des variables et des groupes ou à ajouter/supprimer des variables dans un groupe. Les serveurs OPC peuvent ou ne peuvent pas bloquer les données des requêtes lorsque les données sont dans des groupes multiples.

Lorsque la synchronisation est configurée pour l'interrogation des groupes, vérifiez que l'interrogation ne surcharge pas les équipements terrain. La méthode la plus courante pour interroger les données consiste à définir une période d'interrogation utilisée par chaque groupe pour lire les données. Si cette période est définie à 1 000, le groupe tente d'interroger toutes les données toutes les 1 000 ms. Un problème peut survenir lorsque des groupes multiples sont paramétrés sur la même fréquence d'interrogation. Lorsque la période de 1 000 ms expire, le système SCADA tente de lire plusieurs blocs de données à partir des équipements terrain, entraînant des pics au niveau des charges du réseau et de l'équipement terrain.. Une fois que ces requêtes ont reçu une réponse, l'équipement terrain attend passivement d'être à nouveau interrogé. Selon l'équipement terrain, cette surcharge peut entraîner une défaillance ou des retards de communications.

Si l'équipement peut mettre en mémoire tampon les requêtes et y répondre dans le temps et si la charge moyenne totale est inférieure aux capacités de l'équipement, le seul problème qui subsiste est le petit délai de réponse à la requête.



Pour éviter ce type de surcharge des communications, définissez les périodes d'interrogation des groupes sur des valeurs uniques. Ces valeurs doivent être choisies pour que l'interrogation des groupes multiples ne survienne pas trop souvent (par exemple., 500 ms, 700 ms, 900 ms). La meilleure solution consiste à lier l'interrogation des groupes. Liez l'interrogation pour qu'un groupe ait fini d'être interrogé avant qu'un autre groupe le soit à son tour. Cette solution évite :

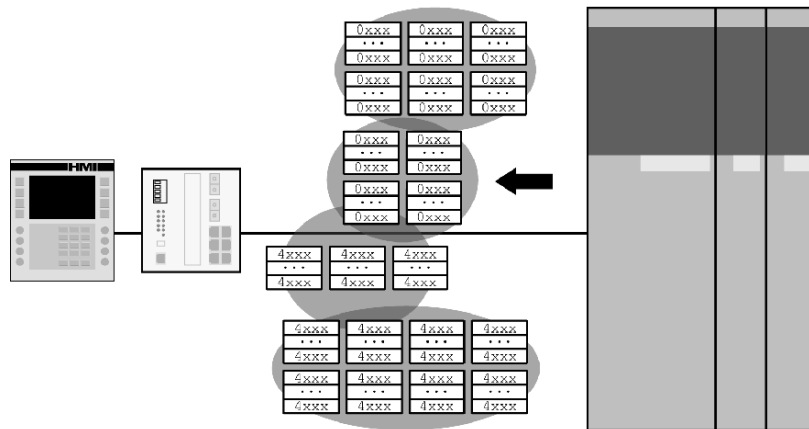
- une surcharge des requêtes qui attendent une réponse de la part des équipements terrain, ce qui entraîne une défaillance des communications ;
- une file d'attente de requêtes se formant dans le système SCADA ou l'équipement terrain.

Certains systèmes SCADA lient automatiquement l'interrogation des groupes. D'autres nécessitent que vous mettiez manuellement en œuvre cette fonction.

Blocage

Pour lire ou écrire le même type de données (le même code de fonction Modbus), le système SCADA peut tenter de combiner plusieurs étiquettes dans un transfert de données unique pour une meilleure efficacité. Ceci s'effectue normalement pour les commandes en écriture, sauf lorsque vous écrivez des tables de données.

La manière dont un système SCADA combine des valeurs dans une lecture unique est connue sous le nom de *blocage*. Le blocage peut améliorer l'efficacité des communications système globales.



Pour avoir un blocage le plus efficace possible, les variables de l'équipement terrain doivent être situées de manière à ce que toutes les données requises par le système SCADA soient regroupées dans la zone mémoire Modbus. Lorsque vous définissez des groupes interrogés par le système SCADA, organisez les variables au sein de l'équipement terrain de telle sorte que toutes les variables d'un groupe soient contiguës. Même si vous n'organisez pas les groupes à interroger, organisez les variables utilisées pour les alarmes et les tendances de manière à ce qu'elles soient contiguës. Les éléments définis à la même fréquence doivent être regroupés, et les alarmes doivent être regroupées.

La règle du blocage des données comporte une exception pour les variables non localisées. Les deux logiciels Unity et Concept permettent aux variables de l'équipement terrain d'exister sans adresse physique. Un code de fonction de messagerie Modbus spécifique peut lire/écrire ces variables. Les variables ne peuvent pas être localisées l'une près de l'autre, mais le système SCADA peut les lire/écrire aussi efficacement qu'un bloc de variables localisées. Néanmoins, certains équipements sont capables de répondre plus vite ou plus souvent à des requêtes de variables localisées que de variables non localisées.

Communications SCADA vers des équipements terrain : Utilisation des sockets et des requêtes

Récapitulatif

Pour déterminer le mode de transfert des données de votre système SCADA vers un équipement terrain, vous devez prendre plusieurs facteurs en compte :

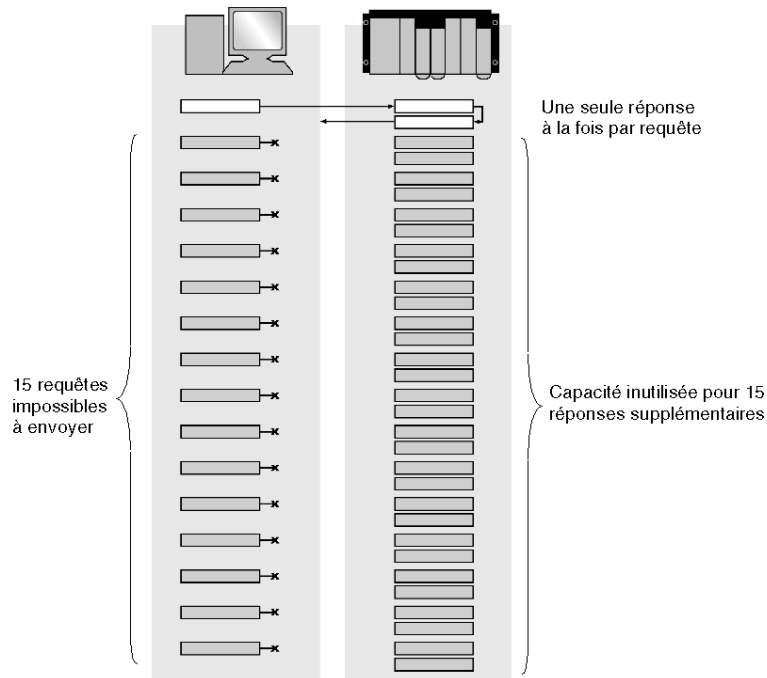
- la manière dont les groupes de données sont structurés
- le moment où une autre section tente de lire les groupes de données
- les sockets TCP et leur utilisation
- le nombre de requêtes de messagerie Modbus pouvant être envoyées sur chaque socket
- les types de requêtes utilisées

Un système SCADA peut ouvrir un ou plusieurs sockets TCP à un équipement. Il peut envoyer des requêtes de messagerie Modbus sur chacun de ces sockets. Selon sa conception, le système SCADA peut vous autoriser à contrôler le nombre de sockets à ouvrir et la méthode de transmission des requêtes, ou tout simplement fonctionner comme prévu sans personnalisation possible.

Les systèmes SCADA classiques utilisent une combinaison de trois méthodes, avec plusieurs sockets utilisés et une ou plusieurs requêtes sur chaque socket. Généralement, un ou plusieurs sockets sont configurés pour lire et écrire des données. Une file d'attente de requêtes peut se former à la fois dans le terminal et le système SCADA.

Une requête à la fois

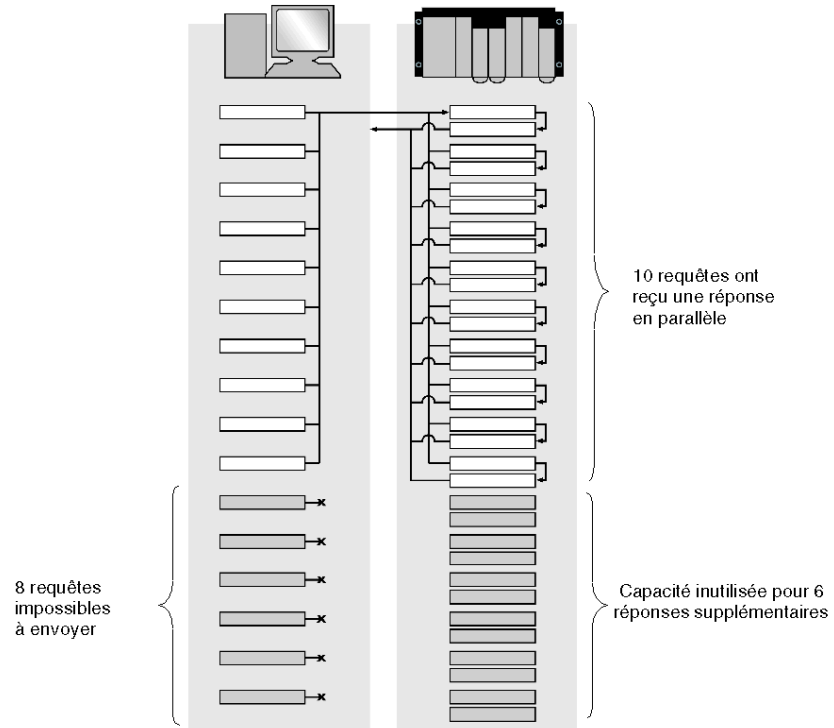
L'efficacité du système SCADA dans l'envoi des requêtes et le traitement des réponses influe considérablement sur le temps de réponse système. Voici un exemple de socket unique prenant en charge une requête à la fois :



Le système SCADA n'ouvre qu'un seul socket à l'équipement terrain et ne peut envoyer qu'une seule requête. Il attend qu'une réponse soit donnée à cette requête avant d'envoyer la requête suivante. Ceci évite la surcharge du terminal en limitant le système à une seule requête à la fois dans le terminal. Ceci affecte également gravement le temps de réponse système. Par exemple, si le système SCADA a dix requêtes à envoyer au terminal, le terminal prend 100 ms pour répondre à chaque requête et 50 ms de plus pour envoyer la nouvelle requête. Le temps total pour répondre à toutes les requêtes est de 1,5 s.

Requêtes multiples sur un socket unique

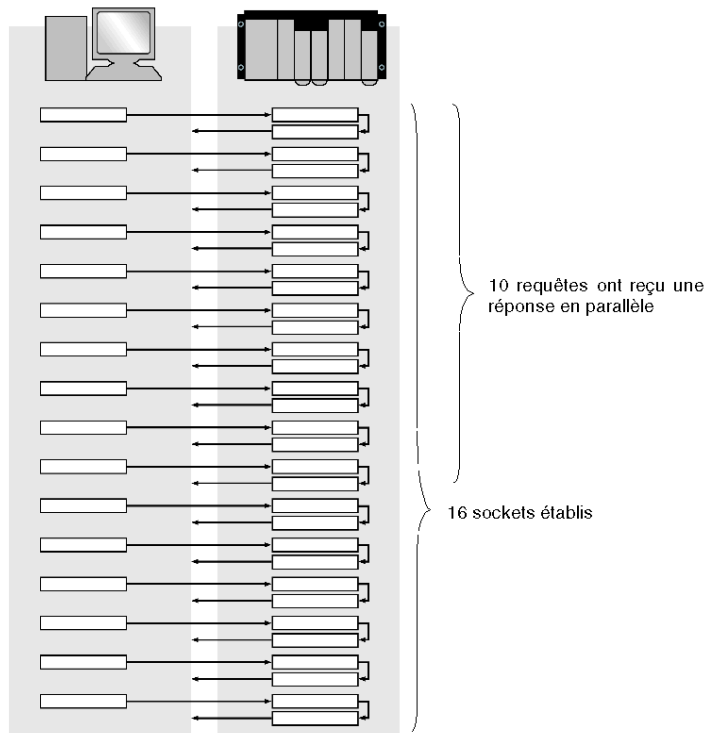
Voici un exemple de socket unique prenant en charge des requêtes multiples, dix dans ce cas :



Le système SCADA ouvre un socket unique à l'équipement terrain mais peut envoyer dix requêtes au terminal sans attendre de réponse. Le terminal peut commencer à répondre aux dix requêtes sans délai. Ce système offre un temps de réponse plus rapide, mais peut également surcharger un terminal si l'équipement ne peut pas traiter dix requêtes simultanément. Même si l'équipement peut traiter les dix requêtes, il risque de ne pas pouvoir traiter plusieurs requêtes simultanément sur un socket TCP unique. Ceci est fréquent avec des équipements anciens ou qui n'utilisent pas l'ID de transaction Modbus TCP. Le temps de réponse système est de 150 ms, au lieu de 1,5 s dans l'exemple précédent.

Sockets multiples envoyant une requête à la fois

Voici l'exemple d'un système SCADA qui utilise dix sockets distincts pour envoyer des requêtes à l'équipement terrain, mais n'envoie qu'une seule requête sur chaque socket. Ce système gère les équipements qui prennent seulement en charge une seule requête par socket.



Ce système évite les problèmes avec les équipements incapables de traiter des requêtes multiples sur le même socket, mais le terminal peut toujours devenir surchargé en raison du nombre total de requêtes. Le temps de réponse système est de 150 ms.

Communications client entre un serveur d'E/S et un affichage

Les communications client entre un serveur d'E/S et un affichage sont couramment basées sur un ou plusieurs des éléments suivants :

- les systèmes propriétaires et les protocoles
- les communications client/serveur OPC
- les communications MS Windows

Dans la mesure où la plupart des communications SCADA à SCADA reposent sur une certaine forme de service de mise en réseau MS Windows (Com/DCom, noms de machine, etc.), ce service doit être installé sur le réseau. Cependant, en installant ce type de service, le réseau devient chargé d'un trafic MS Windows supplémentaire et est sensible à des surcharges par MS Windows et d'autres trafics.

Dans la mesure du possible, les communications SCADA à SCADA doivent être séparées du réseau de communications normal de l'équipement. Pour ce faire, installez des cartes Ethernet distinctes dans les PC SCADA et utilisez un réseau Ethernet distinct pour les communications SCADA à SCADA.

Détails sur la mise en œuvre des produits Schneider

Mise en œuvre de VijeoLook

VijeoLook utilise le serveur OPC Schneider pour les communications
(voir page 281).

Mise en œuvre de Monitor Pro

Monitor Pro prend en charge le modèle serveur d'E/S/clients multiples. Lorsque vous utilisez le système de communications Modbus TCP/IP, Monitor Pro met en œuvre des groupes définis par les utilisateurs, vous permettant de configurer les étiquettes à lire dans chaque groupe. Vous pouvez déclencher la lecture et l'écriture de chaque groupe via une étiquette définie par l'utilisateur. Il peut s'agir d'une étiquette basée sur le temps pour les lectures ou d'une étiquette personnalisée. Pour les écritures, l'étiquette est automatiquement définie dès qu'un élément du groupe est modifié et que cet élément est le seul à être écrit. Pour les lectures, tout le groupe est lu. Les groupes peuvent être ordonnés en évitant que l'étiquette de contrôle ne soit déclenchée avant que l'indicateur de fin soit paramétré pour le groupe précédent.

Monitor Pro utilise un socket TCP pour les lectures, un socket distinct pour les écritures et un autre socket distinct pour les lectures d'exception. Chaque socket autorise la mise en attente d'une seule requête de messagerie Modbus à la fois sur l'équipement.

Vous pouvez créer une instance supplémentaire de la tâche de communications Modbus et répartir les variables à lire entre les deux tâches. Etant donné que des requêtes supplémentaires peuvent être envoyées simultanément à l'équipement terrain, les performances du système sont plus améliorées.

Monitor Pro crée une file d'attente en son sein pour toutes les requêtes de communications déclenchées mais ne pouvant être envoyées à l'automate à cause des requêtes en attente sur un socket. Ces requêtes vont dans la boîte aux lettres des tâches Modbus TCP/IP. La boîte aux lettres peut finir par déborder et entraîner l'arrêt des communications.

3.14 Redondance

Vue d'ensemble

Cette section traite de la redondance des services du point de vue du système. La redondance totale du système est déterminée par le réseau, les équipements et les redondances de services.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Redondance réseau et services de communication	315
Redondance dans un système SCADA	319
SCADA dans un système de redondance d'UC Quantum	323
Permutation de redondance d'UC et services Ethernet	333

Redondance réseau et services de communication

Récapitulatif

La redondance permet au réseau de continuer à transporter des données en cas de défaillance d'un composant ou d'un câble réseau. En cas de panne, un certain temps s'écoule avant que la défaillance soit prise en compte et corrigée par les composants du réseau. Cette correction survient ou non avant que d'autres systèmes aient remarqué le problème.

Les données transportées sur le réseau risquent parfois de se perdre durant la défaillance. Dans ce cas, elles doivent être retransmises.

Si le réseau peut être récupéré avant la fin du délai d'attente sur un service et si aucune donnée n'est perdue pendant l'interruption/récupération, les services ne sont pas affectés. Si le réseau ne peut pas être récupéré avant la fin du délai d'attente sur le service, ce dernier abandonne la requête individuelle. Le service risque de ne pas retenter le transfert (selon le service) ; attendez-vous dans tous les cas à un retard dans le transfert des informations. En mettant en œuvre de nouvelles tentatives, le service peut transmettre les données envoyées avant qu'une erreur d'application ne soit détectée.

Si le réseau ne peut pas être récupéré avant le nombre de tentatives/la fin du délai d'attente, le service enregistre une erreur dans l'application. Vous devez décider si l'application peut tolérer des délais d'attente et des erreurs sur un service ou si le réseau doit être récupéré avant un délai d'attente ou une erreur sur le service. Prenez en compte les délais d'attente sur les services et le nombre de tentatives avant de sélectionner une stratégie de redondance réseau. Un délai de récupération de réseau plus rapide coûte généralement plus cher et n'est pas systématiquement requis dans votre application.

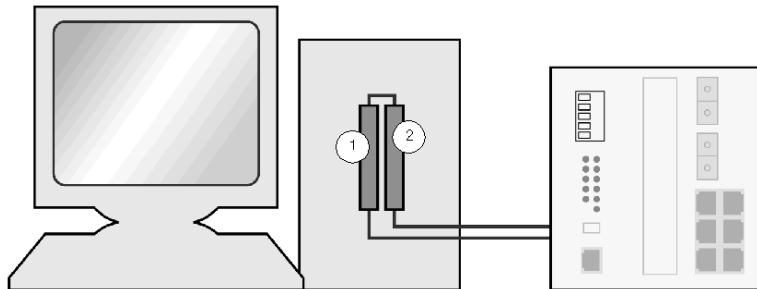
Interfaces Ethernet multiples dans un équipement

De multiples interfaces Ethernet d'un équipement sont résilientes en cas de défaillance d'une des interfaces Ethernet ou du réseau connecté. Cependant, elles nécessitent également que les communications vers et depuis l'équipement soient gérées pour que tous les autres équipements communiquent avec l'interface active. Si deux interfaces Ethernet sont installées dans un équipement, deux méthodes de traitement des communications existent : deux interfaces liées ou deux interfaces indépendantes.

Interfaces liées

Deux interfaces liées partagent la même adresse IP et peuvent apparaître comme une seule et même interface Ethernet pour les autres équipements du réseau. Les deux interfaces surveillent automatiquement leur capacité à communiquer avec le reste du système et décident laquelle est à disposition de l'équipement et du réseau extérieur. Le choix de cette solution n'implique aucun travail supplémentaire.

Les systèmes sur PC utilisent couramment des interfaces liées. Elles sont similaires aux ports redondants Modbus Plus en ce sens que vous ne devez pas intervenir pour bénéficier des deux interfaces. Les interfaces s'auto-surveillent et décident quelle interface présenter au réseau extérieur et quelle interface présenter à l'équipement (pour qu'ils ne voient qu'une interface). Plusieurs cartes Ethernet pour PC offrent cette fonctionnalité et leur utilisation est recommandée.

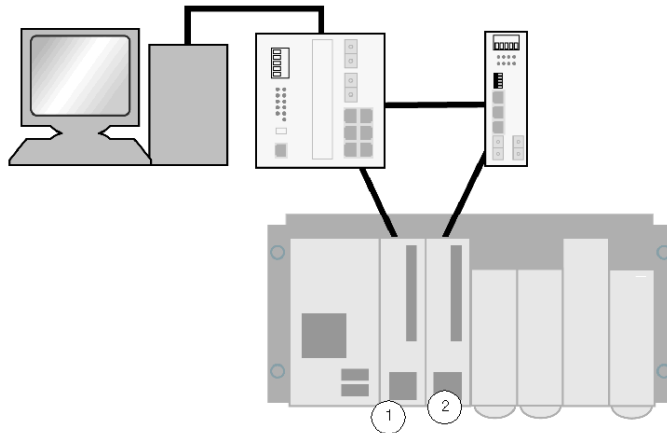


- 1 L'interface 1 offre une présentation unique au système SCADA et à l'automate ; elle surveille la validité de l'interface 2 afin de s'assurer que cette dernière peut prendre la relève si elle venait à défaillir.
- 2 L'équipement 2 surveille l'état de l'interface 1 et partage la même adresse IP que l'interface 1. Il ne présente pas d'informations au système SCADA et à l'automate sauf en cas de défaillance de l'interface 1.

Interfaces indépendantes

Chaque interface possède une adresse IP différente ; une seule interface est active à la fois. Ce procédé d'implémentation d'interfaces multiples nécessite généralement que vous contrôliez la validité des interfaces dans leur application et décidiez de l'interface à activer. Par exemple, avec un logiciel SCADA doté de deux cartes Ethernet non liées installées sur un PC, le système surveille les deux interfaces et en choisit une. Deux modules ETY dans un automate Premium constituent un autre exemple. Tous les équipements Schneider Automation utilisent cette méthode.

Vous devez surveiller la validité de chaque interface et décider du mode de traitement des communications pour que les échanges ne soient pas dupliqués. La surveillance peut réduire le trafic et la charge du réseau sur d'autres équipements, mais le contrôle des communications de cette manière n'est pas toujours possible. Si les deux interfaces doivent être actives (pour Global Data, par exemple), les deux interfaces procèdent aux échanges et transmettent les résultats à l'équipement/application ; l'application doit décider quelles informations utiliser. Voici un automate Premium avec deux modules de communications ETY Ethernet :

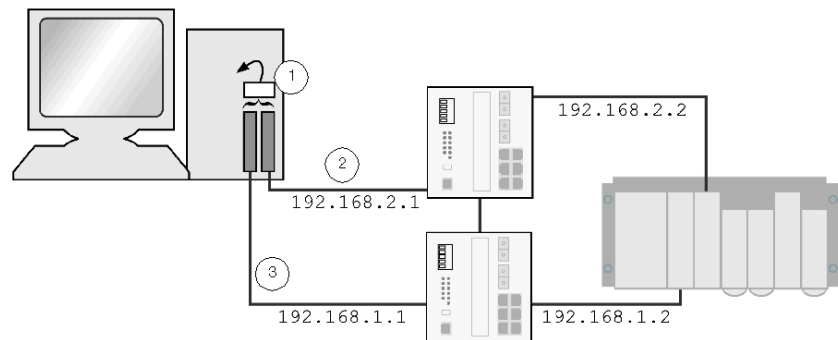


- 1 L'interface 1 possède sa propre adresse IP et apparaît en tant qu'équipement indépendant sur le réseau
- 2 L'interface 2 possède également sa propre adresse IP et apparaît en tant qu'équipement indépendant sur le réseau

Dans des systèmes comme celui illustré ci-dessus, vous risquez de ne pas pouvoir contrôler le mode d'émission des communications de chaque équipement parce que vous ne pouvez pas contrôler l'interface qui est utilisée. Ce problème est courant avec les PC configurés avec deux cartes Ethernet. Le PC choisit une carte à laquelle envoyer des données en fonction du réseau auquel la carte est connectée (défini par l'adresse IP et le masque de sous-réseau). Le PC tente d'envoyer des requêtes par le biais de la carte directement connectée au réseau de destination. Si un PC est configuré avec deux interfaces Ethernet possédant des adresses IP différentes sur le même réseau, le PC ne sait pas quelle carte utiliser. Les communications peuvent alors être défectueuses et échouer.

Pour éviter ce problème, configurez chaque carte Ethernet pour une plage d'adresses réseau distincte et contrôlez manuellement les communications en adressant les communications à un réseau ou à l'autre. Malheureusement, les deux cartes Ethernet utilisant des réseaux IP différents (même si elles sont connectées au même réseau physique) posent des problèmes de communication avec les équipements distants. Les équipements risquent de ne pas pouvoir communiquer simultanément sur les deux réseaux. Deux réseaux complets doivent être construits et tous les équipements doivent être connectés aux deux réseaux. Vous devez déterminer le réseau actif en passant par la gestion de réseau.

L'illustration suivante présente un PC avec deux cartes Ethernet branchées sur le même commutateur et un automate avec deux modules ETY connectés au commutateur.



- 1 Un bloc de décision à l'intérieur du programme SCADA ou PC
- 2 Réseau B
- 3 Réseau A

Deux réseaux indépendants offrent un niveau de redondance élevé, mais un bloc de décision doit être inclus dans le programme SCADA ou PC pour déterminer quel réseau utiliser à tout moment.

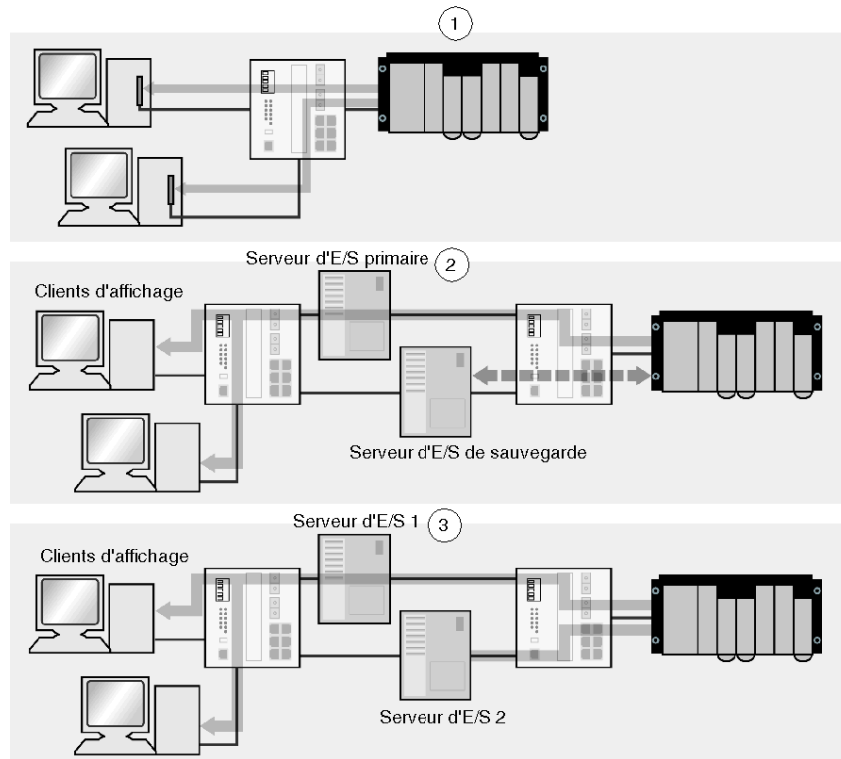
Redondance dans un système SCADA

Récapitulatif

Plusieurs niveaux de redondance sont disponibles dans un système SCADA. Pour les communications au sein d'une usine, le système SCADA doit opérer de telle sorte que seul le serveur d'E/S primaire échange des données avec les équipements terrain. Les avantages sont les suivants :

- réduction considérable du nombre de communications sur les équipements terrain, se traduisant par des temps de réponse plus rapides sur l'ensemble du système,
- réduction du trafic réseau entre les équipements de l'usine,
- trafic réseau plus efficace puisque le trafic SCADA serveur-client peut être optimisé (toutes les données sont transférées vers un client et le client n'a plus besoin de regrouper les informations provenant de chaque équipement terrain). Le trafic peut être reporté sur un réseau autre que le réseau de contrôle de l'usine.

L'illustration suivante présente trois systèmes SCADA entièrement redondants, tous interrogeant l'automate :



- 1 Deux systèmes SCADA distincts, tous les deux interrogeant l'automate.
- 2 Deux clients d'affichage interrogeant un serveur d'E/S primaire. Le serveur d'E/S de sauvegarde se contente de surveiller l'état des connexions vers l'automate.
- 3 Deux clients d'affichage interrogeant un serveur d'E/S qui ignore l'existence d'un système de sauvegarde redondant. Le serveur continue de lire (en mode interrogation) toutes les données provenant de l'automate.

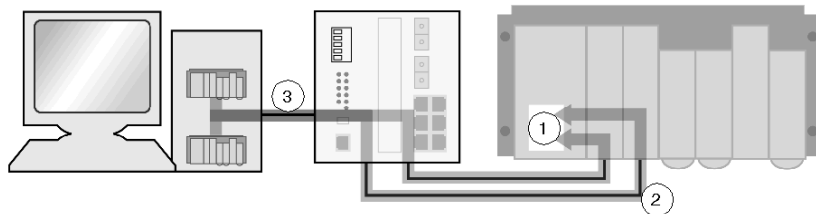
Communication SCADA vers un équipement redondant

Les planificateurs du système SCADA doivent prendre en considération la redondance entre les dispositifs de communication et les équipements redondants. Pour qu'il y ait communication avec un équipement redondant, le système SCADA doit pouvoir échanger les mêmes données avec ce qu'il considère être deux équipements. Par exemple, un système d'automate Quantum avec deux modules NOE permet au système SCADA d'échanger des données avec l'unité centrale de l'automate en utilisant l'un ou l'autre des modules NOE. Si un module (ou le réseau qui lui est associé) tombe en panne, les communications se poursuivent via l'autre module NOE.

Le système SCADA peut gérer automatiquement les communications vers des équipements redondants, mais vous pouvez également les gérer manuellement. Pour une gestion automatique dans SCADA, il suffit d'activer le service et de configurer le système SCADA afin qu'il reconnaisse les deux équipements comme étant identiques. Si cette prise en charge n'est pas proposée par le système SCADA, vous devez procéder à une configuration et à une programmation supplémentaires pour permettre au système de communiquer avec les équipements sur les deux interfaces.

Le problème le plus commun est que le système SCADA est configuré pour communiquer avec l'interface Ethernet de l'équipement terminal, et non avec l'équipement terminal lui-même. Le système SCADA doit percevoir un automate Quantum avec deux modules NOE (par exemple, adresses IP 192.168.1.10 et 192.168.1.11) comme deux équipements distincts, même si l'échange des requêtes SCADA s'effectue via la même unité centrale.

L'illustration suivante présente un système SCADA qui communique avec un automate doté de deux interfaces Ethernet. Le système SCADA considère que deux automates sont présents et doit donc choisir celui avec lequel il va communiquer.



- 1 Les données pour les deux échanges proviennent des mêmes variables de l'automate.
- 2 L'automate a deux modules d'interface.
- 3 Deux ensembles de données sont échangés.

Le système SCADA doit pouvoir extraire depuis un équipement ou l'autre les valeurs à afficher, sans que l'affichage final des données en soit affecté. Si le chemin d'accès à un équipement n'est pas disponible, utilisez le chemin vers l'équipement alternatif ou de sauvegarde jusqu'à ce que le premier chemin redevienne opérationnel.

Chiens de garde de sauvegarde SCADA

La configuration d'un équipement de sauvegarde dans un système SCADA n'est intéressante que lorsque le système peut basculer, de manière fiable, sur l'équipement de sauvegarde en cas de panne de l'équipement primaire.

L'équipement de sauvegarde doit faire l'objet d'une surveillance continue afin de vérifier qu'il est opérationnel. Par ailleurs, il convient de lire périodiquement les données qu'il transmet pour que le système SCADA connaisse à tout moment l'état de la sauvegarde. La surveillance est utile car :

- elle vous avertit des risques de défaillance de la sauvegarde lorsque l'équipement primaire est en cours d'utilisation, de façon à permettre la résolution du problème avant que la sauvegarde ne soit nécessaire ;
- elle permet au système SCADA de vérifier l'état de la sauvegarde avant de procéder à un basculement.

Si l'équipement primaire tombe en panne et si le système SCADA bascule sur un système redondant défaillant, le personnel de l'usine peut être dérouté par la situation, laquelle peut entraîner des pertes de temps, voire l'arrêt de l'application.

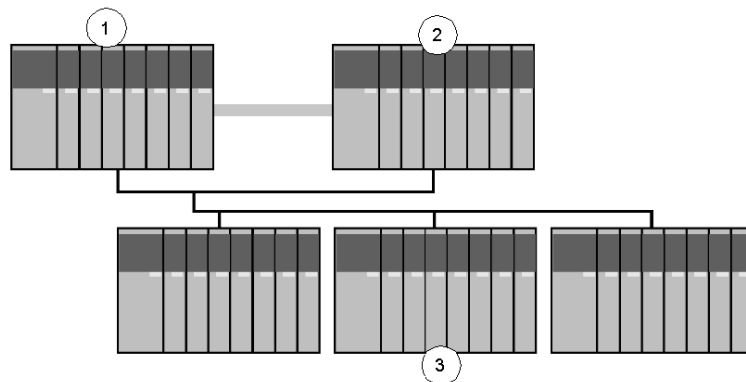
SCADA dans un système de redondance d'UC Quantum

Récapitulatif

Les systèmes de redondance d'UC ont été traditionnellement mis en œuvre pour contrôler les E/S distantes critiques dans les environnements d'automatisation industriels. A mesure que les systèmes SCADA continuent de se développer et jouent un rôle de plus en plus important dans le fonctionnement des usines, la place dévolue aux systèmes de redondance d'UC a évolué. Un système de redondance d'UC peut être nécessaire pour assurer le fonctionnement en mode redondant des réseaux de commande et des communications SCADA. Il est nécessaire de définir de nouvelles règles de redondance d'UC.

Système de redondance d'UC traditionnel

Dans un système d'automatisation industriel traditionnel, l'unique objectif d'un automate avec redondance d'UC était de contrôler l'usine via des E/S physiquement connectées :



- 1 UC primaire
- 2 UC redondante
- 3 Racks des modules d'E/S distants

La redondance d'UC fournit le contrôle redondant d'une usine via des E/S physiques. Le système change de l'UC primaire à l'UC redondante si l'unité primaire ne peut pas contrôler les E/S physiques. Ceci peut se produire du fait de la défaillance des éléments suivants du système primaire :

- alimentation
- UC
- adaptateur RIO
- liaison RIO

Un système de redondance d'UC traditionnel ne bascule pas le contrôle de l'unité primaire sur l'unité redondante pour l'une des raisons suivantes :

- défaillance des liaisons Modbus Plus ou Ethernet
- incapacité du système primaire à communiquer avec un équipement distant via une liaison réseau (autre que E/S via le réseau RIO)

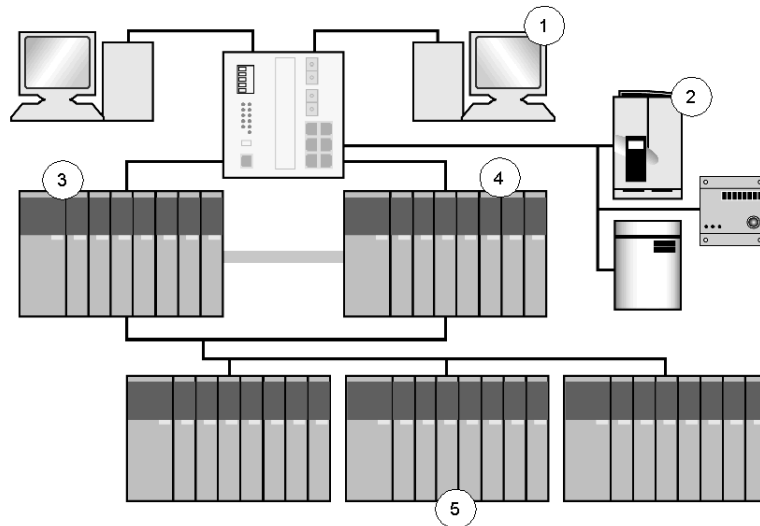
Ces restrictions posent des problèmes pour un système qui repose sur les communications d'un système SCADA ou le contrôle d'une usine via des communications réseau. Dans le cas d'une défaillance de communications de l'automate primaire, le système ne bascule pas automatiquement sur l'unité redondante pour rétablir les communications, même si chaque automate est capable de contrôler l'E/S.

Systèmes centrés sur la communication

Dans un système centré sur la communication, l'intégrité des communications entre le système de redondance d'UC et un équipement du système de l'usine peut être suffisamment importante pour justifier une permutation redondante. Dans ce type de système, le fonctionnement à redondance d'UC Quantum standard doit être modifié afin que les communications vers l'équipement distant soient surveillées et qu'une permutation s'effectue en cas de défaillance des communications.

NOTE : Vous pouvez mettre en œuvre un système de redondance d'UC pour les communications uniquement. Un tel système n'est pas nécessaire pour contrôler les E/S physiques d'une usine. Un rack d'E/S factice doit être configuré, et le réseau RIO doit être physiquement installé pour permettre au système de redondance d'UC de fonctionner.

L'illustration suivante présente un système SCADA redondant avec des automates avec redondance d'UC.



- 1 SCADA surveillant un processus critique contrôlé par l'automate
- 2 Équipements intelligents critiques contrôlés via Ethernet par l'automate
- 3 UC primaire
- 4 UC redondante
- 5 Racks des modules d'E/S distants

Les priorités d'origine de l'automatisation industrielle d'un système de redondance d'UC, qui assurent la redondance de l'E/S distante, restent les mêmes. En outre; vous pouvez affecter une priorité de redondance d'UC égale (ou supérieure) à la liaison de communication de l'usine.

Bien que le système de redondance d'UC Quantum ait été principalement conçu à l'origine pour le contrôle des E/S, le contrôle complet par l'utilisateur de la fonction de permutation est assuré. Vous pouvez personnaliser le fonctionnement afin que les défaillances des communications au niveau de l'usine déclenchent une permutation automate primaire-automate redondant. Vous pouvez programmer votre système pour permuter le contrôle si l'UC primaire courante perd les communications avec les plates-formes SCADA ou avec les équipements Ethernet critiques, même s'il n'existe aucun problème de communication entre l'UC et l'E/S distante.

Règles d'un système de redondance d'UC centré sur les communications

Des réponses doivent être apportées aux questions suivantes pour activer la mise en œuvre d'un système HSBY basé sur les communications :

- Quelles liaisons de communication doivent être surveillées ?
En cas de défaillance, les liaisons doivent-elles provoquer une permutation des automates avec redondance d'UC ?
- Comment se définit une défaillance de communication (délais d'attente, tentatives, etc.) ?
- Des interfaces Ethernet redondantes seront-elles mises en œuvre ?
Si tel est le cas, de quelle manière ?
- Comment sera surveillé l'état du réseau de communications sur l'automate redondant pour s'assurer qu'une permutation améliore les communications ?

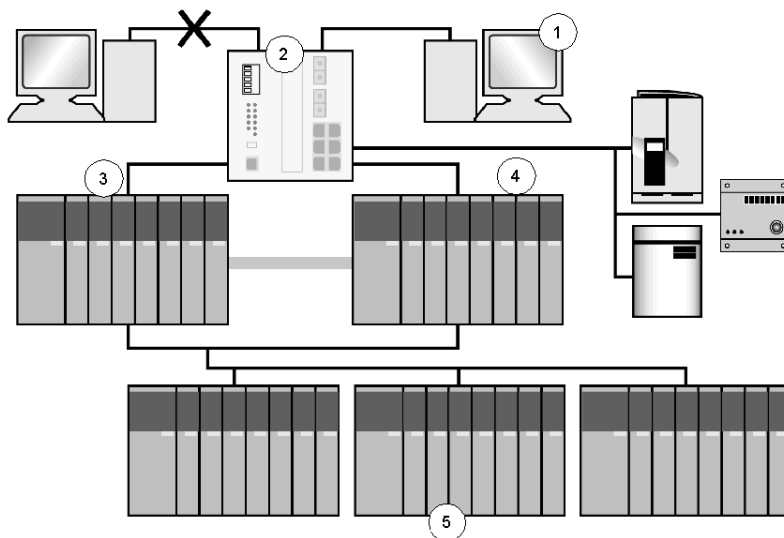
Système redondant de base

Pour assurer la redondance de base des communications pour investissement minimal en matériel et en temps supplémentaires, le système doit comporter :

- une connexion réseau unique à chaque automate dans le système de redondance d'UC ;
- des connexions réseau surveillées en utilisant des fonctions de diagnostic de module.

Limitations du système redondant de base

La permutation peut être configurée pour se produire si l'UC primaire ne parvient pas à trouver une plate-forme SCADA ou si la connexion entre l'UC et le commutateur Ethernet échoue. Toutefois, les automates avec redondance d'UC ne peuvent détecter une défaillance de communication due à une rupture du réseau au-delà de leur connexion locale.

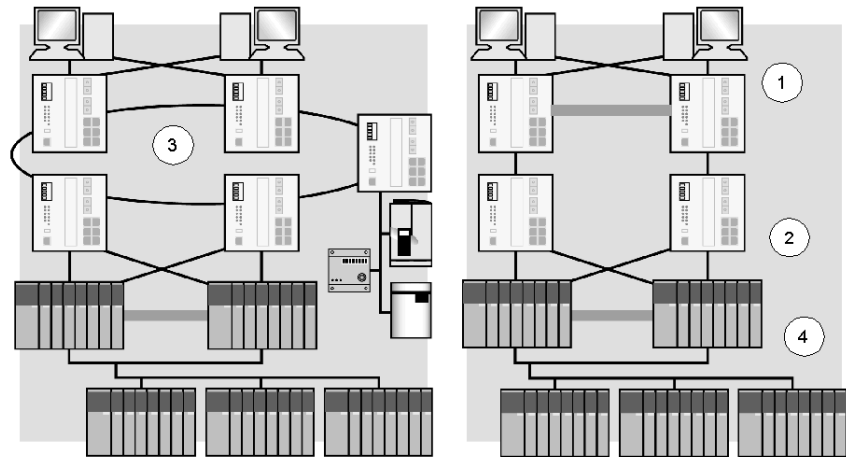


- 1 SCADA surveillant un processus critique contrôlé par l'automate
- 2 Commutateur Ethernet
- 3 UC primaire
- 4 UC redondante
- 5 Racks des modules d'E/S distants

La défaillance d'un seul équipement critique au-delà des connexions locales peut provoquer le dysfonctionnement de l'ensemble du système de communication, comme le montre l'illustration ci-dessus.

Système entièrement redondant

Un système entièrement redondant doit être mis en œuvre lorsque les spécifications nécessitent *aucun point d'erreur* pour le système de contrôle, y compris les communications.



- 1 Système SCADA redondant avec deux interfaces Ethernet liées
- 2 Réseau basé sur des commutateurs avec arbre recouvrant
- 3 Réseau en anneau redondant ConneXium
- 4 Système d'automate avec redondance d'UC avec deux interfaces Ethernet indépendantes

Un système entièrement redondant utilise généralement les éléments suivants :

- matériel réseau supplémentaire installé pour les chemins de réseau redondants ;
- chaque automate du système de redondance d'UC connecté à un chemin de réseau séparé ;
- chaque automate connecté au réseau sur plusieurs points utilisant plusieurs cartes réseau (pour une défaillance du réseau ou d'une carte réseau qui ne déclenche pas une permutation) ;
- des chemins de communications surveillés par des chiens de garde pour l'intégrité des communications tout le long du chemin jusqu'aux terminaux ;
- d'autres équipements (par exemple le système SCADA) connectés au réseau sur plusieurs points utilisant plusieurs cartes réseau ;
- en option, un second réseau physique complet ;
- chaque point de connexion (commutateur ou concentrateur) d'un équipement (par exemple, automate, système SCADA, etc.) alimenté par une alimentation séparée afin que la défaillance d'une alimentation ne déconnecte pas l'équipement du réseau.

Limitations du système entièrement redondant

Les systèmes entièrement redondants présentent les limitations suivantes :

- Coût accru des composants
- Nécessité de modifier les systèmes en dehors de l'automate avec redondance d'UC
- Complexité du système

Surveillance du réseau via l'état du module

L'état du module de communications Ethernet locales peut être surveillé par le programme de l'automate en utilisant le bloc MSTR ou MBP_MSTR pour lire les statistiques locales. Ces blocs fournissent des informations sur l'état du module et de la liaison Ethernet à partir du module jusqu'au premier concentrateur ou commutateur.

Le mot 3 des données renvoyées est défini comme l'état de la carte.

N° de bit	Définition
15...12	Type de module
11	(Réservé)
10	0 = semi-duplex 1 = full duplex
9	0 = non configuré 1 = configuré
8	0 = l'automate ne fonctionne pas 1 = l'automate/NOE fonctionne
7	0 = Voyant Link éteint 1 = Voyant Link allumé
6	0 = Voyant Appl éteint 1 = Voyant Appl allumé
5	0 = paire torsadée 1 = fibre optique
4	0 = 10 Mbits 1 = 100 Mbits
3...0	(Réservé)

Le bit 7 (Voyant Link allumé) peut être surveillé pour déterminer l'état de la connexion du module au concentrateur ou au commutateur local. Si le module Ethernet est défaillant, une erreur est renvoyée par la commande de lecture des statistiques locales.

NOTE : La commande de lecture des statistiques locales ne surveille que la connexion locale. Elle ne garantit que le réseau complet requis pour communiquer avec un équipement distant est intact (par exemple des concentrateurs ou des commutateurs supplémentaires, utilisés pour la connexion à l'autre équipement). Elle ne vérifie pas le fonctionnement de l'équipement distant. La surveillance d'équipements par des chiens de garde est une méthode plus fiable pour déterminer l'état des communications à un équipement distant.

Surveillance des équipements par des chiens de garde

Pour surveiller complètement le fonctionnement d'un équipement distant et la connexion à celui-ci, un chien de garde doit être utilisé. Pour mettre en œuvre un chien de garde d'un système SCADA vers un automate, envoyez un seul registre d'écriture du système SCADA à un registre de l'automate. L'automate incrémente ce registre, le SCADA lit la nouvelle valeur, incrémente de nouveau la valeur, puis écrit cette dernière. Le cycle se poursuit constamment.

Le chien de garde surveille les opérations de la liaison réseau complète entre les deux équipements ainsi que les opérations des systèmes d'automate et des systèmes SCADA. Il informe les deux équipements en cas de panne de l'un des équipements ou du réseau. Un chien de garde plus simple peut être mis en œuvre en faisant lire par l'automate une valeur sur un équipement distant ou en lisant une valeur qui change de façon connue (par exemple un compteur) sur cet équipement distant. Ces deux méthodes vérifient la liaison réseau, mais ne permettent pas à l'équipement distant de connaître l'état de l'automate.

NOTE : Lors de la mise en œuvre de chiens de garde via un registre incrémenté, tenez compte de la situation de redémarrage du registre (par exemple de 32767 à 0).

Surveillance de l'unité redondante

Lorsque vous mettez en œuvre un système de redondance d'UC dans lequel les liaisons de communication sont surveillées et dans lesquelles une liaison défaillante peut déclencher une permutation, vous devez connaître l'état de la liaison redondante. Toutes les liaisons non opérationnelles doivent être surveillées (liaisons de secours sur l'unité primaire et toutes les liaisons de l'automate redondant) pour détecter et corriger la défaillance de la liaison avant que celle-ci ne soit nécessaire.

L'état de la liaison redondante doit également être connue afin que l'automate puisse déterminer si la permutation rétablit les communications. Si des communications ne sont pas rétablies, la permutation n'améliore pas la redondance du contrôle de l'usine. De plus, une permutation peut avoir une incidence sur d'autres équipements.

Les liaisons de communication redondantes de l'automate primaire sont surveillées de la même manière que la liaison primaire. Elles peuvent être surveillées avec une commande de lecture des statistiques locales ou avec un chien de garde complet. Un chien de garde complet pour l'automate redondant est différent d'un chien de garde sur l'automate primaire car l'automate redondant ne traite pas toujours du code.

Utilisez les registres de transfert inversés du système de redondance d'UC pour transférer le registre écrit par le système SCADA vers l'automate primaire et incrémenter le registre à ce stade. Transférez ensuite le registre, soit de nouveau vers le système SCADA en utilisant les liaisons de communication de l'automate primaire, soit de nouveau vers l'automate redondant en utilisant la liaison redondante sur laquelle le système SCADA lit le résultat. Les systèmes de redondance d'UC Quantum actuels permettent l'exécution d'une petite quantité de code dans l'automate redondant. Le code peut permettre d'exécuter la commande de lecture des statistiques locales et de placer les résultats dans les registres de transfert inversés pour le transfert à l'automate primaire.

Adresse IP de l'automate

Dans un système de redondance d'UC Quantum, l'adresse IP des modules Ethernet du rack redondant est automatiquement définie sur l'adresse IP du module Ethernet du rack primaire plus un. Par exemple, si le module NOE du rack primaire a l'adresse 192.168.1.10, le NOE du rack redondant a l'adresse 192.168.1.11. Lorsque le système effectue une permutation, les adresses IP des modules Ethernet permutent également. Ceci simplifie la programmation de la communication pour les autres équipements car ils peuvent toujours communiquer vers une adresse IP unique. Cette fonction est disponible avec la version 2.0 ou supérieure du fichier exécutable des modules NOE 77100/10.

Permutation manuelle des automates avec redondance d'UC

Le code automate d'un automate Quantum peut déclencher la permutation d'un système de redondance d'UC avec le mot de commande de redondance d'UC. Pour que le système change de l'unité primaire à l'unité redondante, l'automate primaire définit le bit pour indiquer qu'il est hors ligne. Après la permutation, le nouvel automate primaire peut être utilisé pour redéfinir l'automate d'origine en ligne. Puisqu'il existe déjà un automate primaire fonctionnant dans le système, l'automate primaire d'origine retourne en ligne en tant qu'automate redondant.

NOTE : La configuration manuelle de l'automate primaire hors ligne pour forcer une permutation ne fonctionne que si l'unité redondante est disponible et est en mesure de passer en ligne. Assurez-vous que le code automate vérifie ce point en utilisant le mot de l'état de redondance avant le déclenchement d'un changement par ce code. Si vous ne le faites pas, les deux automates risquent de passer hors ligne.

Problème courant (instabilité)

Instabilité est le terme utilisé en cas de problème dans un système de redondance d'UC mis en oeuvre avec plusieurs chemins de communication. Il décrit une situation dans laquelle un équipement (par exemple le système SCADA) tente de communiquer en utilisant une liaison de communication (par exemple vers l'automate redondant) pour déterminer si cette liaison est la bonne. L'automate primaire attend un chien de garde valide de communications du système SCADA. Aucun des deux systèmes n'étant en mesure de recevoir un chien de garde valide de communications, chacun essaie un nouveau chemin. Si les deux systèmes permutent au même moment, ils ne font que continuer à permuter et n'établissent jamais de communications sur la même liaison.

Pour éviter l'instabilité :

- Surveillez les liaisons de communication actives des chiens de garde, y compris les liaisons dans l'automate redondant.
- Définissez clairement un système maître, par exemple l'automate primaire. Si l'automate primaire voit les communications vers le système SCADA sur les liaisons de l'automate primaire et les liaisons de l'automate redondant, il ne permute pas. Il attend que le système SCADA établisse les communications sur la liaison correcte (dans le cas d'une liaison vers l'automate primaire).
- Définissez des délais différents pour les tentatives d'établissement des liaisons de communication par le système SCADA et l'automate. Si l'automate est le système maître, il doit attendre et surveiller sa liaison actuelle pendant le délai requis pour que le système SCADA tente d'établir les communications sur toutes les liaisons possibles. Après ce délai seulement l'automate peut basculer sur une autre liaison de communication.

Permutation de redondance d'UC et services Ethernet

Services disponibles

Les services suivants sont disponibles dans un système de redondance d'UC :

Service	Description
Client Modbus	Exécuté dans les automates primaire et redondant. Seule la première section de l'application de l'automate fonctionne dans l'unité redondante pour déclencher des requêtes du client Modbus.
Serveur Modbus	Exécuté dans les automates primaire et redondant. Les requêtes adressées à l'automate redondant sont traitées par l'UC redondante ; les données d'écriture Modbus peuvent être remplacées suite au transfert des données redondantes.
Scrutateur d'E/S	Exécuté dans l'automate primaire, arrêté dans l'automate redondant
Global Data	Exécuté dans l'automate primaire ; l'automate redondant peut envoyer certains messages de maintenance au démarrage mais ne publie pas de données et n'y souscrit pas
FTP/TFTP	Exécuté dans les automates primaire et redondant
SNMP	Exécuté dans les automates primaire et redondant
SMTP	Exécuté dans les automates primaire et redondant ; les messages électroniques de l'automate redondant ne peuvent être déclenchés que dans la première section de l'application de l'automate (la seule section qui fonctionne)
NTP	Exécuté dans les automates primaire et redondant ; le module de communication Ethernet primaire configure l'horloge de l'UC primaire, tandis que le module de communication Ethernet redondant configure l'horloge de l'UC redondante. L'horloge NTP n'est pas transférée entre les UC primaire et redondante.
Web (intégré et FactoryCast)	Exécuté dans les automates primaire et redondant en tant que services indépendants

Services non disponibles

Le service FDR (*voir page 226*) n'est pas proposé car le serveur DHCP n'est pas disponible.

Opération de permutation

En cas de permutation de l'automate primaire vers l'automate redondant, la fonction de permutation des adresses IP affecte automatiquement l'adresse IP du module de communication Ethernet de l'automate primaire au module de communication Ethernet située dans l'automate redondant. La permutation est transparente pour les autres équipements du réseau. Après avoir fermé les connexions courantes client/serveur et du scrutateur d'E/S sur Ethernet à l'aide d'une réinitialisation, chaque module de communication Ethernet envoie un message de permutation UDP au module de communication Ethernet de l'autre automate. Le module de communication Ethernet qui envoie le message attend la réponse de l'autre module de communication Ethernet ou attend environ 500 ms. Dès que le message est reçu ou une fois le délai dépassé, l'adresse IP permute.

Au cours de la permutation, toutes les communications de messagerie Modbus en cours (client ou serveur) sont abandonnées et doivent être renvoyées. Tout bloc MSTR ou de lecture/écriture au niveau de l'application de l'automate doit être redéclenché, et toute requête distante (par exemple, SCADA) doit être renvoyée par l'équipement distant.

Le service I/O Scanning doit rétablir l'adresse MAC (via des requêtes ARP) et les connexions de socket vers chaque équipement distant avant la reprise du transfert des données. Le temps requis dépend du temps nécessaire à l'équipement distant pour répondre à la nouvelle demande d'ouverture de socket.

NOTE : Chaque ligne du scrutateur d'E/S est une entrée indépendante ; chacune commence le transfert des données à une heure différente. Le scrutateur d'E/S a uniquement besoin de l'adresse MAC et du socket de l'équipement apparaissant sur une ligne pour pouvoir lancer la communication avec ce dernier. Le scrutateur d'E/S commence donc à communiquer avec chaque équipement lorsque chacun est prêt, plutôt que d'attendre que tous soient prêts.

Pour le service Global Data, le module NOE redondant quitte le groupe Global Data et le nouveau module primaire rejoint le groupe et démarre la publication. Le temps nécessaire dépend de la mise en œuvre du filtrage de multidiffusion (*voir page 149*) et du nombre d'équipements présents dans le groupe (temps de démarrage Global Data).

Tous les autres services forcent les clients à se déconnecter (opération de réinitialisation ou expiration du délai). Les services sont redémarrés sur les modules de communication Ethernet primaire et redondant. Ils deviennent alors indisponibles pendant une courte durée, sans pour autant affecter le fonctionnement global du système. Par exemple, pendant que le service NTP redémarre, l'horloge de l'UC conserve sa précision. Une session Telnet est déconnectée et vous devez vous reconnecter.

Les versions les plus récentes des E/S distribuées sur Ethernet TCP/IP possèdent une fonction permettant de conserver l'état des sorties en cas de rupture des communications (par exemple, en cas de permutation de redondance d'UC). Les équipements contrôlés par les E/S distribuées continuent de fonctionner pendant la permutation.

Numéro des sockets TCP

Dans tous les cas, les sockets TCP sources utilisés sur le nouveau et l'ancien module doivent être différents. L'utilisation de sockets différents évite la confusion entre les anciennes et les nouvelles connexions à l'équipement distant.

3.15 Systèmes de passerelle/pont

Vue d'ensemble

Cette section présente les systèmes de passerelle et de pont.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

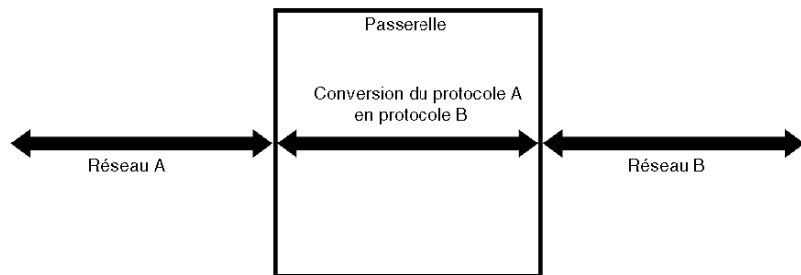
Sujet	Page
Vue d'ensemble des passerelles et des ponts	336
Fonctionnement des passerelles et des ponts	340

Vue d'ensemble des passerelles et des ponts

Récapitulatif

Une passerelle permet aux équipements d'un réseau de communiquer avec les équipements d'un autre réseau en remplaçant le protocole d'un côté par le protocole de l'autre côté. Les passerelles, également appelées ponts, sont utilisées dans un système Ethernet pour convertir un type de réseau à un autre (par ex. d'Ethernet coaxial à paire torsadée, de Token Ring à Ethernet).

L'illustration suivante présente le protocole A d'un côté et le protocole B de l'autre avec un message allant de l'un à l'autre.



Fonctionnement

Les passerelles peuvent être groupées en trois types différents, selon le mode d'activation de la communication des équipements sur les deux réseaux connectés, comme suit :

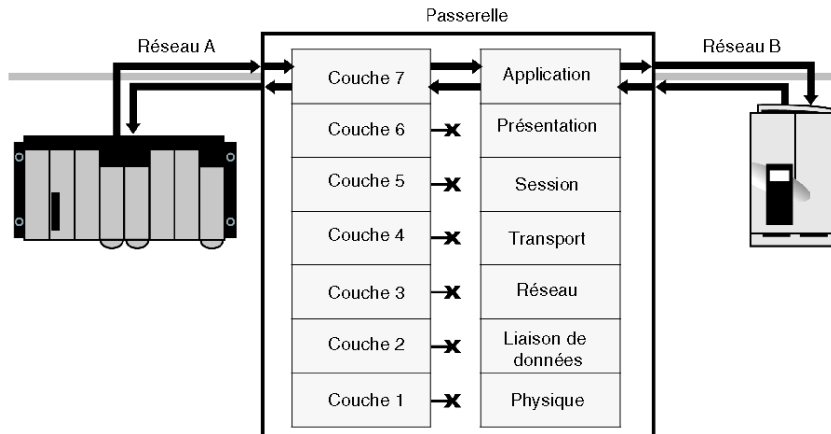
- passerelle sans conversion de protocole
- passerelle avec conversion de protocole
- passerelle utilisant une mémoire partagée (lecture et écriture)

Passerelle sans conversion de protocole d'application

Une passerelle sans conversion de protocole peut prendre un message du réseau source et le transmettre au réseau cible sans modifier le protocole d'application. La passerelle attend une réponse, puis la retransmet au réseau source. Ce type de passerelle correspond à la mise en œuvre la plus efficace et la plus puissante car aucune limite ne s'applique au protocole. Cependant, cette passerelle n'est envisageable que si les réseaux source et cible utilisent le même protocole de couche d'application. Les passerelles Modbus Ethernet à Modbus série et Ethernet à Modbus Plus de Schneider sont des exemples de ce type de passerelle.

NOTE : Une modification mineure du message d'application est apportée dans le processus de conversion d'Ethernet à Modbus Plus ou à Modbus série ; un index de pont et une ID de transaction sont inclus dans un paquet Ethernet Modbus, mais ils ne sont pas présents au niveau de la couche d'applications pour Modbus Plus ou Modbus série. Sur Modbus Plus, l'index de pont fait partie de l'adressage utilisé par les couches inférieures. Sur Modbus série, l'index n'est pas requis. Aucune ID de transaction n'est requise sur quelque système que ce soit.

Ce type de passerelle reçoit le paquet contenant le message de la couche d'application et supprime les couches inférieures avant de transmettre le message au réseau cible. Le message réel n'étant pas interprété, le temps de réponse total du système peut être plus faible et vous pouvez utiliser des fonctions prises en charge par les deux réseaux.

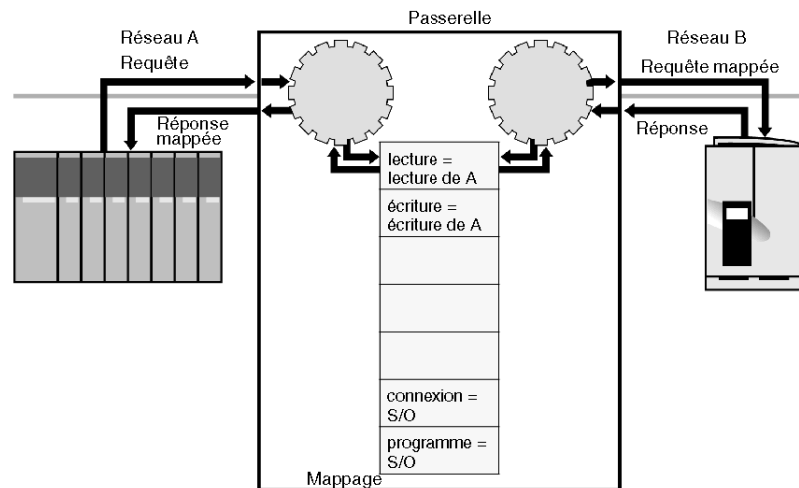


Passerelle avec conversion de protocole d'application

Une passerelle avec conversion de protocole prend un message du réseau source et le convertit au format de message de destination approprié, puis l'envoie au réseau cible. La passerelle attend alors une réponse, puis la convertit avant de la renvoyer au réseau source. En réalité, la passerelle lit le message d'application du réseau source, mais se réfère à une table interne pour rechercher le message à envoyer au réseau cible.

Cette conversion est requise lorsque les réseaux source et cible n'utilisent pas le même protocole de couche d'application. Les passerelles qui utilisent ce système incluent celles qui connectent les réseaux Modbus aux réseaux d'autres fournisseurs. Comme le message du réseau source doit être reçu et interprété avant qu'un message sortant ne soit envoyé, ce type de passerelle est plus lent qu'une passerelle qui ne réalise pas de conversion du protocole d'application.

Les règles de conversion du protocole sont basées sur des règles définies par le concepteur de la passerelle ; seuls les messages identifiés par le concepteur peuvent être convertis. Les messages définis après la conception de la passerelle ne sont pas convertis. Vous ne pouvez normalement pas modifier le mappage des messages d'un réseau à l'autre. Ce type de passerelle est uniquement en mesure de mapper un message simple pour lequel il existe un équivalent sur les deux réseaux. Les messages sans équivalent sur l'autre réseau ne peuvent pas être mappés. Il en résulte qu'il n'est pas possible de programmer par-dessus ce type de passerelle.

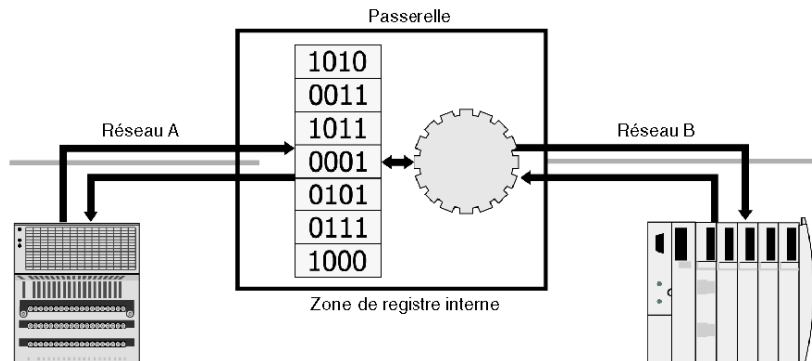


Passerelles utilisant une mémoire partagée

Certaines passerelles peuvent présenter une zone de mémoire partagée aux équipements des deux réseaux. Les équipements des deux réseaux peuvent lire ou écrire des données de cette zone de mémoire et partager des données même si aucun message n'est réellement transmis d'un réseau à l'autre. Un équipement du réseau source peut écrire des données dans la zone de mémoire partagée, et un équipement du réseau cible peut ensuite les lire à partir de cette même zone.

Une passerelle de ce type ne transmet jamais réellement de message du réseau source au réseau cible. Aucune programmation n'est requise et aucun message complexe n'est transmis. Seules les données utilisant les types de mémoire présentés dans la zone de mémoire partagée peuvent être transférées. Par exemple, si seuls les mots sont pris en charge, la transmission de bits individuels n'est pas acceptée.

Cette passerelle découple les deux réseaux. Du fait qu'elle n'attend pas de réponse du réseau cible avant de répondre à la requête, cette passerelle peut répondre très rapidement en utilisant les données de sa zone de mémoire partagée. Bien que cette passerelle semble être très rapide, le temps de réponse réel est long car toutes les données doivent être traitées deux fois : une première fois dans la mémoire partagée et une deuxième fois sur l'autre réseau. Ces deux tâches ne sont pas synchronisées, ce qui induit que le temps de réponse du système est long et irrégulier.



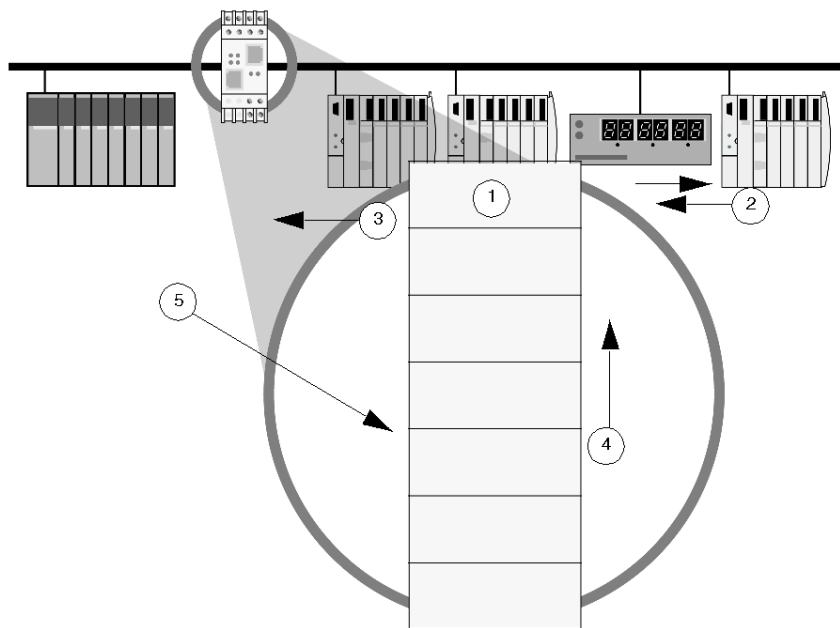
Fonctionnement des passerelles et des ponts

Files d'attente

Si les équipements d'un réseau envoient des requêtes à la passerelle plus rapidement que la durée nécessaire à leur traitement sur le réseau cible, une file d'attente de messages se forme à l'intérieur de la passerelle. Selon la passerelle, la file d'attente peut être limitée à une longueur maximale définie. Une fois que la file d'attente est pleine, la passerelle se bloque ou renvoie une nouvelle requête de message avec une réponse d'erreur.

Prenez en considération le temps de réponse du réseau cible et l'effet d'un timeout concernant les files d'attente à l'intérieur de la passerelle du réseau cible. Pour éviter qu'une file d'attente grandisse de manière démesurée, les équipements émettant des requêtes ne doivent pas envoyer de tentative de message avant que la passerelle n'ait traité le message : ils doivent attendre la réception d'une réponse ou d'un message d'erreur avant d'envoyer la tentative. Les équipements doivent conserver une trace des messages envoyés à la passerelle, pour lesquels ils n'ont pas reçu de réponse ; ce nombre doit être maintenu aussi bas que possible.

La file d'attente affecte le temps de réponse système. Si un équipement source envoie une commande à l'équipement du réseau cible, celle-ci doit, avant d'être traitée, rester dans la file d'attente jusqu'à ce que tous les messages en attente soient envoyés. Ce phénomène peut engendrer des temps de réponse système longs. Pour atteindre des temps de réponse optimaux, la file d'attente ne doit jamais être vide et contenir 1 ou 2 messages maximum.



- 1 requête en attente
- 2 réponse
- 3 réponse au client
- 4 toutes les requêtes montent dans la file d'attente
- 5 une nouvelle requête est placée à la fin de la file d'attente

Sockets de passerelle

Une passerelle permet à un grand nombre d'équipements d'un réseau de communiquer avec un grand nombre d'équipements sur un autre réseau. Lorsque de nombreux équipements se connectent à une passerelle réseau Ethernet, beaucoup de sockets TCP doivent être ouverts. Pour les passerelles bon marché, le nombre de sockets est limité par la faible puissance de traitement et le peu de mémoire des composants choisis. Une fois que ce nombre de sockets est dépassé, aucun équipement supplémentaire ne peut se connecter à la passerelle. Des problèmes peuvent survenir lorsque :

- les équipements émettant la requête choisissent des services de communications qui requièrent un socket TCP pour chaque équipement avec lequel ils communiquent ;
- les services conservent un socket ouvert une fois que les communications sont terminées.

Parmi ces services se trouvent notamment le service de scrutateur d'E/S et le service client Modbus sur les équipements plus anciens. Pour réduire le nombre de sockets maintenus ouverts sur une passerelle, utilisez la fonction d'activation/désactivation dans les requêtes du scrutateur d'E/S ou du client Modbus.

Timeouts de passerelle

Lorsqu'une passerelle envoie un message au réseau cible, ce message suit le timeout et les délais d'attente du réseau en question. Cependant, l'équipement a envoyé un message à la passerelle, lequel se conforme au timeout et aux délais d'attente du réseau source.

Si la durée totale du timeout et des tentatives sur le réseau cible est supérieure au timeout du réseau source, ce dernier renvoie la requête. Les messages en double sont placés dans la file d'attente. Lorsque Modbus TCP/IP est le réseau source, aucune tentative de couche d'application n'est réalisée et tant que la passerelle accuse réception du paquet TCP, il n'y a aucune tentative sur le réseau source. Toutefois, vous pouvez renvoyer manuellement le même message.

Si le premier message de la file d'attente est envoyé à un équipement déconnecté, ce message expire et une nouvelle tentative d'envoi est effectuée. Tous les autres messages de la file d'attente sont reportés et éventuellement considérés comme expirés par l'équipement émettant la requête. Si ces messages expirent, ce dernier peut renvoyer le message, ce qui génère un grand nombre de messages dans la file d'attente. Lorsque le message initial reçoit une réponse de la passerelle, il est ignoré par l'équipement émettant la requête car il a déjà été considéré comme expiré.

Pour éviter cette situation, le timeout de tous les messages envoyés à partir du réseau source doit être défini de sorte qu'il soit supérieur à :

timeout x nombre de tentatives sur le réseau cible x nombre maximum de requêtes attendu dans la file d'attente

Évitez de trop laisser grandir cette valeur. Définissez une valeur faible pour le nombre de tentatives sur le réseau cible et n'envoyez pas de requête aux équipements que vous savez indisponibles. Si un équipement est normalement interrogé toutes les 5 secondes mais qu'il a renvoyé 2 erreurs de suite, contrôlez l'équipement une fois toutes les 30 secondes pour vérifier qu'il est en mesure de répondre à nouveau.

Temps de réponse

Les temps de réponse pour les systèmes de passerelle Schneider sont indiqués dans l'annexe A (*voir page 411*).

Problèmes courants

Les problèmes courants rencontrés avec les systèmes de passerelle comprennent :

- les passerelles surchargées en raison des équipements réseau qui envoient des requêtes plus rapidement que la durée nécessaire à leur traitement sur le réseau cible ;
- les erreurs de communications vers l'un ou tous les équipements de destination lorsqu'un équipement de destination unique est retiré, causées par des timeouts qui affectent la rapidité du traitement des communications sur le réseau de destination et produisent des surcharges ;
- les requêtes expirées émanant de l'équipement source avant que le message ne soit traité sur le réseau cible, causées par le paramétrage incorrect des valeurs de timeout ou par la méconnaissance des conséquences de la mise en attente de messages dans la passerelle ;
- l'incapacité à se connecter à la passerelle du fait que toutes les connexions de socket sont en cours d'utilisation.

3.16 Services pris en charge par équipement

Services Ethernet et équipements Transparent Ready qui les prennent en charge

Equipements Quantum

Le tableau suivant énumère les services Ethernet pris en charge par les UC Quantum avec ports Ethernet intégrés et par les modules de communication Ethernet Quantum :

Service	140CPU65150	140CPU65160	140NOE77101	140NOE77111	140NWM10000
Scrutateur d'E/S	X	X	X	X	-
Serveur Modbus	X	X	X	X	X
Client Modbus	X	X	X	X	X
Global Data	X	X	X	X	-
Serveur FDR	X	X	X	X	-
Client FDR	-	-	-	-	-
Client BootP	X	X	X	X	X
Synchronisation horaire	-	-	-	X	-
Notification par message électronique	X	X	X	X	X
Diagnostics Web/intégrés	X	X	X	X	X
Serveur Web FactoryCast	-	-	-	X	X
Serveur Web FactoryCast HMI	-	-	-	-	X
SNMP	X	X	X	X	X
Serveur FTP	X	X	X	X	X
Serveur TFTP	X	X	X	X	-
Serveur Telnet	X ¹	X ¹	X ¹	X ¹	X ¹
¹ A des fins de diagnostic en usine seulement.					

UC Premium

Le tableau suivant énumère les services Ethernet pris en charge par les UC Premium avec ports Ethernet intégrés :

Service	TSXP571634M	TSXP572634M	TSXP573634M	TSXP574634M	TSXP575634M
Scrutateur d'E/S	X	X	X	X	X
Serveur Modbus	X	X	X	X	X
Client Modbus	X	X	X	X	X
Global Data	X	X	X	X	X
Serveur FDR	X	X	X	X	X
Client FDR	-	-	-	-	-
Client BootP	X	X	X	X	X
Synchronisation horaire	-	-	-	-	-
Notification par message électronique	X	X	X	X	X
Diagnostics Web/intégrés	X	X	X	X	X
Serveur Web FactoryCast	-	-	-	-	-
SNMP	X	X	X	X	X
Serveur FTP	X	X	X	X	X
Serveur TFTP	X	X	X	X	X
Serveur Telnet	X ¹	X ¹	X ¹	X ¹	X ¹
¹ A des fins de diagnostic en usine seulement.					

Modules de communication Ethernet Premium

Le tableau suivant énumère les services Ethernet pris en charge par les modules de communication Ethernet Premium :

Service	TSXETY4103	TSXETY110WS	TSXETY5103	TSXWMY100
Scrutateur d'E/S	X	-	X	-
Serveur Modbus	X	X	X	X
Client Modbus	X	X	X	X
Global Data	X	-	X	-
Serveur FDR	X	-	X	-
Client FDR	-	-	-	-
Client BootP	X	X	X	X
Synchronisation horaire	-	-	X	-
Notification par message électronique	X	-	X	X

Service	TSXETY4103	TSXETY110WS	TSXETY5103	TSXWMY100
Diagnostics Web/intégrés	X	X	X	X
Serveur Web FactoryCast	-	X	X	X
Serveur Web FactoryCast HMI	-	-	-	X
SNMP	X	X	X	X
Serveur FTP	X	X	X	X
Serveur TFTP	X	-	X	-
Serveur Telnet	X ¹	X ²	X ²	X ¹

¹ A des fins de diagnostic en usine seulement.

Modules de communication Ethernet TSX Micro

Le tableau suivant énumère les services Ethernet pris en charge par les modules de communication Ethernet TSX Micro :

Service	TSXETZ410	TSXETZ510
Scrutateur d'E/S	-	-
Serveur Modbus	X	X
Client Modbus	X	X
Global Data	-	-
Serveur FDR	-	-
Client FDR	X	X
Client BootP	X	X
Synchronisation horaire	-	-
Notification par message électronique	-	-
Diagnostics Web/intégrés	X	X
Serveur Web FactoryCast	-	X
SNMP	X	X
Serveur FTP	X	X
Serveur TFTP	-	-
Serveur Telnet	X ¹	X ¹

¹ A des fins de diagnostic en usine seulement.

Processeurs Momentum M1E

Le tableau suivant énumère les services Ethernet pris en charge par les modules processeurs Momentum M1E :

Service	171CCC96020	171CCC96030	171CCC98020	171CCC98030
Scrutateur d'E/S	X	X	X	X
Serveur Modbus	X	X	X	X
Client Modbus	X	X	X	X
Global Data	-	-	-	-
Serveur FDR	-	-	-	-
Client FDR	-	-	-	-
Client BootP	X	X	X	X
Synchronisation horaire	-	-	-	-
Notification par message électronique	-	-	-	-
Diagnostics Web/intégrés	X	X	X	X
Serveur Web FactoryCast	-	-	-	-
SNMP	-	-	-	-
Serveur FTP	-	-	-	-
Serveur TFTP	-	-	-	-

Modules de communication Ethernet Momentum

Le tableau suivant énumère les services Ethernet pris en charge par les modules de communication Ethernet Momentum :

Service	170ENT11001	170ENT11002
Scrutateur d'E/S	-	-
Serveur Modbus	X	X
Client Modbus	-	-
Global Data	-	-
Serveur FDR	-	-
Client FDR	X	-
Client BootP	X	X
Synchronisation horaire	-	-
Notification par message électronique	-	-
Diagnostics Web/intégrés	X	-
Serveur Web FactoryCast	-	-
SNMP	X	-

Service	170ENT11001	170ENT11002
Scrutateur d'E/S	-	-
Serveur FTP	X	-
Serveur TFTP	-	-
Serveur Telnet	X ¹	-
¹ A des fins de diagnostic en usine seulement.		

Equipements Twido

Le tableau suivant énumère les services Ethernet pris en charge par une UC Twido et un module de communication Ethernet Twido :

Service	TwidoPort 499TWD01100
Scrutateur d'E/S	-
Serveur Modbus	X ¹
Client Modbus	X ¹
Global Data	-
Serveur FDR	-
Client FDR	-
Client BootP	X
Synchronisation horaire	-
Notification par message électronique	-
Diagnostics Web/intégrés	-
Serveur Web FactoryCast	-
SNMP	-
Serveur FTP	X
Serveur TFTP	-
Serveur Telnet	X
¹ L'équipement reçoit et envoie les messages Modbus en agissant comme une passerelle.	

Système d'E/S distribuées Advantys STB

Le tableau suivant énumère les services Ethernet pris en charge par un module d'interface réseau (NIM) Ethernet standard Advantys STB :

Service	STBNIP2212
Scrutateur d'E/S	-
Serveur Modbus	X

Service	STBNIP2212
Client Modbus	-
Global Data	-
Serveur FDR	-
Client FDR	X
Client BootP	X
Synchronisation horaire	-
Notification par message électronique	-
Diagnostics Web/intégrés	X
Serveur Web FactoryCast	-
SNMP	X
Serveur FTP	X
Serveur TFTP	-
Serveur Telnet	-
¹ L'équipement peut être scruté par le scrutateur d'E/S lorsqu'il met en œuvre le serveur Modbus.	

Variateur de vitesse Altivar ATV 38/58

Le tableau suivant énumère les services Ethernet pris en charge par la carte VW3A58310 du variateur de vitesse Altivar ATV 38/58 :

Service	VW3A58310
Scrutateur d'E/S	-
Serveur Modbus	X
Client Modbus	-
Global Data	-
Serveur FDR	-
Client FDR	X
Client BootP	X
Synchronisation horaire	-
Notification par message électronique	-
Diagnostics Web/intégrés	X
Serveur Web FactoryCast	-
SNMP	-
Serveur FTP	-
Serveur TFTP	-
Serveur Telnet	-

Passerelles/ponts Power Logic

Le tableau suivant énumère les services Ethernet pris en charge par les passerelles Power Logic :

Service	EGX200	EGX400
Scrutateur d'E/S	-	-
Serveur Modbus	X ¹	X ¹
Client Modbus	-	-
Global Data	-	-
Serveur FDR	-	-
Client FDR	-	-
Client BootP	X	X
Synchronisation horaire	-	-
Notification par message électronique	-	-
Diagnostics Web/intégrés	X	X
Serveur Web FactoryCast	-	-
SNMP	X	X
Serveur FTP	X	X
Serveur TFTP	-	-
Serveur Telnet	X	X
¹ L'équipement reçoit et envoie les messages Modbus en agissant comme une passerelle.		

Systèmes de câblage ConneXium

Le tableau suivant énumère les services Ethernet pris en charge par les commutateurs gérés ConneXium NES/NOS et les passerelles CEV :

Service	499NES17100	499NOS17100	174CEV30020	174CEV20030	174CEV20040
Scruteur d'E/S	-	-	-	-	-
Serveur Modbus	-	-	X ¹	X ¹	X ¹
Client Modbus	-	-	X ¹	X ¹	X ¹
Global Data	X ²	X ²	-	-	-
Serveur FDR	-	-	-	-	-
Client FDR	-	-	-	-	-
Client BootP	X	X	X	X	X
Synchronisation horaire	-	-	-	-	-
Notification par message électronique	-	-	-	-	-
Diagnostics Web/intégrés	X	X	-	-	X
Serveur Web FactoryCast	-	-	-	-	-
SNMP	X	X	X	X	X
Serveur FTP	X	X	-	-	X
Serveur TFTP	-	-	X	X	-
Serveur Telnet	X	X	X ³	X ³	-
¹ L'équipement reçoit et envoie les messages Modbus en agissant comme une passerelle.					
² Prise en charge du filtrage de multidiffusion pour Global Data.					
³ A des fins de diagnostic en usine seulement.					

3.17 Evaluation des performances système

Vue d'ensemble

Cette section explique comment obtenir des temps de réponse système pour chacune des communications choisies dans votre usine. Elle décrit également les contrôles devant être effectués sur les équipements et le réseau pour que la charge globale de messages d'un équipement ne dépasse pas ses capacités et que la charge globale du réseau n'entraîne pas des retards de communications.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Communications système	353
Temps de réponse de la messagerie Modbus	353
Temps de réponse du serveur Modbus	354
Temps de réponse du client de messagerie Modbus	359
Scrutateurs d'E/S	363
Charge totale sur les équipements	365
Solutions pour les performances système	366
Temps de réponse de la passerelle	372

Communications système

Récapitulatif

Les performances de l'architecture Ethernet sont liées au matériel et aux services d'application utilisés, ainsi qu'aux paramètres définis pour ces services.

Considérations matérielles

- bande passante du réseau
- ressources du module ou de l'UC avec Ethernet
- ressources du processeur intégré (automate, PC ou autres UC)

Services d'application

- service de traitement de messagerie industrielle Modbus (ou Uni-TE)
- service Global Data, analyse de données entre automates
- service I/O Scanning, analyse de données d'E/S distribuées
- autres (accès Web, communication ouverte TCP)

Il est parfois difficile de déterminer la taille correcte d'une architecture du fait de l'interconnexion de ces paramètres.

Le temps de réponse de n'importe quel système est déterminé à l'aide des graphiques des annexes A à D, qui montrent des temps de réponse pour des exemples de systèmes ou de calculs utilisant des formules.

Temps de réponse de la messagerie Modbus

Le service de messagerie Modbus implique les composants suivants dans un transfert de données :

- client Modbus,
- transfert réseau,
- serveur Modbus.

Ces composants sont les mêmes pour tous les systèmes de messagerie Modbus. Pour déterminer le temps de réponse d'un système Modbus, il est nécessaire de calculer la synchronisation de chaque élément ci-dessus. Chaque composant peut être calculé séparément, pour permettre ensuite de déterminer le temps de réponse total.

Temps de réponse du serveur Modbus

Récapitulatif

Les temps de réponse du serveur Modbus peuvent être calculés à l'aide de l'une des deux méthodes suivantes :

- des temps de réponse mesurés, pour les durées globales pour tous les équipements (par ex. les automates) et en tant que valeur réelle pour les équipements simples (par ex. un VSD, un bloc d'E/S) ;
- un calcul basé sur le fonctionnement du système pour les équipements plus complexes tels que les systèmes d'automate Quantum ou Premium.

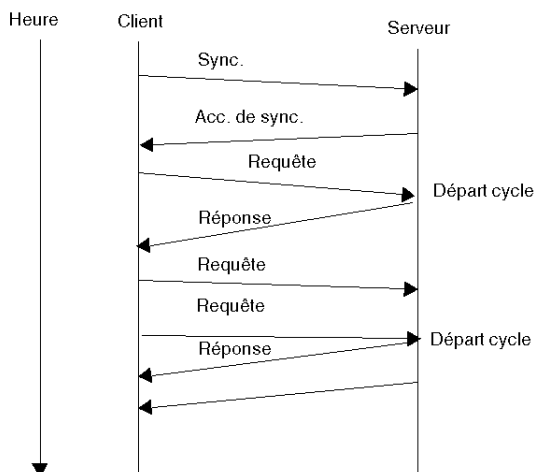
Les temps de réponse mesurés pour divers équipements serveur Schneider Modbus sont décrits dans une annexe (*voir page 441*). Ces temps de réponse ont été mesurés dans des conditions contrôlées et peuvent varier par rapport aux résultats obtenus sur le terrain. Ces graphiques sont valides uniquement si les limites globales des communications d'équipement sont respectées.

Les temps de réponse du serveur Modbus pour les équipements suivants ne sont pas fixes et doivent être calculés :

- Système d'automate Premium
- Système d'automate Momentum
- Système d'automate Quantum

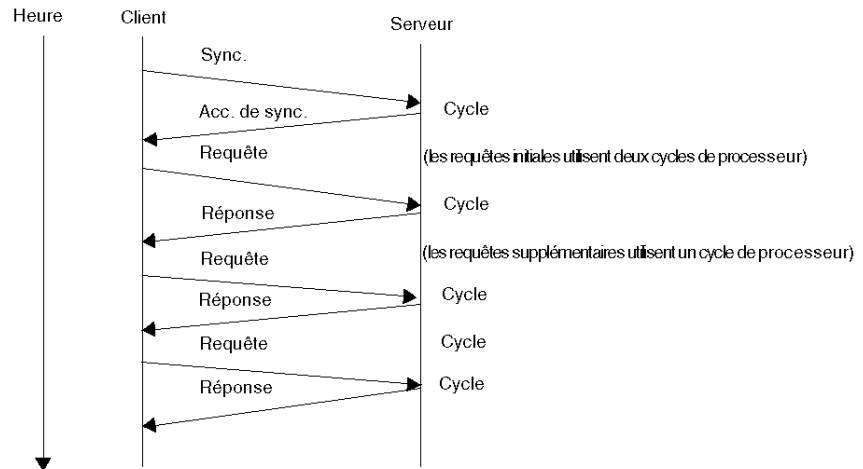
Système d'automate Premium

Le temps de réponse du système d'automate pour toutes les requêtes de messagerie Modbus reçues correspond à la durée d'un cycle de processeur. Toutes les requêtes de messagerie Modbus reçues pendant le cycle de processeur reçoivent une réponse avant le début du cycle suivant. Si le nombre total de requêtes de messagerie Modbus reçues par le processeur lors d'un même cycle est supérieur à la limite en vigueur pour ce type de processeur, toutes les requêtes supplémentaires reçoivent une réponse à la fin du même cycle. Néanmoins; la réponse en question pour ces requêtes est la réponse d'exception Modbus *Serveur occupé*, au lieu des données réelles demandées.



Système d'automate Momentum

Le temps de réponse du système d'automate Momentum pour toutes les requêtes de messagerie reçues correspond à la durée d'un cycle de processeur. Toutes les requêtes de messagerie Modbus reçues pendant le cycle de processeur reçoivent une réponse à la fin du cycle de processeur courant. L'automate requiert plusieurs cycles de processeur pour répondre à une requête initiale ; en effet, un socket TCP doit être établi, ce qui prend plusieurs cycles de processeur.



Système d'automate Quantum

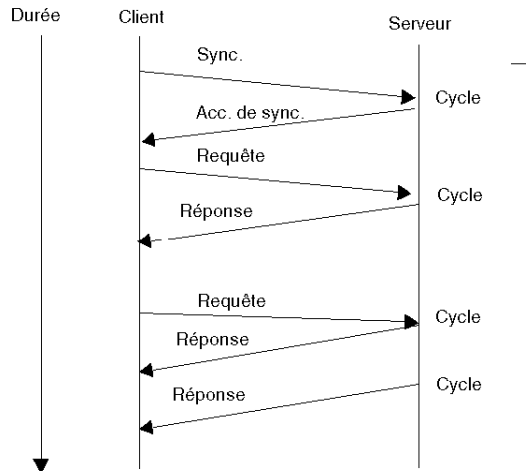
Le temps de réponse du système d'automate Quantum dépend du nombre de requêtes traitées.

Le système répond aux requêtes grâce à trois méthodes différentes :

- accès direct à la mémoire du processeur par les modules NOE ;
- transmission des requêtes au processeur à partir des modules NOE ;
- accès direct à l'aide d'un port Ethernet intégré sur le processeur.

Chacune de ces méthodes permet au système d'automate de répondre à un certain nombre de requêtes par cycle de processeur. Toutes requêtes parvenant au module Ethernet sont placées dans la file d'attente du module ; chaque port Ethernet possède sa propre file d'attente. A la fin du cycle de processeur, les requêtes sont traitées à partir du haut de la file d'attente. Toutes les requêtes sans réponse restent dans la file d'attente et sont traitées dans l'ordre de leur réception. Il peut s'écouler un ou plusieurs cycles avant que les nouvelles requêtes placées dans la file d'attente n'en atteignent le haut.

Si la file d'attente ne contient aucune requête, le temps de réponse d'une nouvelle requête arrivant sur le système d'automate est compris entre 0 ms et un cycle de processeur, selon le stade auquel la requête est parvenue dans le cycle de processeur.



S'il existe déjà des requêtes dans la file d'attente lorsqu'une nouvelle requête arrive, cette dernière est placée à la fin de la file. Elle sera traitée une fois parvenue en haut de la file d'attente. Le temps de réponse peut être calculé en divisant le nombre de requêtes dans la file d'attente par le nombre de requêtes pouvant être traitées par cycle de processeur, puis en multipliant par la durée du cycle de processeur.

NOTE : Chaque méthode possède sa propre file d'attente. Décidez de la file d'attente dans laquelle placer la nouvelle requête, puis effectuez les calculs sur la base du nombre de requêtes dans la file.

Vous devez ajouter quelques millisecondes aux temps obtenus ci-dessus afin de prendre en compte les surdébits éventuels. Ce temps est nettement inférieur à la durée du cycle de processeur et n'affecte pas particulièrement le résultat global.

Temps de réponse pour les équipements

Produit	Meilleur des cas	Moyenne	Pire des cas
Premium	1/2 ms	0,5 x cycle de processeur	1 cycle de processeur
Momentum	1/2 ms	0,5 x cycle de processeur	1 cycle de processeur ou 2 si la requête initiale ouvre un socket TCP. L'équipement client doit être en mesure de réaliser l'ouverture de socket dans un délai correspondant à un cycle de processeur pour que cette opération soit précise.
Port intégré ou NOE Quantum : pas de surcharge dans le nombre de requêtes, donc aucune requête dans la file d'attente	1/2 ms	0,5 x cycle de processeur	1 cycle de processeur
Registre de lecture/écriture NOE Quantum avec requêtes en surcharge	-	-	Nombre de requêtes dans la file d'attente / 8 x 1 cycle de processeur
Registre de non-lecture/écriture NOE Quantum avec requêtes en surcharge	-	-	Nombre de requêtes dans la file d'attente / 4 x 1 cycle de processeur
Port Ethernet intégré Quantum avec requêtes en surcharge	-	-	Nombre de requêtes dans la file d'attente / 16 x 1 cycle de processeur

Limites de communication pour la messagerie Modbus

Produit	Nombre de requêtes	Nombre de sockets TCP	Requêtes multiples par socket
Quantum : registre de lecture/écriture 4x NOE	8 / cycle de processeur par module NOE	64 par module NOE	oui
Quantum : registre de lecture/écriture non-4x NOE	4 / cycle de processeur par module NOE ¹	64 par module NOE	oui
Port Ethernet intégré Quantum	16 / cycle de processeur	64	oui
Premium TSXP571xx	4 / cycle de processeur	-	oui
Premium TSXP572xx	8 / cycle de processeur	-	oui
Premium TSXP573xx	12 / cycle de processeur	-	oui
Premium TSXP574xx	16 / cycle de processeur	-	oui
Premium TSXP575xx	16 / cycle de processeur	-	oui
Advantys	-	4	oui
ENT V1	-	4	-
ENT V2	-	4	-
Momentum	Illimité	16	non
¹ 20 / cycle de processeur maximum pour tous les NOE et ports intégrés			

Temps de réponse du client de messagerie Modbus

Récapitulatif

Le temps de réponse du client de messagerie Modbus fait partie du temps de réponse total du système de messagerie Modbus. Deux méthodes permettent de déterminer les temps de réponse du client Modbus :

- la prise en compte de tout le système de messagerie Modbus (client et serveur) en tant qu'unité
- le calcul séparé des temps des composants système

Dans le premier cas, le temps de réponse système total entre la requête du client et la réponse du serveur est mesuré. Dans le deuxième cas, des résultats plus spécifiques que les graphiques de temps total utilisés dans la première méthode sont fournis pour un système particulier.

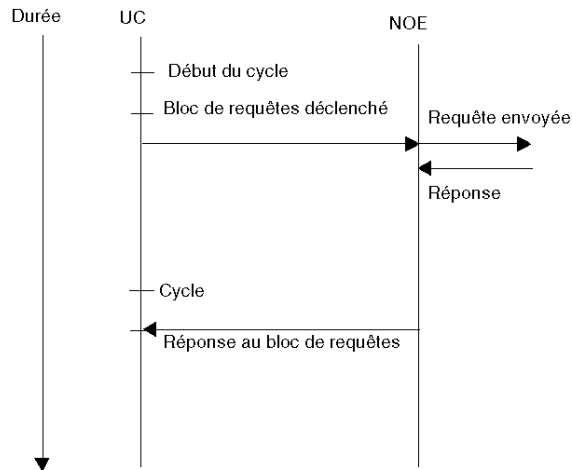
Les temps de réponse mesurés pour plusieurs systèmes client Modbus de Schneider basés sur différents temps de réponse serveur sont décrits dans une annexe (*voir page 447*). Ces temps de réponse ont été mesurés dans des conditions contrôlées et peuvent varier par rapport aux résultats obtenus sur le terrain. Les graphiques de cette annexe sont valides uniquement si les limites globales des communications d'équipements ne sont pas dépassées sur le client ou le serveur.

Les équipements suivants peuvent nécessiter le calcul du temps de réponse du client de messagerie Modbus dans la mesure où elle n'est pas fixe :

- système d'automate Quantum
- système d'automate Premium
- système d'automate Momentum
- système SCADA
- serveur OFS

Système d'automate Quantum

Pour un système Quantum, la requête de messagerie Modbus est envoyée immédiatement après le déclenchement de la fonction à l'intérieur de la logique utilisateur. Lorsque la réponse est reçue du serveur Modbus, elle est traitée dans la mémoire logique utilisateur lors du traitement suivant de la fonction d'appel. Ceci se passe normalement pendant le cycle du processeur juste après que le système automate a reçu le message.



S'il s'agit de la seule requête envoyée et qu'il n'y a pas de requêtes antérieures dans la file d'attente, le temps de réponse est :

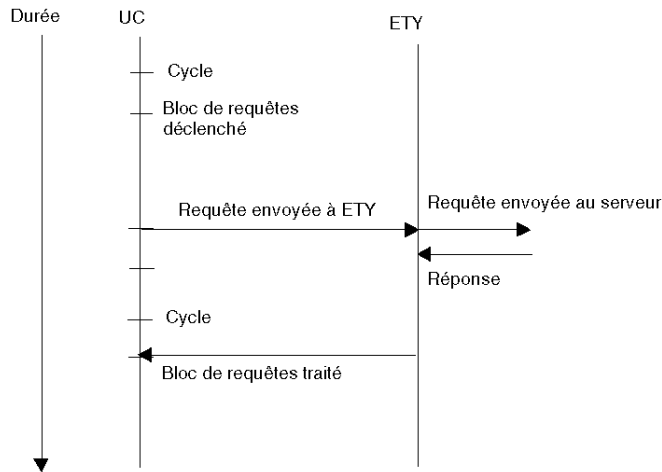
$$\text{temps de réponse} = \text{temps de réponse serveur} + 1 \text{ cycle de processeur}$$

Si le nombre maximum de requêtes client Modbus dépasse les limites du système, les requêtes de messagerie Modbus supplémentaires sont placées dans une file d'attente. Chaque fois que la fonction de requête est évaluée par l'UC, un contrôle est effectué pour voir si le nombre de requêtes en attente d'une réponse du serveur est inférieur au nombre maximum pris en charge par le système. Si c'est le cas, la requête suivante dans la file d'attente est envoyée au serveur. Le temps de réponse du client de messagerie Modbus est :

$$\text{temps de réponse} = \text{nombre de requêtes dans la file d'attente} \times (\text{temps de réponse du serveur Modbus pour chaque requête} + 1 \text{ cycle de processeur}) + \text{temps de réponse du serveur Modbus à la nouvelle requête} + 1 \text{ cycle de processeur}$$

Système d'automate Premium

Pour un système Premium, la requête de messagerie Modbus est envoyée à la fin du cycle du processeur juste après le déclenchement de la fonction à l'intérieur de la logique utilisateur. Lorsque la réponse est reçue du serveur Modbus, elle est traitée dans la mémoire logique utilisateur lors du traitement suivant de la fonction d'appel. Ceci se passe normalement pendant le cycle du processeur juste après que le système automate a reçu le message.



Pour un système Premium, le temps de réponse est :

$$\text{temps de réponse} = 1 \text{ cycle de processeur} + \text{temps de réponse serveur} + 1 \text{ cycle de processeur}$$

Si le nombre maximum de requêtes client Modbus est dépassé, les requêtes de messagerie Modbus supplémentaires sont refusées et ne sont pas envoyées ; une erreur est générée dans la logique utilisateur.

Système d'automate Momentum

Pour un système Momentum, chaque requête de messagerie Modbus nécessite l'ouverture d'un socket TCP pour pouvoir être envoyée. Le socket Modbus TCP est fermé à la fin de chaque requête. Le temps de réponse à la requête client Modbus est :

temps de réponse = 1 cycle de processeur (pour envoyer la requête du socket ouvert) + *temps de réponse serveur au socket ouvert* + 1 cycle de processeur (pour envoyer la requête) + *temps de réponse serveur Modbus* + 1 cycle de processeur (pour recevoir la réponse dans la logique utilisateur)

Si le nombre maximum de requêtes client Modbus est dépassé, les requêtes de messagerie Modbus supplémentaires sont refusées et ne sont pas envoyées ; une erreur est générée dans la logique utilisateur.

Limites de communication du client Modbus

Produit	Nombre de requêtes	Utilisation du socket TCP	Requêtes multiples par socket
Quantum NOE	16	Un par équipement distant	oui
Port Ethernet intégré Quantum	64	Un par équipement distant	oui
Premium TSXP571xx	16	Un par équipement distant	oui
Premium TSXP572xx	32	Un par équipement distant	oui
Premium TSXP573xx	48	Un par équipement distant	oui
Premium TSXP574xx	64	Un par équipement distant	oui
Premium TSXP575xx	80	Un par équipement distant	oui
Momentum	16	Un par requête de messagerie Modbus	non

Scrutateurs d'E/S

Vue d'ensemble

Le scrutateur d'E/S fonctionne différemment dans les systèmes d'automates Quantum et Premium (*voir page 183*). Le calcul du temps de réponse système pour chaque système dépend de plusieurs facteurs et se traduit par une formule compliquée. La formule est fournie à titre de référence, mais vous devriez vous reporter aux graphiques de l'annexe pour la plupart des systèmes (*voir page 413*). Ces graphiques fournissent les temps de réponse système du scrutateur d'E/S depuis :

- l'entrée terrain à la mémoire d'automate ;
- la mémoire d'automate à la sortie terrain ;
- l'entrée terrain à l'automate par le biais d'une décision et retour à une sortie terrain.

NOTE : Pour les calculs suivants, le taux de répétition du scrutateur d'E/S doit être réglé à 0 ms.

Tnet correspond à 0,05 ms à 10 Mo et 0,005 ms à 100 Mo. Pour des résultats plus précis, le temps de transmission réel du réseau peut être calculé en utilisant le nombre d'octets envoyés, le trafic réseau, la vitesse réseau et la latence du commutateur.

Tios correspond au nombre d'entrées dans la table du scrutateur d'E/S x 0,3 ms.

Formules des temps de réponse : Entrée terrain à la mémoire d'automate

Pour un système Quantum NOE, le temps de réponse depuis une entrée terrain aux informations de l'automate est donné par les deux formules suivantes :

$$\text{temps max} = T_{\text{mod}} + T_{\text{ios}} + T_{\text{net}} + 2 \text{ cycles de processeur}$$

$$\text{temps moyen} = T_{\text{mod}} + (T_{\text{ios}} \times 0,5) + T_{\text{net}} + 1,5 \text{ cycle de processeur}$$

Pour un système d'automate Premium ou un port Ethernet intégré Quantum, le temps de réponse depuis une entrée terrain aux informations de l'automate est donné par les deux formules suivantes :

$$\text{temps max} = T_{\text{mod}} + T_{\text{ios}} + T_{\text{net}} + 2 \text{ cycles de processeur}$$

$$\text{temps moyen} = T_{\text{mod}} + (T_{\text{ios}} \times 0,5) + T_{\text{net}} + 0,5 \text{ cycle de processeur}$$

Formules des temps de réponse : Entrée terrain à décision à sortie terrain

Pour un automate Quantum, le temps de réponse depuis une entrée terrain à une décision dans une sortie terrain est :

$$\text{temps max} = T_{mod} + T_{ios} + T_{net} + 3 \text{ cycles de processeur} + T_{ios} + T_{net} + T_{mod}$$

$$\text{temps moyen} = T_{mod} + (T_{ios} \times 0,5) + T_{net} + 2,5 \text{ cycles de processeur} + (T_{ios} \times 0,5) + T_{net} + T_{mod}$$

Pour un automate Premium, le temps de réponse depuis une entrée terrain à une décision dans une sortie terrain est :

$$\text{temps max} = T_{mod} + T_{ios} + T_{net} + 3 \text{ cycles de processeur} + T_{ios} + T_{net} + T_{mod}$$

Formules des temps de réponse : Décision à sortie terrain

Pour un automate Quantum, le temps de réponse depuis une décision à une sortie terrain est :

$$\text{temps max} = 1 \text{ cycle de processeur} + T_{ios} + T_{net} + T_{mod}$$

$$\text{temps moyen} = 0,5 \text{ cycle de processeur} + T_{ios} + T_{net} + T_{mod}$$

Pour un automate Premium, le temps de réponse depuis une décision à une sortie terrain est :

$$\text{temps max} = 2 \text{ cycles de processeur} + T_{ios} + T_{net} + T_{mod}$$

$$\text{temps moyen} = 1 \text{ cycle de processeur} + T_{ios} + T_{net} + T_{mod}$$

Charge totale sur les équipements

Récapitulatif

Veillez à ce que le nombre total de messages Ethernet envoyés vers et à partir de l'équipement ne dépasse pas les limites suivantes :

Capacité de traitement des connexions Ethernet	Premium Ethernet TCP/IP			Quantum Ethernet TCP/IP	
	TSXETY110	TSXETY4103	TSXP575xx	140NOE771**	140CPU65150
	TSXETY210	TSXETY5103		140NWM10000 (5)	140CPU65160
	TSXETY110WS	TSXWMY100 (5)			140CPU67160
		TSXP571xx			
		TSXP572xx			
		TSXP573xx			
		TSXP574xx			
Transactions de messages par seconde	60	450	500	350	350
Analyse des transactions d'interrogation d'E/S par seconde	-	2 000	2 000	2 000	2 000
Transactions de souscription Global Data par seconde		800	800	800	800

Solutions pour les performances système

Récapitulatif

Voici plusieurs situations, présentées sous forme de problèmes posés et de réponses apportées, susceptibles de vous aider à évaluer les performances de votre système.

Problème 1

Problème : Un SCADA interrogeant un automate Quantum avec un module NOE envoie 15 requêtes séparées pour lire des blocs de registres Modbus 4x. Toutes ces requêtes sont envoyées simultanément.

Combien de temps faut-il pour terminer toutes les transactions lorsque le temps de cycle de processeur est de 50 ms ?

Solution : Le module NOE peut desservir 8 requêtes Modbus TCP par cycle de l'automate ; 15 requêtes prennent $15/8 = 2$ cycles de l'automate. Toutes les requêtes reçoivent une réponse en 100 ms.

Problème 2

Problème : Un automate Premium lit les données d'un équipement terrain et écrit les données dans un autre équipement terrain. L'équipement terrain d'entrée a un temps de réponse de 80 ms et a déjà traité l'entrée dans sa mémoire. L'équipement terrain de sortie a un temps de réponse de 30 ms, et le temps de cycle de processeur est de 70 ms.

Quel est le temps de réponse (c'est-à-dire entre le moment où l'automate lit l'entrée de champ et celui où la nouvelle sortie de champ s'active) ?

Solution : Si l'automate Premium déclenche une requête de lecture au démarrage du cycle de processeur, il y a un retard d'un cycle de processeur (70 ms) avant l'envoi de la requête. L'équipement terrain répond après 80 ms. La réponse est lue dans l'automate lors du prochain appel de la fonction de lecture, ce qui peut durer un cycle de processeur (70 ms). Le Premium déclenche une fonction d'écriture au cours du même cycle de processeur et envoie la réponse à la fin du cycle (70 ms). L'équipement terrain reçoit la réponse et définit la sortie (30 ms). Le temps total est de :

$$70 \text{ ms} + 80 \text{ ms} + 70 \text{ ms} + 70 \text{ ms} + 30 \text{ ms} = 320 \text{ ms}$$

Problème 3

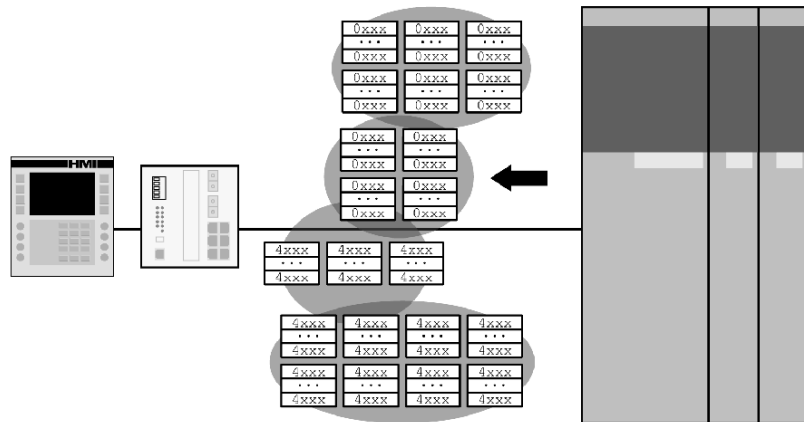
Hypothèse : Un système SCADA interroge un automate Quantum exécutant le logiciel Unity Pro. Le temps de cycle de processeur Quantum est de 140 ms. Le système SCADA interroge les éléments suivants chaque seconde :

- 250 registres pour les tendances
- 750 bits pour les alarmes
- 30 registres pour un écran en cours d'affichage
- 20 bits pour un écran en cours d'affichage
- 1 bit écriture pour démarrer un moteur en réponse à une commande utilisateur sur l'écran en cours

Pour calculer le nombre de requêtes, vous pouvez consulter la configuration et déterminer le nombre de requêtes envoyées ou vous pouvez estimer le nombre de requêtes. Dans ce cas, le nombre de requêtes vous a été fourni. Notez que tous les registres ne se trouvent pas dans l'ordre congestif, c'est pourquoi le nombre de requêtes est supérieur à la quantité idéale.

- 3 requêtes pour les tendances chaque seconde
- 6 requêtes pour les alarmes chaque seconde
- 8 requêtes pour les registres affichés à l'écran chaque seconde
- 4 requêtes pour les bits affichés à l'écran chaque seconde

L'emplacement des variables est indiqué dans le diagramme suivant :



Problème : Déterminez le temps de réponse du système SCADA dans chacun des cas suivants.

Premier cas : SCADA ouvre un socket et n'envoie qu'une requête à la fois.

Solution : Dans ce scénario, le SCADA n'envoie une nouvelle requête que lorsqu'une réponse est reçue pour la requête précédente. Ceci se traduit par la formation d'une file d'attente dans le SCADA. L'automate ne doit répondre qu'à une requête à la fin de chaque cycle de processeur dans lequel une réponse à la requête est garantie à la fin de chaque cycle de processeur.

Dans ce cas, 21 requêtes se trouvent dans la file d'attente. Le SCADA envoie la première requête à l'automate ; ce dernier envoie une réponse en 140 ms, après quoi le SCADA envoie la seconde requête de la file d'attente à l'automate. Par conséquent, l'automate met 2,94 secondes à répondre aux 21 requêtes. Le temps de réponse du SCADA est de 2,94 secondes.

Second cas : SCADA ouvre un socket, mais envoie simultanément plusieurs requêtes à l'automate.

Solution : Dans ce cas, l'automate doit répondre à plusieurs requêtes simultanément, ce qui peut dépasser ses capacités. Ceci se traduit par plusieurs cycles de processeur de l'automate pour répondre à toutes les requêtes. Le SCADA envoie les 21 requêtes à l'automate et forme deux files d'attente dans l'automate, l'une pour 0x et l'autre pour 4x. A partir des informations ci-dessus, vous voyez que l'automate a 11 requêtes dans le registre 4x et 10 requêtes dans la file d'attente 0x. Le NOE peut traiter 8 requêtes 4x et 4 autres requêtes par cycle de processeur. Dans ce scénario, il faut 2 cycles de processeur (280 ms) pour répondre aux requêtes 4x et 3 cycles de processeur (420 ms) pour les requêtes 0x, ce qui est beaucoup plus rapide que dans le premier cas.

Si l'utilisateur envoie une commande d'écriture à l'automate pour démarrer le moteur, il y a plusieurs possibilités :

- **Cas 1a** : Le SCADA peut interrompre l'interrogation et envoyer la requête immédiatement (dès la fin de la requête en cours). Le moteur démarre deux cycles de processeur plus tard, un cycle de processeur pour finir la requête en cours et un autre pour traiter la requête de démarrage du moteur.
- **Cas 1b** : Le SCADA peut placer la requête à la fin de la file d'attente ; il fait jusqu'à 2,94 secondes avant que la requête d'écriture soit envoyée. Le moteur démarre un cycle de processeur après ce délai.
- **Cas 2** : La requête est envoyée et placée à la fin de la file des autres requêtes ox dans le module NOE. Ce traitement s'effectue sur le troisième cycle de processeur ; le retard est de 3 cycles de processeur (420 ms).

Pour plus de détails, *Fonctionnement du serveur Modbus dans les systèmes Quantum*, page 209

Problème 4

Problème : Un automate Quantum lit les données d'un automate Premium. Le cycle de processeur du Quantum est de 50 ms, et celui du Premium, de 70 ms.

Quel est le temps de réponse du système pour lire un bloc de 50 registres Modbus 4x ?

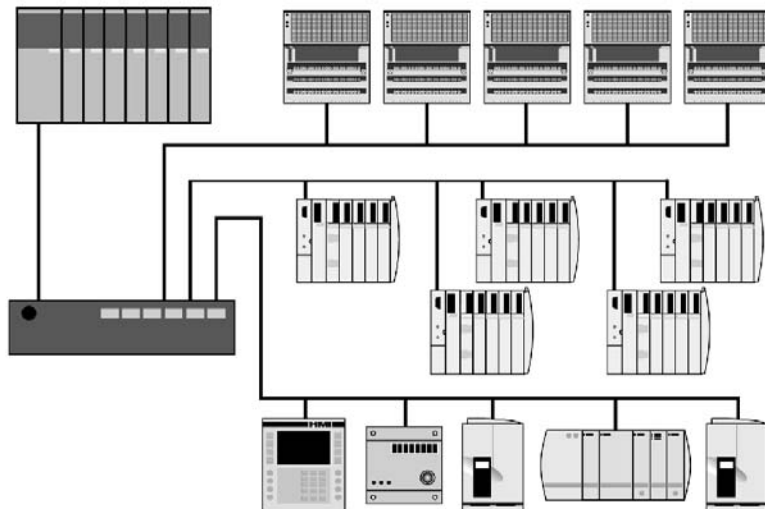
Solution : Pour les communications de Quantum à Premium, il existe deux méthodes : l'utilisation des graphiques de l'annexe ou le calcul à partir du fonctionnement du système. Le bloc de 50 registres Modbus peut être lu dans une seule requête Modbus. Recherchez une seule requête de messagerie Modbus à la fois sur un équipement avec un temps de réponse de 70 ms. 70 ms est utilisé car c'est le temps de cycle de l'automate Premium ; un automate Premium peut répondre aux requêtes dans un cycle de processeur.

L'automate Quantum déclenche une requête de lecture, qui est immédiatement envoyée à l'automate Premium. Le Premium y répond dans un temps de cycle de processeur (70 ms). Le Quantum reçoit cette réponse et l'intègre à l'application de l'automate lors du traitement suivant du bloc de requête, ce qui se traduit par un retard d'un cycle de processeur (50 ms). Le temps total entre le déclenchement du bloc et la disponibilité de la réponse est de 120 ms.

Problème 5

Problème : Quel est le temps de réponse d'un automate Quantum avec un temps de cycle de 50 ms pour lire 10 registres 4x à partir de chacun des 25 dispositifs de mesure de puissance distants ayant chacun un temps de réponse de 100 ms ?

Automate Quantum avec 25 dispositifs de mesure de puissance ayant un seul bloc de 10 registres chacun.



Solution : Le Quantum ne peut envoyer que 16 requêtes de messagerie à la fois à partir d'un seul module NOE. Il existe deux méthodes pour l'évaluation : l'utilisation d'un graphique de l'annexe ou l'évaluation à partir du système.

Si 25 requêtes sont déclenchées, 16 sont envoyées immédiatement. Les dispositifs de mesure répondent après 100 ms et les réponses sont intégrées à l'application de l'automate lors du traitement suivant du bloc de requête. Ceci se traduit par un retard d'un cycle de processeur (50 ms). Après 150 ms, l'automate obtient les réponses aux 16 requêtes à l'intérieur de l'application de l'automate. Les 9 blocs restants sont envoyés. Les dispositifs de mesure répondent (100 ms) et l'automate lit les données lors du cycle suivant (50 ms). Le temps supplémentaire est de 150 ms. Le temps de réponse système total est de 300 ms.

NOTE : Il est possible de calculer un temps légèrement inférieur si le temps de réponse réel des autres équipements et le cycle de processeur sont pris en compte. La réponse doit arriver partiellement dans un cycle de processeur, de sorte que l'on peut calculer uniquement le temps de cycle de processeur restant avant que la réponse ne soit traitée dans l'application. Cette méthode n'est pas recommandée car on doit toujours supposer le cas le plus défavorable. Vous n'avez aucun contrôle sur la synchronisation des deux équipements.

Problème 6

Problème : Un scrutateur d'E/S Quantum 140CPU65150 (avec un port Ethernet intégré) sur un automate dont le temps de cycle de processeur est de 20 ms interroge cinq équipements d'E/S Momentum, Advantys et tiers (15 équipements en tout). Le temps de réponse de l'équipement tiers est de 100 ms.

Quels sont les temps de réponse de chaque type d'équipement pour lire une entrée, la traiter en code automate et écrire une sortie en réponse au même équipement ?

Déterminez comment le temps de réponse change si le temps de cycle de processeur augmente à 100 ms.

Déterminez comment le temps de réponse change si le temps de cycle de processeur est de 10 ms mais que la période de répétition configurée est de 50 ms.

Solution : Pour l'E/S Momentum le temps de réponse de l'équipement terrain est minime. Le Momentum a été utilisé pour les graphiques de performances du scrutateur d'E/S dans l'annexe (*voir page 413*). Le graphique permettant d'évaluer le temps de réponse du système est choisi sur le processeur du scrutateur d'E/S utilisé et le type de système (entrée terrain à sortie terrain). Pour 16 équipements et un temps de cycle de processeur de 20 ms, le temps de réponse du système (entrée terrain à sortie terrain) est de 49 ms.

Pour les équipements Advantys, le temps de réponse doit être calculé en utilisant les formules du système pour prendre en compte les retards de l'équipement terrain.

Problème 7

Problème : Un équipement d'E/S Momentum est interrogé par :

- un scrutateur d'E/S Quantum lisant trois blocs de données séparés
- un automate Premium lisant un bloc de données en utilisant une requête de messagerie Modbus

Si un SCADA souhaite accéder au Momentum, peut-il lire les données ? Comment peut-on modifier le système afin que le SCADA puisse lire les données ?

Solution : L'équipement d'E/S Momentum I/O ne peut ouvrir que quatre sockets TCP simultanément. Le scrutateur d'E/S du Quantum conserve les sockets TCP ouverts (le scrutateur d'E/S conserve toujours les sockets ouverts). L'automate Premium ouvre un seul socket lorsque la requête de lecture Modbus est déclenchée. Un total de quatre sockets sont ouvert sur le Momentum. Le socket utilisé par le Premium peut être fermé après la transaction si le Momentum en demande la fermeture, mais le Momentum n'est pas conçu pour cela. Du fait du nombre maximum de sockets ouverts, la requête d'ouverture de socket du SCADA est rejetée.

Pour permettre au système SCADA d'ouvrir un socket, l'un des autres sockets doit être fermé. Ceci ne peut s'effectuer sur le Premium, mais le scrutateur d'E/S Quantum peut fermer l'un de ses sockets. Il le fait en désactivant la ligne du scrutateur d'E/S, ce qui provoque l'arrêt du transfert de données mais active la communication du Premium. Lorsque les données du scrutateur d'E/S sont requises, la ligne peut être réactivée. Le problème de cette solution est qu'il n'existe aucune coordination entre le SCADA et le Quantum quant au système tentant d'utiliser le socket. Ceci peut se traduire par des erreurs de communication ou des tentatives sur les deux équipements tentent de lire des données en même temps.

Temps de réponse de la passerelle

Récapitulatif

Le temps de réponse d'un système de passerelle peut être calculé de l'une des deux manières suivantes :

- Pour une passerelle avec ou sans conversion de protocole : calcul réel incluant le temps de réponse des équipements du réseau cible et des files d'attente à l'intérieur de la passerelle.
- Pour une passerelle utilisant une mémoire partagée : pour le temps de réponse simple, vous pouvez utiliser uniquement la durée nécessaire à la lecture de la mémoire interne. Pour une réponse complète d'un système concernant les données dans un équipement de destination via la passerelle et vers un équipement sur le réseau source, la lecture des données dans la passerelle (souvent basée sur un temporisateur) doit être incluse.

La méthode la plus simple pour calculer un temps de réponse consiste à prendre en compte un message unique pour lire les données. Les actions suivantes doivent se produire :

- Un équipement sur le réseau source doit envoyer une requête pour lire les données ; le délai dépend de l'équipement qui émet la requête.
- La passerelle reçoit la requête ; le délai s'écoulant entre le moment où l'équipement envoie la requête et celui où la passerelle la reçoit dépend du réseau source. Sur un réseau Ethernet, le délai est normalement 0,05 ms. Pour un réseau Modbus Plus, il peut atteindre la durée d'une rotation de jeton, soit la durée nécessaire au jeton (paquet de messages) pour tourner autour de l'anneau et revenir à l'équipement émetteur. Pour plus d'informations, reportez-vous au guide de l'utilisateur de Modbus Plus.
- La passerelle transmet la requête au réseau cible ; cela s'appelle le délai de passerelle (*voir page 411*). S'il existe une file d'attente, celui-ci peut être considérable. Le délai de passerelle est courant si les deux réseaux connectés par la passerelle possèdent des temps de réponse très différents.
- La requête est reçue par l'équipement de destination ; le délai est basé sur l'aptitude du réseau cible à transmettre le message. Pour Modbus Plus, il correspond à la durée de rotation d'un jeton. Pour les réseaux série, il dépend de la vitesse du réseau.
- La requête est traitée par l'équipement de destination ; cela dépend concrètement de l'équipement.
- Une réponse est renvoyée à la passerelle ; le délai est basé sur l'aptitude de la cible à transmettre le message. Pour Modbus Plus, il correspond à la durée de rotation d'un jeton ; pour les réseaux série, il dépend de la vitesse du réseau.

- La passerelle retransmet la réponse au réseau source ; cela s'appelle le délai de passerelle (*voir page 411*). S'il existe une file d'attente, celui-ci peut être considérable. Le délai de passerelle est courant si les deux réseaux connectés par la passerelle possèdent des temps de réponse très différents.
- La réponse est reçue par l'équipement qui a émis la requête ; le délai s'écoulant entre le moment où l'équipement envoie la requête et celui où la passerelle la reçoit dépend du réseau source. Sur un réseau Ethernet, le délai est normalement 0,05 ms. Pour un réseau Modbus Plus, il peut correspondre à la durée de rotation d'un jeton maximum.

Dans les étapes impliquant un délai, le temps de réponse système est égal au total de tous les délais.

Le délai de transmission de la requête et celui de la réponse sur le réseau peuvent être différents. Par exemple, un réseau série met beaucoup plus de temps à transmettre une réponse comprenant 100 registres de données qu'à transmettre la requête elle-même qui ne contient aucune donnée réelle.

Deux éléments compliquent le calcul du temps de réponse système :

- une file d'attente de messages dans la passerelle, due à des timeouts ou à des requêtes multiples ;
- le timeout d'un message sur le réseau cible : cela s'applique dans un réseau qui doit contenir tous les messages futurs jusqu'à ce que le message courant soit dépassé (par ex. ligne série Modbus).

Pour améliorer le temps de réponse système, réduisez le nombre de requêtes envoyées via la passerelle en limitant le nombre d'équipements connectés à chaque passerelle.

Calcul du temps de transmission de la ligne série

Le temps de réponse de la ligne série est déterminé par le nombre de bits envoyés et par la vitesse de la ligne série. Reportez-vous aux spécifications du protocole Modbus pour connaître le nombre exact de bits par message Modbus. Pour le temps de transmission réel du réseau, utilisez :

$$(\text{nombre de bits dans le message}/8) \times (1/\text{débit en bauds})$$

Pour une requête de lecture Modbus à 9 600 bauds, le temps est d'environ 5 ms. Une réponse prend approximativement 100 ms pour 100 registres de données.

Calcul du nombre d'équipements pris en charge par pont

Le temps de réponse système est déterminé par le nombre de requêtes envoyées via le pont ; plus il y a de requêtes envoyées, plus le temps de réponse global pour tous les équipements sera long. Pour déterminer le nombre d'équipements sur un système, commencez par calculer le nombre total de requêtes Modbus afin de collecter les données. Le meilleur temps de réponse que peut donner le système est le suivant :

nombre de requêtes x (temps de transmission de la requête sur la ligne série + temps de réponse de l'équipement série + temps de transmission de la réponse sur la ligne série + ~50 ms)

Le temps de réponse moyen pour un équipement série est de 200 ms, mais il peut varier de 50 à 500 ms. Le temps de transmission de la requête/réponse dépend de la vitesse du réseau et des paramètres Modbus RTU/ASCII.

- RTU est beaucoup plus rapide car la quantité d'octets transmis est moindre.
- Une requête de lecture Modbus moyenne à 9 600 bauds prend environ 5 ms.
- Le temps de réponse maximum est d'environ 100 ms.

La meilleure réponse système qui soit envisageable serait par conséquent de :

5 ms (requête) + 200 ms (réponse de l'équipement série) + 100 ms (réponse) + 50 ms = ~350 ms/requête

Pour 8 équipements Modbus avec 2 requêtes chacun, le meilleur temps de réponse envisageable pour obtenir les données du système est donc de
 $16 \times 350 \text{ ms} = 5,6 \text{ s}$.

Ce délai d'attente de réponse est trop long pour la plupart des utilisateurs système, ce qui implique donc que le nombre d'équipements par pont soit revu à la baisse.

Toutefois, avec un temps de réponse d'équipement série plus court, le calcul de ce temps de réponse optimal pour un pont nécessiterait la formule suivante :

5 ms (requête) + 50 ms (réponse de l'équipement série) + 20 ms (réponse) + 50 ms = ~125 ms/requête

Pour 8 équipements Modbus avec 2 requêtes chacun, le temps de réponse optimal aurait alors la valeur acceptable suivante : $16 \times 125 \text{ ms} = 2,0 \text{ s}$.

Calcul du timeout Ethernet

Si le timeout d'une requête est inclus, le calcul du plus mauvais temps de réponse possible pour le pont donne la valeur requise pour le champ de timeout Ethernet :

timeout Ethernet = timeout d'une requête de ligne série x nombre de tentatives de la ligne série x nombre de requêtes envoyées au pont

Si ce calcul de timeout n'est pas utilisé et si la valeur du champ est trop lente, l'échec d'un ou plusieurs équipements série peut entraîner l'expiration des requêtes Ethernet envoyées à d'autres équipements série en raison du délai généré par la valeur incorrecte.

Introduction

Ce chapitre décrit les procédures de dépannage générales et explique comment identifier des problèmes. Il propose également des tableaux permettant d'identifier et de résoudre les problèmes.

Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
4.1	A propos du dépannage	376
4.2	Dépannage réseau	380
4.3	Dépannage des services	389
4.4	Dépannage en cas de lenteur de réponse d'un système SCADA/HMI	401
4.5	Dépannage du pont	403
4.6	Dépannage en cas de perte de paquets	404

4.1 A propos du dépannage

Introduction

Ce sous-chapitre décrit le dépannage des réseaux Transparent Ready.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Introduction au dépannage	377
Identification générale des problèmes	378

Introduction au dépannage

Vue d'ensemble

Les tableaux de dépannage de ce chapitre couvrent les problèmes les plus fréquemment rencontrés avec un réseau Transparent Ready. En raison de la complexité de la conception du réseau, il est impossible de tenir compte de tous les types de problèmes qui peuvent se produire.

Voici quelques questions à se poser qui couvrent les problèmes les plus fréquemment rencontrés :

- L'appareil est-il sous tension ?
- Les câbles sont-ils correctement connectés ?
- L'adresse IP est-elle correcte ?

Afin d'éviter toute redondance, ce manuel décrit les problèmes ci-dessus dans les tableaux réseau (*voir page 380*) et non pas pour chaque service (Modbus, scrutateur d'E/S, etc.) auxquels ils pourraient s'appliquer.

Ce manuel n'est pas capable d'anticiper les défaillances et les verrouillages pour tous les appareils sur le marché, donc il existe peu d'exemples dans lesquels Schneider recommande un redémarrage d'un périphérique réseau. Pour résoudre rapidement un problème, vous pouvez redémarrer un appareil défectueux, mais vous devez d'abord évaluer si le cycle interfère avec les opérations sur site. Une mise sous tension peut temporairement rétablir les communications vers l'appareil, mais il n'identifiera pas, ni ne corrigera le problème.

Identification générale des problèmes

Avant de commencer

Réunissez autant d'informations que vous le pouvez au sujet des caractéristiques, des symptômes et du déroulement d'un problème avant de procéder au dépannage. Les problèmes qui semblaient au départ liés au réseau peuvent s'avérer être dus à l'application, à la gestion des terminaux ou à l'installation.

Posez-vous ces questions essentielles avant de procéder au dépannage :

- Les symptômes sont-ils réguliers ou intermittents ?
- Quelle est l'étendue du problème ? Cela affecte-t-il un appareil, plusieurs appareils ou tous les appareils ? Les appareils affectés sont-ils situés dans la même zone du site ?
- Les symptômes sont-ils liés à une ou à l'ensemble des applications/services ? Quelles sont les applications/services qui fonctionnent simultanément ?
- Quand, ce problème, s'est-il manifesté pour la première fois ?
- Ces incidences coïncident-elles avec des activités réseau inhabituelles ou irrégulières qui à priori ne sembleraient pas provoquer de problèmes ?
- Avez-vous récemment changé le matériel réseau ou des composants logiciels ? Avez vous récemment ajouté des terminaux au réseau ?
- Des travaux de maintenance (déplacement, nettoyage, gestion de câbles, électricité, etc.) pourraient-ils affecter des opérations réseau ?

Souvenez-vous des réponses à ces questions lorsque vous utiliserez les tableaux de dépannage.

Identification des problèmes

Thème	Description	Exemples
Problèmes réseau	Problèmes au niveau : - des connexions physiques des équipements ; - des adresses logiques ; - de l'émission des paquets Ethernet vers et depuis les équipements.	- Aucune liaison Ethernet avec l'équipement. - Impossible de localiser l'équipement avec la commande ping. - Impossible d'effectuer un contact avec l'équipement.
Services	Problèmes avec un ou plusieurs services Transparent Ready. Il est possible de localiser l'équipement avec une commande ping et d'obtenir une réponse, mais d'autres erreurs de communication peuvent survenir.	- Echec des communications Modbus, mais les pages Web sont OK. - Erreur du scrutateur d'E/S, mais les programmations sont OK.
Système SCADA	Informations spécifiques sur l'amélioration des performances des systèmes SCADA.	Des lenteurs du système SCADA sont observées lors du diagnostic de l'état de l'équipement en unité ou de l'exécution des commandes.
Ponts Ethernet vers série	Informations spécifiques concernant le dépannage des communications via des ponts Ethernet vers série.	Le routage est lent ou les communications vers les équipements sont intermittentes suite à une défaillance sur un seul équipement.
Outil de capture du paquet Ethernet	Informations spécifiques sur la capture et l'analyse des paquets Ethernet pour un dépannage détaillé.	

4.2 Dépannage réseau

Introduction

Ce sous-chapitre décrit le mode de dépannage réseau, notamment pour la couche 1 (la couche physique) et la couche 2 (problèmes IP) de la pile TCP.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Introduction au dépannage réseau	381
Dépannage des connexions	383
Dépannage en cas de connexions intermittentes	385
Dépannage en cas de connexions lentes	386
Dépannage de l'accès distant	387

Introduction au dépannage réseau

Types de problèmes

Les problèmes réseau les plus fréquents sur les systèmes Transparent Ready sont liés :

- à l'infrastructure physiques ;
- aux ressources logiques ;
- à l'encombrement du trafic.

Sur les réseaux modernes, les commutateurs intelligents et les cartes d'interface réseau rapides entraînent des configurations réseau et des conditions de fonctionnement complexes. Par conséquent, les problèmes peuvent être difficiles à isoler dans un tel environnement.

Les problèmes intermittents sont les plus difficiles à résoudre. En effet, si le problème est constant, il est immédiatement possible d'évaluer le résultat des corrections apportées.

Pour pouvoir résoudre facilement un problème, il convient de disposer d'une parfaite compréhension de la conception logique et physique du réseau. (La qualité de la documentation disponible peut aussi s'avérer un facteur déterminant.)

Connexions physiques

Les problèmes de connexion physique sont généralement plus faciles à résoudre par rapport aux autres types de problèmes. La vérification du branchement du câble réseau n'est que la première étape des investigations à réaliser pour tester la connectivité physique du réseau. Les testeurs de câbles et les indicateurs de performance du matériel (la plupart du temps des voyants situés sur les périphériques du réseau) aident à identifier et à isoler les problèmes de connexion physique.

Des problèmes de connexion physique complexes supplémentaires peuvent être liés aux éléments suivants :

Câbles	Avez-vous installé le bon type et la bonne qualité de câble ?
	Avez-vous pris en compte les problèmes d'interférences des câbles (bruit et mise à la terre) ?
	Avez-vous correctement utilisé les câbles simples ou inverseurs ?
	Est-ce que les paramètres et les configurations conviennent aux communications duplex (vitesse de transmission) ?
Interférences	Connexions sans fil
	Interférences normales

Connexions logiques

Pour résoudre les problèmes liés aux connexions logiques qui présentent davantage de complexité, il faut d'abord disposer d'une parfaite compréhension des connexions physiques et des composants réseau.

Généralement, le dépannage des connexions logiques nécessite une certaine expertise des logiciels et applications spécifiques, même si vous pouvez régler certains problèmes avec les commandes DOS standard qui fonctionnent avec la plupart des systèmes d'exploitation courants.

Une mauvaise administration du réseau entraîne souvent des problèmes de connexion logique. Si vous ne redémarrez pas le système avant de tester les dernières modifications apportées à l'administration du réseau, les utilisateurs finals peuvent rencontrer ultérieurement des problèmes, surtout lors de l'accès à des applications ou des programmes spécifiques après un redémarrage du système. Les modifications susceptibles de provoquer des problèmes de connexion logique sont les suivantes :

- changements importants au niveau des applications ou du système d'exploitation du serveur (serveurs DHCP, serveurs DNS, serveurs de messagerie, etc.) ;
- changements au niveau des ouvertures de session, des règles, des scripts et de l'authentification ;
- changements liés à la sécurité (règles des pare-feu, ports/services et paramètres de cryptage) ;
- changements des fonctionnalités du matériel réseau (filtrage de multidiffusion, routage de la passerelle par défaut, configuration).

Encombrement du trafic réseau

Un volume important de trafic réseau peut provoquer des problèmes difficiles à isoler et à résoudre. Les utilitaires logiciels, tels que les analyseurs de réseau et de protocole, vous aident à résoudre les problèmes d'encombrement. (Dans la plupart des cas, vous avez besoin d'une formation pour utiliser ces outils spécifiques.) Malheureusement, ces outils ne signalent que des problèmes d'ordre général, tels que des erreurs de diffusion.

Dans le cas de réseaux commutés étendus, il est difficile d'isoler et d'évaluer l'encombrement sans l'aide de sondes matérielles et d'outils logiciels spécifiques au fournisseur. Une analyse rapide de l'étendue et de la gravité d'un problème peut vous aider à trouver une solution plus rapidement et plus efficacement.

Si ce problème concerne seulement un nombre restreint d'utilisateurs et si ses conséquences ne sont pas critiques, vous pouvez opter pour une méthode de dépannage qui ne nécessite pas une coupure réseau complète. Par contre, en cas de problèmes de communication étendus, il peut s'avérer nécessaire de segmenter physiquement le réseau afin de vous aider à isoler rapidement la panne.

Dépannage des connexions

Problème	Thème	Cause et actions
Contrôle physique	câbles (voir remarque)	Le terminal doit être raccordé à la prise murale, au panneau de raccordement, au concentrateur ou au commutateur à l'aide de câbles adéquats. Vérifiez aussi l'absence de défauts ou d'entailles sur les câbles, et toute cause d'interférences (comme le bruit électrique). Remplacez les câbles de raccordement suspects.
		Vérifiez, le cas échéant, les voyants de connexion des appareils. En général, les voyants sont verts lorsque tout est opérationnel, orange en cas d'erreur et éteints lorsque aucune connexion physique n'est détectée par le matériel. (Voir le Guide d'utilisateur du matériel, pour plus de détails.)
		Vérifiez, le cas échéant, les voyants du mode duplex sur l'appareil, pour les paramètres de vitesse (10 Mbit, 100 Mbit, auto, etc.). Voir le chapitre chapitre sur les configurations physiques (<i>voir page 29</i>).
		Assurez-vous que des câbles inverseurs ont été utilisés pour relier les périphériques du réseau (concentrateur à concentrateur, commutateur à commutateur), lorsque cela s'avère nécessaire. Vérifiez la documentation de l'appareil pour connaître les configurations requises pour les câbles simples ou inverseurs.
		Les longueurs des câbles ne doivent pas excéder les spécifications Ethernet.
		Testez l'intégrité du câblage fédérateur avec un équipement de test et recommencez les terminaisons au niveau du panneau de raccordement en cas de doute une fois les vérifications logiques effectuées.
	Carte d'interface réseau	Assurez-vous que la carte réseau PCMCIA ou classique est correctement installée. Echangez votre carte réseau pour tester ses performances.
	matériel réseau	Vérifiez : ● l'alimentation des concentrateurs, commutateurs, routeurs et autres équipements réseau ; ● l'activité de la liaison sur les ports grâce aux voyants (généralement verts, clignotant ou non) ; ● la connectivité des câbles de liaison montante pour des appareils superposés. En cas de doute sur un port de concentrateur ou de commutateur, remplacez-le par un port identique une fois les vérifications logiques effectuées.

Problème	Thème	Cause et actions
Vérifications logiques	système d'exploitation	A l'invite DOS, saisissez ping pour vérifier la connectivité réseau, notamment au niveau des réponses et des timeouts.
		A l'invite DOS, saisissez ipconfig pour voir si l'appareil reçoit une adresse IP et un IP associé.
		Vérifiez la configuration réseau du système d'exploitation. Par exemple : ● La carte matérielle est-elle opérationnelle ? ● Les protocoles TCP/IP sont-ils correctement raccordés à la carte réseau ?
		Vérifiez la configuration de l'adresse IP : ● Pour l'adresse statique, l'adresse IP et le masque de sous-réseau sont-ils saisis correctement ? ● L'adresse par défaut de la passerelle (le cas échéant) est-elle correcte pour l'équipement source et l'équipement terminal ?
		Si vous rencontrez un problème pendant la connexion aux réseaux distants, saisissez traceroute à l'invite DOS pour vérifier les bonds de routage aux points défectueux. En cas de temporisation sur un bond de routage, traitez et validez le problème avec la personne responsable de ce routeur.
		Pour les connexions sans fil, vérifiez la validité des paramètres de configuration suivants : ● SSID ● Voie ● Type (a, b, g) ● Clé de chiffrement
	Carte d'interface réseau	Vérifiez les paramètres (vitesse) du mode duplex (autonégociation, 10 Mbit, 100 Mbit, etc.). Si possible, faites coïncider les paramètres du terminal avec ceux de son port réseau.
		Assurez-vous que les pilotes de l'interface réseau et les paramètres de l'adaptateur ont été correctement configurés sur le terminal. Mettez à jour ou rechargez les pilotes du logiciel de la carte réseau du fabricant.
	matériel réseau	Activez les ports auxquels vos concentrateurs et vos commutateurs sont connectés.
		Vérifiez la configuration du commutateur pour les réseaux locaux virtuels (facultatif).
	applications	Vérifiez les paramètres de pare-feu ou de proxy qui peuvent bloquer les ports ou les protocoles entre les équipements source et cible.
		Pour les applications serveurs/clients, vérifiez que le serveur (autre équipement cible) fonctionne correctement en réseau. Vérifiez si d'autres clients présentent le même problème, afin de déterminer si celui-ci concerne un seul client ou l'ensemble du réseau.
Remarque : Des outils spécifiques sont disponibles pour tester automatiquement un câble. Ces outils vérifient la sélection du type de câble, le raccordement des broches, etc. Pour plus de détails sur les marques et modèles, voir le chapitre chapitre sur les configurations physiques (voir page 29).		

Dépannage en cas de connexions intermittentes

Catégorie du problème	Thème	Cause et actions
Vérification physique	Câbles (voir remarque)	• Vérifiez les connexions lâches, en particulier si un dongle avec PCMCIA est installé entre les connexions de câbles NIC et RJ45. • Vérifiez que les câbles ne sont pas défectueux. • Vérifiez la mise à la terre et les connexions du panneau de raccordement. • Vérifiez l'intégrité des câbles à l'aide d'un équipement de test de câbles, après avoir effectué les vérifications logiques nécessaires.
	NIC	En cas de connexions sans fil, vérifiez l'intensité du signal et rafraîchissez le signal ou éliminez les interférences entre un équipement terminal et un point d'accès sans fil.
Vérification logique	Applications/système d'exploitation	A l'invite DOS, utilisez la commande <i>ping</i> pour vérifier le niveau de base de la connectivité du réseau, notamment au niveau des réponses et des timeouts.
		Si vous rencontrez un problème pendant la connexion aux réseaux distants, saisissez <i>tracert</i> à l'invite DOS pour vérifier les bonds de routage aux points défectueux.
		Lancez une scrutation du système d'exploitation, pour rechercher des virus ou des problèmes de ressources de mémoire éventuels.
	Matériel réseau	Vérifiez les concentrateurs, les commutateurs ou les routeurs (le cas échéant) pour détecter une congestion du trafic réseau ou d'éventuelles perturbations de la diffusion réseau. Le cas échéant, contrôlez les journaux d'erreurs sur le matériel réseau.
	NIC	Pour les connexions sans fil, utilisez la configuration réseau pour vérifier l'intensité du signal sur l'équipement terminal.
Remarque : Des outils spécifiques sont disponibles pour tester automatiquement un câble. Ces outils vérifient la sélection du type de câble approprié, le raccordement correct des broches, etc. Pour plus d'informations sur les marques et les modèles, voir le chapitre Configuration physique (<i>voir page 29</i>).		

Dépannage en cas de connexions lentes

Catégorie du problème	Thème	Cause et actions
Vérification physique	Câbles (voir remarque)	Vérifiez l'intégrité des câbles et leur conformité aux exigences de câblage appropriées (catégorie 3, 5, etc.).
		Si l'intégralité du réseau dans un environnement de commutateur important continue à être sérieusement affecté, même après vérification de toutes les connexions logiques, déconnectez tous les segments de réseau au niveau du réseau fédérateur central et contrôlez le trafic jusqu'à ce qu'il redevienne normal. Ainsi, vous pourrez repérer précisément le site, le bâtiment, l'armoire, le commutateur, le port, la cabine de distribution, l'équipement terminal ou le câble qui pose problème.
	Matériel réseau	Vérifiez les voyants de liaison du concentrateur, du commutateur ou du routeur afin de repérer les problèmes de trafic réseau. Dans des circonstances normales, ces voyants d'indication sont allumés en permanence. Reportez-vous à la documentation du vendeur de l'équipement pour l'interprétation des différents modes de clignotement.
		Vérifiez qu'un segment de réseau comporte le nombre maximum de répéteurs (concentrateurs).
		Vérifiez la présence de boucles dans le réseau Ethernet, pouvant être due à : • un anneau ConneXium sans gestionnaire de redondance configuré ; • des arbres recouvrants installés de manière incorrecte ; • une boucle créée par un câblage incorrect entre les commutateurs.
Vérification logique	Système d'exploitation	Lancez une scrutation du système d'exploitation, pour rechercher des virus ou des problèmes de ressources de mémoire.
	Applications	Vérifiez que les applications ne contiennent pas d'instances multiples de ressources système surchargées.
		Etablissee si le problème est général au système en examinant d'autres équipements réseau.
	Matériel réseau	Vérifiez le concentrateur, le commutateur ou le routeur (le cas échéant) à la recherche de : • congestion du trafic réseau ; • perturbations de diffusion éventuelles sur le réseau ; • l'utilisation d'une large bande passante (téléchargements importants, lecture en transit audio/vidéo, etc.). Un analyseur de trafic réseau (sniffer) peut vous aider.
Remarque : Des outils spécifiques sont disponibles pour tester automatiquement un câble. Ces outils vérifient la sélection du type de câble approprié, le raccordement correct des broches, etc. Pour plus d'informations sur les marques et les modèles, voir le chapitre Configuration physique (voir page 29).		

Dépannage de l'accès distant

Catégorie du problème	Thème	Cause et actions
Vérification physique	Câbles	Vérifiez que le terminal est correctement raccordé à la prise murale, au panneau de raccordement, au concentrateur ou au commutateur à l'aide de câbles adéquats. Vérifiez aussi l'absence de défauts ou d'entailles sur les câbles, et toute source d'interférences (comme le bruit électrique). Remplacez les câbles de raccordement défectueux par de nouveaux câbles (RJ-11 pour un accès commuté). Pour les connexions d'accès commuté, vérifiez la tonalité au niveau de la prise RJ-11 à l'aide d'un téléphone analogique standard.
	NIC	Assurez-vous que la carte réseau PCMCIA ou standard est correctement installée. Testez les performances de la carte en remplaçant une carte NIC par une autre.
	Matériel réseau	Contrôlez le concentrateur, le commutateur, le routeur, le point d'accès sans fil, le serveur RAS et les autres matériels du réseau pour vérifier que les voyants de liaison des ports et d'alimentation fonctionnent correctement (ils doivent généralement être allumés en permanence ou clignoter en vert). Vérifiez la connectivité des câbles de liaison montante en cas d'équipements superposés. En cas de doute sur un port de concentrateur ou de commutateur, remplacez-le par un port identique une fois les vérifications logiques effectuées. (Consultez la documentation du vendeur pour des informations spécifiques aux équipements.)
Vérification logique	Système d'exploitation	Si vous travaillez à distance (dans un nouvel hôtel, un centre de conférence, sur le site d'un client, etc.), vérifiez auprès de votre administrateur réseau que votre méthode d'accès est prise en charge et autorisée sur le réseau du site distant.
		Si vous utilisez une connexion d'accès commuté ou VPN sur une connexion Internet existante, vérifiez les performances de la connexion en utilisant le navigateur Internet avant d'essayer de dépanner le client ou le serveur.
		Si vous utilisez une connexion d'accès commuté, vérifiez la bonne installation et configuration du réseau d'accès commuté.
		A l'invite DOS, utilisez la commande ping pour vérifier le niveau de base de la connectivité réseau, notamment au niveau des réponses et des timeouts. Pour des raisons de sécurité, les requêtes ping ICMP sont parfois bloquées. Contactez votre administrateur réseau à ce sujet.
		A l'invite DOS, utilisez la commande ipconfig pour vérifier si un équipement reçoit une adresse IP et les paramètres IP associés.
		Vérifiez la configuration réseau du système d'exploitation. Par exemple : • La carte matérielle est-elle opérationnelle ? • Les protocoles TCP/IP sont-ils correctement raccordés à la carte réseau ?

Catégorie du problème	Thème	Cause et actions
		Vérifiez la configuration de l'adresse IP : • Dans le cas d'adressage statique, l'adresse IP et le masque de sous-réseau ont-ils été saisis correctement ? • Le cas échéant, l'adresse par défaut de la passerelle est-elle correcte pour l'équipement source et l'équipement terminal ?
		Si vous rencontrez un problème pendant la connexion aux réseaux distants, saisissez traceroute à l'invite DOS pour vérifier les bonds de routage aux points défectueux. Si vous détectez un timeout sur un bond de routage, traitez et validez le problème avec la personne responsable de ce routeur.
	Application	Pour les logiciels client VPN spécifiques, vérifiez que vous disposez d'un accès Internet de base avant d'établir le tunnel VPN. Configurez le VPN avec les options d'authentification appropriées. (Contactez l'administrateur du réseau informatique local.)
		Vérifiez que le logiciel de coupe-feu (facultatif) installé sur les équipements terminaux ne filtre pas la connectivité de certaines applications ou certains protocoles spécifiques.
	Matériel réseau	Vérifiez le serveur d'accès à distance ou la configuration VPN (et les journaux VPN) à la recherche : • d'informations sur des événements ; • de tentatives de connexion.
		Si le réseau utilise un serveur d'authentification indépendant, vérifiez que les comptes de l'utilisateur final ont été correctement créés et examinez les journaux système pour repérer les tentatives d'authentification. L'administrateur système local peut vous aider sur ce point.

4.3 Dépannage des services

Introduction

Ce sous-chapitre décrit les problèmes récurrents et les solutions pour corriger une erreur de communication sur les services Transparent Ready. Ce type de dépannage est plus simple pour certains équipements que pour d'autres, car les informations de diagnostic sont fournies par différents équipements. La complexité du dépannage varie également suivant les produits Schneider et les équipements tiers. Le voyant d'un équipement s'allume et les informations fournies par son logiciel de diagnostic ou de programmation peuvent faciliter le dépannage.

Dans certains cas, vous pouvez utiliser un outil de capture de paquet réseau (*voir page 406*). Cet outil permet de diagnostiquer avec précision le problème sur un service et indiquer l'action corrective correspondante à effectuer. L'installation d'un tel outil peut prendre un certain temps, c'est pourquoi vous pouvez tenter une solution intuitive (permuter un équipement suspect ou modifier la configuration d'un service) avant d'essayer d'effectuer une analyse à l'aide de l'outil de capture de paquet.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Dépannage des services	390
Dépannage de la messagerie Modbus et du scrutateur d'E/S	391
Dépannage SNMP	394
Dépannage Telnet et FTP	395
Dépannage pour remplacement d'équipements défectueux/BootP	396
Dépannage SMTP	398
Tableau de dépannage de synchronisation horaire (NTP)	399
Tableau de dépannage Web	400

Dépannage des services

Catégorie du problème	Thème	Cause et actions
Echec de service	Echec de tous les services	Vous pouvez saisir une commande ping pour un équipement réseau, mais aucun autre service de l'équipement ne fonctionne (<i>voir page 380</i>).
	Messagerie Modbus	La messagerie Modbus ne fonctionne pas. Par exemple : • communications entre l'automate et les équipements distants ; • communications entre la plupart des systèmes SCADA et un automate ou un équipement.
	Scrutateur d'E/S	Le service de scrutation des E/S a échoué, comme indiqué par les bits d'erreur qui se trouvent dans le service de scrutation des E/S.
	Gestion du réseau (SNMP)	Un système de gestion réseau ne peut pas lire ou écrire des valeurs vers l'équipement terminal. Par exemple, un système de gestion réseau peut détecter un équipement, mais ne peut pas lire les informations sur cet équipement.
	Données globales	Le service de données globales a échoué, comme indiqué par les bits de fonctionnement désactivés dans le service de données globales.
	Telnet/FTP	Telnet ne peut pas se connecter à l'équipement, par exemple vous ne pouvez pas configurer un pont avec Telnet. FTP ne peut pas se connecter ou transférer des fichiers vers l'équipement, par exemple vous ne pouvez pas télécharger des pages Web avec un client FTP.
	Remplacement d'équipements défectueux/BootP	Un équipement ne peut pas obtenir une adresse ou des paramètres IP appropriés via BootP ou FDR, ce qui est signalé par l'envoi en permanence de requêtes BootP depuis l'équipement. (Cette erreur est également signalée par les voyants.) L'équipement accède sinon à l'adresse IP par défaut.
	Web	Vous ne pouvez pas accéder à des pages Web ou certaines fonctions de pages Web ne fonctionnent pas correctement. Par exemple, vous pouvez afficher des pages Web, mais les données interactives d'un équipement sont remplacées par un message d'erreur ou un espace vide.
	NTP (horodatage)	Un équipement ne peut pas obtenir l'heure du serveur NTP (ou l'heure n'est pas précise).
	SMTP (messagerie électronique)	Un appareil ne peut pas envoyer un message électronique.

Dépannage de la messagerie Modbus et du scrutateur d'E/S

Erreurs générales

Thème	Problème	Résolution
Réponse du service trop lente (aucune erreur générée)	Les causes possibles sont : • un client ou un serveur surchargé (<i>voir page 365</i>) qui ralentit la réponse ; • un problème de socket TCP ou une perte de paquet (<i>voir page 405</i>).	
Erreur de timeout (données non transférées)	La réponse d'erreur du client identifie les erreurs de timeout, généralement dues à : • une réponse lente provenant du serveur ; (<i>voir page 354</i>) • la perte d'un paquet sur le réseau ; (<i>voir page 405</i>) • une erreur de socket. (<i>voir page 354</i>)	
Erreur de socket TCP (données non transférées)	Il s'agit d'une erreur qui se produit sur le socket TCP transportant le message Modbus. Dans ce cas, le socket TCP est abandonné ou fermé avant le transfert de données. Certains équipements renvoient un code d'erreur, mais la plupart signalent un message de timeout ou d'erreur générale. Sans rapport d'erreur, cet événement ne peut être détecté qu'avec un outil de capture de paquet.	Pour résoudre le problème, corrigez l'erreur de socket TCP dont la cause peut-être : • un paquet perdu sur le réseau ; (<i>voir page 405</i>) • un problème de séquence ou de numéro d'acquittement survenu suite à une mauvaise implémentation TCP de l'un des terminaux (<i>voir Dépannage en cas de perte de paquets, page 405</i>).

Erreurs client

Thème	Problème
Adresse MAC incorrecte	Une entrée de la combinaison adresse IP/MAC du serveur doit figurer dans le cache ARP de l'équipement qui envoie la requête client. L'équipement client génère normalement cette entrée, mais elle peut être incorrecte, surtout lorsque : ● un équipement défectueux est remplacé par un équipement avec une adresse MAC différente pour la même adresse IP ; ● deux équipements échangent leurs adresses IP et créent des combinaisons IP/MAC différentes pour chaque équipement ; ● un équipement client enregistre sa table ARP dans la mémoire, sans la rafraîchir après une nouvelle mise sous tension.
Surcharge du client	Un système client surchargé ne peut plus envoyer de requêtes. Ceci concerne particulièrement les systèmes dans lesquels l'utilisateur commande l'heure de la requête de déclenchement (comme dans un automate). Ce problème n'apparaît pas lorsque le système (SCADA ou HMI) programme les requêtes. Les équipements propices à la surcharge sont : ● le système Modbus de l'équipement ; ● un équipement ayant une ouverture de sockets TCP limitée (l'ouverture d'un nouveau socket peut être requise pour la transmission d'une nouvelle requête Modbus). Cette erreur est généralement indiquée par un message d'erreur ou un long délai avant l'envoi de la requête.

Erreur serveur

Thème	Problème	Résolution
Code fonction	Les serveurs de réseau ne prennent pas tous en charge tous les codes fonction. Un serveur qui reçoit un code fonction non pris en charge répondra généralement au client par un message d'erreur. Indication de l'erreur : ● le client rapporte l'erreur ; ● l'utilisateur constate l'erreur en contrôlant le paquet réseau pour détecter une absence de réponse ou une réponse d'exception Modbus. Exemples de nouveaux codes fonction Modbus pouvant générer cette erreur : ● registres lecture/écriture FC23 (les scrutateurs d'E/S Quantum et Premium utilisent le registre FC23 lorsque des données de lecture et d'écriture sont fournies sur la même ligne) ; ● statistiques ou identification Ethernet.	Choisissez un code fonction pris en charge pour corriger l'erreur.
Requête non acceptée	Une connexion par socket au serveur ne peut pas être établie pour les raisons suivantes : ● accès contrôlé ; ● présence d'un coupe-feu ; ● nombre de sockets serveur disponibles dépassé.	

Thème	Problème	Résolution
Zone de registre non prise en charge	Si une requête est envoyée vers une zone de registre inexistante ou vers une plage de registres contenant des registres inexistants, le serveur répond par un code d'erreur (comme prévu par la spécification Modbus) ou rejette la requête. Cette erreur est détectée via : ● le rapport de réponse d'erreur de Modbus ; ● un examen de la documentation des registres pris en charge. Cette erreur survient le plus fréquemment lorsque le personnel SCADA ou d'administration tente de lire des blocs ou des registres multiples dans une seule requête à partir d'un serveur qui implémente des registres spécifiques entrecoupés de registres non pris en charge.	
Requêtes pipeline	Les serveurs doivent prendre en charge les requêtes pipeline, sans pour autant avoir à implémenter des requêtes pipeline à chaque occasion. Pour plus d'informations, voir les sections Passerelle (<i>voir page 335</i>) et Messages Modbus (<i>voir page 197</i>). Les requêtes pipeline se produisent lorsqu'une nouvelle requête est envoyée sur un même socket, avant que le serveur ait répondu à la requête précédente. En cas d'incapacité à traiter une requête pipeline, le serveur : ● répondra par un code d'erreur : requête non prise en charge ou serveur occupé (notamment si le serveur est un pont série-Ethernet) ; ● rejettera la requête : sans réponse ; ● se bloquera. Ce problème ne peut être identifié que de deux façons : ● avec une connaissance du fonctionnement de l'équipement ; ● en contrôlant les paquets à l'aide d'un outil de capture de paquet Ethernet. Un problème similaire se produit lorsqu'un équipement envoie plusieurs requêtes Modbus dans un seul paquet Ethernet, opération non permise par la spécification Modbus. Toutefois, dans ce cas, le problème se manifestera davantage par un rejet de la requête ou un blocage de l'équipement.	
Réponse incorrecte	Si une requête Modbus renvoie une réponse incorrecte (soit des données erronées, soit des données de type ou de taille non valide), le client/serveur ne pourra pas utiliser correctement les ID de transaction Modbus. Les ID de transaction dans la spécification TCP (sauf série) Modbus prennent en charge les requêtes pipeline, même si tous les équipements ne les implémentent pas. Les données renvoyées sont alors incorrectes et l'équipement n'est plus conforme à la spécification TCP/IP Modbus. Pour détecter ce problème, contrôlez la requête et la réponse à l'aide d'un outil de capture de paquet Ethernet.	

Dépannage SNMP

Localisation de l'équipement

Thème	Problème
Impossible de localiser un équipement	Un équipement de réseau connu ne peut pas être localisé par un système de gestion SNMP, soit parce que l'équipement ne prend pas en charge SNMP, soit parce qu'un coupe-feu bloque le trafic SNMP. Vérifiez l'équipement du réseau à l'aide d'une requête ping émise par une invite DOS. Si la requête ping est réussie, l'erreur se situe probablement au niveau du logiciel de gestion du réseau. Un échec de la requête ping signifie que c'est l'équipement qui est défaillant. Voir Dépannage réseau (<i>voir page 380</i>).

Accès aux données

Thème	Problème
Un équipement peut être localisé, mais il est impossible d'y accéder pour lire les données.	● <i>Chaînes de communauté incorrectes</i> : la chaîne de lecture doit être correcte pour lire les données, et la chaîne d'écriture correcte pour écrire des données. ● <i>Versions différentes de SNMP (V1, V2, V3)</i> : pour plus d'informations sur les versions, voir sous-chapitre Services SNMP (<i>voir page 269</i>).

Dépannage Telnet et FTP

Les tableaux ci-dessous décrivent les solutions de dépannage pour les problèmes Telnet (voir page 272) et FTP (voir page 280) rencontrés.

Accès à l'équipement

Thème	Problème	Résolution
Impossible d'accéder à l'équipement	Les coupe-feu limitent souvent les accès.	Un message d'erreur côté client permet parfois de détecter ce problème, mais dans une situation idéale : • l'utilisateur connaît l'existence du coupe-feu ; • l'utilisateur examine les paquets à l'aide d'un outil de capture de paquets Ethernet pour vérifier la transmission correcte de la requête d'ouverture de socket et constate qu'un socket n'a pas été établi en raison de l'échec de réception de la réponse.

Connexion incorrecte ou accès limité

Thème	Problème
Impossible de se connecter à l'équipement ou d'effectuer l'action requise.	Un nom d'utilisateur ou un mot de passe incorrect est souvent à l'origine de ce problème. L'interface utilisateur peut détecter ce problème et affiche un message d'erreur. Sans interface utilisateur, il est difficile de faire la distinction entre ce problème et l'erreur précédente (ci-dessus).
Impossible d'effectuer la fonction requise	Ce problème apparaît souvent lorsque le nom d'utilisateur défini n'autorise pas l'accès à l'action souhaitée (par exemple, tentative d'écriture d'un fichier avec une connexion en lecture seule). L'interface utilisateur peut détecter ce problème et affiche un message d'erreur. Sans interface utilisateur, il est difficile de faire la distinction entre ce problème et l'erreur précédente (ci-dessus).

Dépannage pour remplacement d'équipements défectueux/BootP

Les tableaux ci-dessous décrivent les solutions de dépannage pour le remplacement d'équipements défectueux (*voir page 225*) et BootP (*voir page 146*).

Affectation des adresses

Thème	Problème	Résolution
Aucune réponse du serveur à une requête d'adresse IP	- Le serveur ne recense pas l'équipement par son nom de rôle ou son adresse MAC. Cela se produit généralement lorsque vous ajoutez un équipement de remplacement (avec une nouvelle adresse MAC), sans mettre à jour la table du serveur. - Un coupe-feu ou un routeur empêche le client d'accéder au serveur. Configurez le serveur comme agent de relais DHCP, afin de corriger ce problème. Lorsque le client n'obtient pas d'adresse IP, soit il renvoie un code d'erreur, soit il accède à l'adresse IP invalide (ou les deux).	Si vous ne maîtrisez pas très bien le réseau, utilisez un outil de capture de paquet Ethernet pour détecter le problème.
Réponse lente du serveur provoquant un timeout sur le client	Le serveur peut répondre lentement dans les cas suivants : - surcharge, due notamment à la mise sous tension simultanée de plusieurs équipements ; - mise sous tension simultanée du client et du serveur (en général, les équipements côté client démarrent plus rapidement et parviennent à envoyer une requête avant que le serveur ne soit opérationnel). Lorsque le serveur est long à répondre, le client ne parvient pas à obtenir une adresse IP. Dans ce cas, il envoie un code d'erreur ou accède à l'adresse IP par défaut (ou les deux).	Vous ne pouvez faire la distinction entre ce problème et les erreurs ci-dessus qu'avec un outil de capture de paquet. Utilisez alors un outil de capture de paquet Ethernet pour détecter ce problème.
Le serveur envoie une réponse négative, empêchant l'équipement d'obtenir une adresse IP	Plusieurs serveurs DHCP/BootP connectés sur le même réseau peuvent générer différentes réponses pour une même requête. Une réponse de serveur peut fournir l'adresse correcte alors qu'une autre réponse de serveur indique qu'aucune adresse n'est disponible. La réponse négative peut forcer le client à entrer en état d'erreur ou à prendre une adresse de repli.	Vous ne pourrez faire la distinction entre ce problème et les erreurs ci-dessus qu'avec un outil de capture de paquet. Utilisez alors un outil de capture de paquet Ethernet. Le résultat visible est que le client ne peut pas obtenir d'adresse IP. (L'équipement côté client peut renvoyer un code d'erreur ou accéder à l'adresse IP par défaut.)

Fichier de configuration

Thème	Problème
Adresse IP obtenue mais aucun fichier de configuration pour le système FDR	Un coupe-feu installé sur le serveur FDR peut autoriser la requête DHCP (pour une adresse IP) mais bloquer la requête FTP/TFTP pour le fichier de configuration. Lorsqu'un ordinateur est utilisé comme serveur FDR, le serveur de fichiers peut être placé sur une machine différente (inaccessible).

Dépannage SMTP

Les tableaux ci-dessous décrivent les solutions de dépannage pour les problèmes SMTP (*voir page 394*) rencontrés.

Connexion au serveur impossible

Thème	Problème	Résolution
Coupe-feu		Vérifiez que le coupe-feu autorise le trafic SMTP.
Mot de passe	Mot de passe incorrect.	Vérifiez que le serveur utilise le même mot de passe que le client. Vérifiez que les mots de passe sont corrects.

Envoi de messages impossible

Thème	Problème
Panne serveur	Vérifiez le compteur d'erreurs de connexion du serveur.

Messages lents à arriver

Problème	Résolution
Retards du serveur	Envoyez un message électronique à partir de l'ordinateur client pour confirmer qu'il s'agit bien d'un retard du serveur et non du client. Si le retard du serveur est confirmé, veuillez contacter le personnel informatique.

Tableau de dépannage de synchronisation horaire (NTP)

Les tableaux ci-dessous décrivent les solutions de dépannage pour la synchronisation horaire (NTP) (*voir page 230*).

Impossible d'obtenir l'heure du serveur

Thème	Problème
Format d'échange horaire invalide	Le serveur peut implémenter des diffusions générales SNTP. Les équipements Schneider prennent uniquement en charge les réponses de requêtes NTP/SNTP (et non pas les diffusions). Ce problème peut être détecté en examinant les configurations des équipements.
Impossible d'obtenir l'heure du serveur	Le serveur peut être protégé par un coupe-feu.

Imprécision de l'heure

Thème	Problème	Résolution
L'heure du serveur est imprécise ou instable	L'heure du serveur n'est pas précise, en particulier si le réseau utilise un ordinateur (au lieu d'un serveur dédié) comme serveur NTP. Les ordinateurs Windows sont particulièrement sensibles à ce problème, contrairement à un système Linux ou à un serveur de synchronisation dédié, qui sont eux capables de le corriger.	
Les retards du réseau entraînent des imprécisions horaires	Les charges irrégulières du réseau peuvent entraîner des retards conséquents dans le message de requête ou de réponse, sachant que les algorithmes NTP qui calculent l'heure se basent sur des retards de réseau uniformes. Ce problème peut être détecté en examinant les charges du réseau ou en utilisant un outil de capture de paquet Ethernet pour capturer les paquets de requête et de réponse. Certains équipements répertorient également les retards sur une page de diagnostic.	Pour résoudre ce problème, rapprochez le serveur de l'équipement client du réseau en : ● supprimant les routeurs et les commutateurs entre le serveur et le client ; ● mettant en place un réseau séparé (si possible un VLAN) pour le système NTP.

Tableau de dépannage Web

Accès impossible aux pages statiques

Thème	Problème	Résolution
Coupe-feu		Vérifiez que vous disposez de l'accès de sécurité approprié pour tous les équipements auxquels vous tentez d'accéder. De plus, le coupe-feu doit être configuré de façon à vous permettre d'accéder à votre requête HTTP.
Serveur proxy	Un serveur proxy peut autoriser l'accès à certaines pages Web uniquement par filtrage. Vérifiez que le serveur proxy ne filtre pas la page Web à laquelle vous souhaitez accéder.	

Accès impossible aux données dynamiques

Thème	Problème
Version Java	Si vous avez accès aux pages Web mais pas aux données dynamiques (comme les statistiques Ethernet), il se peut que l'applet Java ne soit pas compatible avec votre JVM. Une boîte de dialogue Java grise ou une erreur dans la barre d'état, au bas de la fenêtre du navigateur Web, signale ce problème.
Coupe-feu	Un coupe-feu peut également bloquer un protocole d'application particulier (comme Modbus TCP ou Uni-TE (502)), vous empêchant de visualiser vos données. Par exemple, une page Web ne pouvant afficher des données en temps réel indique que le protocole 502 est bloqué. Dans ce cas, les indications suivantes apparaissent : • points d'interrogation dans les champs de données ; • erreur signalant que l'équipement Modbus ne peut pas être atteint.
Paramètres de sécurité du navigateur	Vous ne pouvez pas télécharger d'applets Java si vous définissez des paramètres de sécurité élevés dans vos options Internet. Dans ce cas, une erreur de sécurité apparaît dans la barre d'état, au bas de la fenêtre du navigateur Web, pour signaler ce problème.
Contrôle d'accès à Modbus	Vérifiez l'équipement Schneider pour vous assurer que votre IP est bien défini comme l'IP dédié aux communications avec l'équipement. Dans ce cas, les indications suivantes apparaissent : • points d'interrogation dans les champs de données ; • erreur signalant que l'équipement Modbus ne peut pas être atteint.

4.4 Dépannage en cas de lenteur de réponse d'un système SCADA/HMI

Dépannage en cas de lenteur de réponse (SCADA/HMI)

Catégorie du problème	Thème	Suggestions
Déterminer la cause du retard	Déterminer si le retard se situe au niveau du trafic en écriture ou du trafic en lecture	Envoyez une commande d'opération de l'équipement et mesurez l'intervalle entre la transmission de la commande et la réaction de l'équipement. Déterminez si : - le retard se situe au niveau de l'écriture des données ou de la lecture de la réponse ; - une différence existe entre la lecture et l'écriture numérique et analogique des données. Remarque : Déterminez la réaction de l'équipement à partir de l'observation physique de l'équipement même et non pas à partir de l'affichage des états sur le système SCADA/HMI.
	Déterminer si le retard se situe côté SCADA ou côté serveur	A l'aide d'un outil PC séparé, envoyez une requête au serveur et mesurez le temps de réponse. Des requêtes de lecture et d'écriture distinctes doivent être envoyées pour chaque type de données pouvant être lu par le système SCADA. - Une réponse rapide du PC et une réponse lente du système SCADA indiquent un problème dans les communications SCADA. Les réponses SCADA peuvent être ralenties par le système SCADA ou par une file d'attente de requêtes SCADA sur le serveur. (Les autres requêtes, telles que les requêtes du PC, ne sont pas conservées dans cette file d'attente.) - Une réponse lente du PC révèle une surcharge du serveur, à laquelle vous pouvez remédier en réduisant la charge du serveur (voir page 308).

Catégorie du problème	Thème	Suggestions
Réponse lente provoquée par le système SCADA	SCADA est lent mais l'outil PC est rapide (vérifier le temps de réponse des requêtes SCADA du serveur)	Examinez le temps de réponse d'une requête SCADA sur le serveur à l'aide d'un outil de capture de paquet Ethernet. Pour cela, vérifiez chaque type de requête (lecture, écriture, numérique, analogique) utilisé par le système SCADA. Lors de cet examen, vous constaterez que, après avoir envoyé votre requête à mesurer, le serveur renvoie les réponses aux requêtes précédentes. Attendez impérativement la réponse à votre requête spécifique avant de calculer le temps de réponse. Pour identifier une paire de requête/réponse spécifique, vous devez utiliser un ID de transaction Modbus ou une autre caractéristique unique de la requête (par exemple, le nombre de registres requis). Si le temps de réponse observé est lent, une file d'attente de requêtes SCADA sur le serveur risque alors de retarder sérieusement le processus. Pour améliorer la réponse : ● réduisez le nombre de requêtes envoyées vers le serveur ; (voir page 308) ● créez une autre file d'attente pour l'accès aux données et envoyez les requêtes sur ce chemin. Cette méthode est efficace car l'ordinateur est capable d'obtenir une réponse rapide, indiquant que le serveur n'est pas surchargé. Pour cela, forcez le système SCADA à ouvrir des sockets TCP supplémentaires et répartissez les requêtes entre les sockets.
	SCADA est lent alors que l'ordinateur est rapide et qu'aucun retard n'est constaté sur les requêtes SCADA de l'équipement du serveur	Une file d'attente dans le système SCADA lui-même provoque ce retard. Cela peut se produire lorsque le système SCADA envoie une seule requête à la fois au serveur, notamment dans les systèmes dotés d'un seul socket TCP vers le serveur. La section SCADA (voir page 300) explique comment ouvrir davantage de sockets et envoyer plusieurs requêtes via un socket unique.

4.5 Dépannage du pont

Dépannage du pont

Catégorie du problème	Thème	Suggestions
Réponse lente ou communication défectueuse	réponse lente	Le pont comporte beaucoup trop d'appareils, côté ligne série.
	socket refusé	La plupart des ponts peuvent implémenter uniquement un nombre limité de sockets Ethernet. Ce nombre est généralement inférieur au nombre d'appareils connectés côté ligne série. Par conséquent, si nous utilisons un socket par équipement série, le nombre de sockets disponibles par pont sera inadéquat. Pour remédier à cela, réduisez le nombre d'appareils sur la ligne série ou sélectionnez l'appareil client Modbus qui peut envoyer des requêtes à des équipements série multiples sur un seul socket. Pour un scrutateur d'E/S qui analyse les appareils sur un pont, vous devez soit implémenter la fonctionnalité d'activation/désactivation, soit passer du scrutateur d'E/S aux blocs de communication du client Modbus. Le client peut signaler cette erreur. Sinon, vous devez soit connaître le numéro des sockets utilisés (via l'analyse des communications), soit utiliser un outil de capture de paquets Ethernet afin de visualiser le rejet du socket.
Communications défectueuses par intermittence	erreurs successives sur différents appareils	Les timeouts du côté Ethernet ne sont pas assez longs. (Ils sont inférieurs au nombre total de timeouts, côté série.) Voir le chapitre sur les passerelles (<i>voir page 335</i>) pour plus d'informations.
	erreurs intermittentes	Les timeouts côté Ethernet sont trop proches du temps requis pour collecter des données d'une ligne série. Voir le chapitre sur les passerelles (<i>voir page 335</i>) pour plus d'informations.

4.6 Dépannage en cas de perte de paquets

Introduction

Ce sous-chapitre décrit le mode de dépannage en cas de perte de paquets de données.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Dépannage en cas de perte de paquets	405
Utilisation d'un outil de capture de paquet	406
Dépannage de capture de paquet	408

Dépannage en cas de perte de paquets

Catégorie du problème	Thème	Cause et actions
Généralités	effet d'une perte d'un paquet	Une perte d'un paquet provoque une erreur sur un socket TCP. Cette erreur est généralement rétablie automatiquement, évitant ainsi tout avertissement en provenance de la couche applicative (par exemple, Modbus ou scrutateur d'E/S). Cependant, une erreur survient au niveau de la couche applicative lorsque le temps de récupération est supérieur au timeout de la couche applicative.
	détection des pertes de paquets	Il existe deux façons de détecter les pertes de paquets : ● <i>compteur de paquets reçus/envoyés</i> : utilisez cette méthode lorsque vous souhaitez vérifier qu'un paquet est envoyé pour chaque paquet reçu (par exemple, un système avec seulement un trafic client/serveur Modbus). Les compteurs conviennent aussi pour détecter un grand nombre de paquets perdus. ● <i>outil de capture de paquet Ethernet</i> : utilisez cette méthode pour visualiser la séquence TCP et les numéros d'accusés de réception pour identifier les paquets perdus. Les captures de paquets doivent utiliser la fonctionnalité horodateur pour corréler l'heure d'une perte de paquets avec l'heure de l'alarme sur un système SCADA ou l'heure d'un problème sur site.
Interventions en cas de perte de paquets	perte de paquets dans un commutateur ou un périphérique réseau	Cette erreur survient lorsque un paquet s'affiche sur un seul des côtés du commutateur. Ceci nécessite l'installation simultanée de deux outils de capture de paquets. Vérifiez la charge du commutateur afin de résoudre ce problème. Les appareils réseau rejettent certains paquets en cas de surcharge du commutateur. Le bruit électrique peut également altérer les paquets et provoquer un rejet.
	une perte de paquet entraîne une erreur au niveau de l'application	Si une perte de paquet provoque une erreur au niveau de l'application : ● augmentez le timeout de l'application pour permettre le rétablissement de la couche TCP ; ● modifiez les équipements pour accélérer le rétablissement de la couche TCP (nécessite le changement du micrologiciel) ; ● réduisez le nombre de pertes de paquets. Pour réduire le nombre de paquets perdus, vous devez : ● réduire le trafic sur le réseau ; ● éliminer les liens semi-duplex ; ● réduire le bruit électrique. Ces changements ne réduisent que la perte de paquets. Ils n'éliminent pas le problème.

Utilisation d'un outil de capture de paquet

Vue d'ensemble

Dans un système idéal, tous les équipements devraient détecter et signaler la cause exacte des erreurs réseau, mais cela n'est pas toujours possible. Un équipement peut être incapable de détecter ou de signaler une erreur.

Si l'équipement indique uniquement une erreur générale (au lieu d'une erreur spécifique), vous pouvez utiliser un outil de capture de paquet Ethernet pour contrôler les paquets Ethernet et déterminer l'erreur spécifique et sa cause. Ceci permet de déterminer l'erreur réelle et la couche précise (IP/TCP ou application) où l'erreur s'est produite, afin de prendre une mesure corrective. Nous ne recommandons pas l'utilisation d'outils de capture de paquet pour l'entretien général d'une usine, mais ces outils s'avèrent particulièrement adaptés au diagnostic de problèmes intermittents ou qui se produisent lors de l'installation des équipements.

Ces outils capturent les paquets réseau et les affichent à l'écran. Ils sauvegardent également les paquets dans un fichier que vous pouvez analyser ultérieurement.

Types d'outils

Types d'outils de capture de paquet Ethernet :

- *Couche physique* : ces outils coûteux capturent les signaux physiques sur le câble et les données logiques sur la couche supérieure.
- *Portatifs* : ces outils analysent uniquement les couches 2, 3 et 4. Ils ne coûtent pas aussi chers que les outils de couche physique et sont suffisamment solides pour être utilisés sur le terrain.
- *Basés sur ordinateur* : ces outils utilisent une carte Ethernet d'ordinateur pour capturer les données réseau et les analyser dans un logiciel. Du fait des grandes différences de prix entre les modèles (des logiciels gratuits à ceux coûtant plus de 20 000 dollars), le niveau d'analyse automatique et les services d'assistance technique de ces outils varient eux aussi de manière significative. Ils analysent uniquement les couches 2, 3 et 4.

Capacités des outils

Les outils de capture de paquet Ethernet peuvent détecter ou déterminer :

- la charge totale du trafic réseau, à savoir : les équipements contribuant à la congestion du réseau, la nature du trafic (VoIP, diffusion Windows ou trafic de scrutation des E/S) ;
- le trafic de diffusion et ses causes ;
- la liste d'équipements auxquels un équipement spécifique s'adresse et le protocole de communication utilisé ;
- les détails des communications entre les équipements : protocoles, codes fonction, adresses et valeurs des données transférées/demandées ;
- le temps de réponse d'une couche d'application d'un équipement ;
- les pertes de paquets ou les multiples tentatives TCP ;
- les communications depuis et vers un équipement subissant des erreurs de socket TCP (connexions rejetées, paquets perdus, etc.).

Tous les outils de capture de paquet Ethernet peuvent analyser l'ensemble de ces points, mais seuls les outils plus performants effectuent une analyse automatique et signalent les erreurs sur l'écran d'alarme.

Dépannage de capture de paquet

Catégorie du problème	Thème	Suggestions
Les paquets émis par l'équipement requis ne sont pas visibles	Seuls les paquets émis par et vers l'ordinateur hôte sont capturés par l'outil.	Le logiciel n'est pas en <i>mode promiscuité</i>. Activez ce mode pour permettre à l'ordinateur de capturer toutes les données visibles sur le câble Ethernet connecté à l'ordinateur. Sur la plupart des outils, vous pouvez régler ce mode comme option générale pour toutes les captures ou uniquement lorsque la capture commence. Vous avez besoin d'un lecteur de carte Ethernet spécial pour activer cette fonction. La plupart des outils incluent des lecteurs de carte Ethernet, mais les cartes ne fonctionnent pas toutes sur tous les systèmes.
	Les paquets émis par l'équipement en cours d'analyse ne sont pas capturés, contrairement aux paquets de diffusion.	Lorsqu'un paquet arrive au niveau d'un commutateur, ce dernier envoie le paquet uniquement sur le dernier port à avoir été connecté à l'équipement de destination. C'est pourquoi un outil de capture de paquet connecté à un port libre sur le commutateur ne voit pas le paquet. Pour permettre à l'outil de capture de paquet de voir le paquet, effectuez les opérations suivantes : ● Remplacez le commutateur par un concentrateur : dans ce cas, tout le trafic depuis et vers les équipements connectés au concentrateur sera visible. ● Insérez un concentrateur entre l'équipement en question et le commutateur : l'outil de capture de paquet est alors connecté au concentrateur, ce qui vous permet de voir uniquement les paquets émis par et vers l'équipement en question. ● Activez la mise en miroir des ports : cette opération configure le commutateur pour qu'il transmette une copie de tous les paquets envoyés et reçus sur un port à un autre port auquel l'outil de capture de paquet est connecté. (La mise en miroir des ports n'est pas prise en charge par tous les commutateurs.) ● Configurez le commutateur pour qu'il fonctionne comme un concentrateur : certains commutateurs gèrent cette fonction comme une option de désactivation de la mémorisation. Dans ce cas, le commutateur ne détermine plus la destination des données et envoie l'ensemble des données à tous les ports. Remarque : Ces solutions de dépannage entraînent des transmissions de données à des ports Ethernet qui ne reçoivent normalement pas de données lorsque le réseau n'est pas analysé. Cela risque d'entraîner un accroissement du trafic sur le réseau (en plus d'autres résultats indésirables).

Catégorie du problème	Thème	Suggestions
Paquets d'erreurs trouvés dans une capture	La capture de données dans le cas d'erreurs intermittentes génère des fichiers de taille excessive.	Pour les erreurs qui se produisent plusieurs fois par heure ou par jour, la capture risque de devoir fonctionner pendant plusieurs heures. Cela génère des milliers de paquets dans le fichier qui doit être analysé lors de la recherche d'erreurs. Etant donné qu'un fichier aussi volumineux consomme des centaines de Mo d'espace disque, il est difficile de lancer une analyse sur des périodes de 24 heures. Par conséquent, une erreur peut se produire alors que l'analyseur ne fonctionne pas. Pour éviter cela, l'outil de capture de paquet peut être réglé pour limiter la durée de collecte des données ou le nombre de paquets dans le fichier de capture. Lorsque la limite prédéfinie est atteinte, le fichier se ferme et l'outil ouvre un nouveau fichier. Une fois le nombre défini de fichiers atteint, l'outil arrête d'enregistrer ou commence à écraser les fichiers existants, dans l'ordre de leur création. Chaque fichier ainsi créé est horodaté lorsqu'il est fermé par l'outil. En utilisant un système SCADA ou un autre système d'usine pour enregistrer les heures de génération des erreurs (par exemple, l'arrêt de l'usine ou la non disponibilité d'un équipement), vous pouvez ouvrir le fichier correct pour trouver les paquets échangés au moment de l'erreur. L'outil marque sur chaque paquet l'heure exacte, ce qui vous permet de trouver les paquets spécifiques au moment de l'erreur. Notez que les paquets rapportant le problème sont généralement visibles avant que le système SCADA ne signale l'erreur, du fait des délais de rapport et de timeout.
	Filtrage des données capturées (afin d'obtenir uniquement les paquets requis).	Utilisez le filtrage de données pour trouver les paquets que vous souhaitez analyser. Utilisez pour cela l'une des deux méthodes de filtrage suivantes : ● <i>Pendant la capture</i> : le filtrage effectué pendant la capture risque d'ignorer les paquets nécessaires pour l'analyse ultérieure. Dans ce cas, vous devez recommencer la capture. ● <i>Parmi les données stockées</i> : méthode conseillée. Filtrez en fonction de l'adresse (IP ou MAC) et du protocole (numéro de socket de destination). Filtrez ensuite les données visibles vers un socket TCP unique en fonction du numéro de socket source.

Annexes



Contenu de cette annexe

Cette annexe contient les chapitres suivants :

Chapitre	Titre du chapitre	Page
A	Temps de réponse de la scrutation d'E/S	413
B	Débit de serveurs Modbus	441
C	Temps de réponse des clients Modbus	447
D	Mesures du timeout et du temps de réponse de la passerelle	491
E	Normes et autres considérations relatives aux réseaux Ethernet industriel	525
F	Procédures de mise à la terre (masse)	547

Temps de réponse de la scrutation d'E/S



Vue d'ensemble

Cette annexe indique les temps de réponse du scrutateur d'E/S pour les systèmes Premium et Quantum qui utilisent un réseau Ethernet industriel.

Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
A.1	Temps de réponse du scrutateur d'E/S des automates Premium	414
A.2	Temps de réponse du scrutateur d'E/S des automates Quantum	427

A.1 Temps de réponse du scrutateur d'E/S des automates Premium

Vue d'ensemble

Les courbes de temps de réponse système illustrées dans cette section sont basées sur des mesures effectuées sur des automates Premium qui scrutent des équipements Momentum 170 ENT 110 00. Momentum a été utilisé car il fournit les meilleurs temps de réponse pour les applications Ethernet (entre 5 et 8 ms). Trois scénarios de temps de réponse sont présentés.

Contenu de ce sous-chapitre

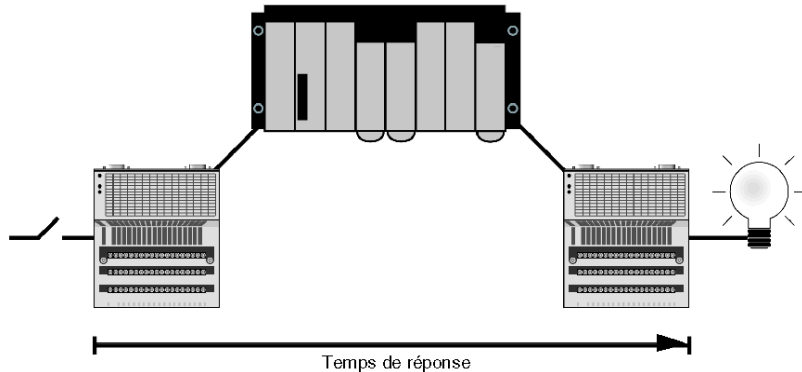
Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du scrutateur d'E/S Premium : Entrée distante vers sortie distante	415
Temps de réponse du scrutateur d'E/S Premium : Entrée distante vers sortie locale	419
Temps de réponse du scrutateur d'E/S Premium : Mémoire de l'automate vers sortie distante	423

Temps de réponse du scrutateur d'E/S Premium : Entrée distante vers sortie distante

Configuration de la mesure

Les courbes ci-dessous illustrent les temps de réponse de l'automate Premium lorsqu'un signal est envoyé d'un module d'entrée distant à un module de sortie distant via l'automate :



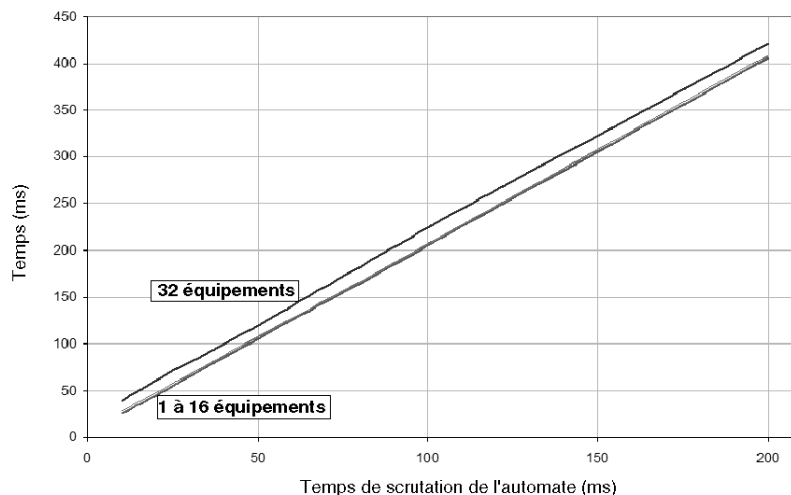
Le signal est :

- déclenché par un module d'entrée Momentum avec un temps de réponse d'environ 2 ms ;
- analysé dans l'automate Premium à une fréquence de répétition de 0 ms (*voir page 192*) ;
- copié dans une autre variable interne de l'automate ;
- écrit dans un module de sortie Momentum avec un temps de réponse d'environ 2 ms.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

UC TSXP575634M avec port Ethernet intégré

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0, tout comme son port Ethernet intégré.



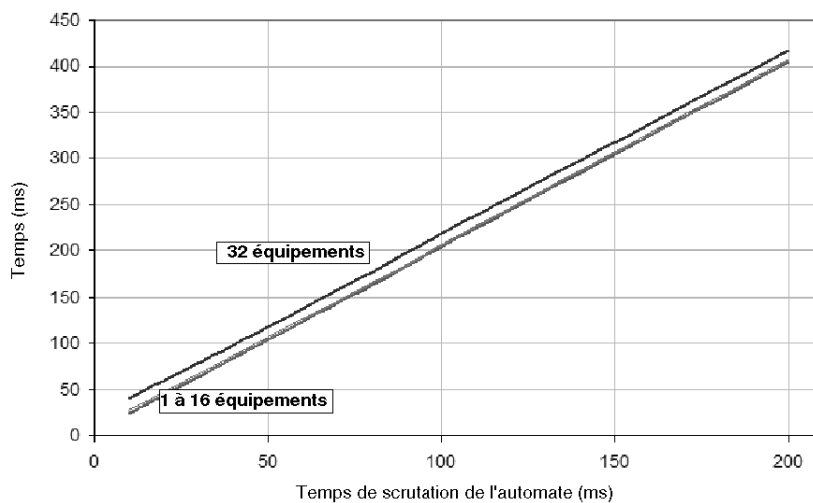
La courbe du bas indique que les temps de réponse pour 1 à 8 équipements présentent un écart inférieur à 1 ms. Les temps de réponse pour 16 équipements augmentent de 2 à 3 ms. Pour 32 équipements, les temps de réponse sont plus longs de 11 à 14 ms environ.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634M (v2.0) + port Ethernet intégré (v2.0)					
1 équipement	25	45	106	205	406
8 équipements	26	46	107	206	407
16 équipements	28	48	108	207	409
32 équipements	39	61	120	224	421

UC TSXP575634M avec module TSXETY5103

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



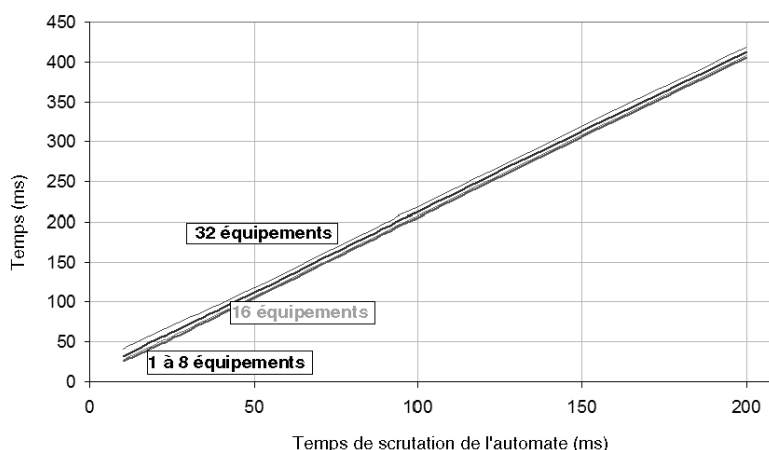
La courbe du bas indique que les temps de réponse pour 1 à 8 équipements présentent un écart inférieur à 1 ms. Les temps de réponse pour 16 équipements augmentent de 2 à 3 ms. Pour 32 équipements, les temps de réponse sont plus longs de 12 à 16 ms environ.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634 (v2.0) + ETY 5103 (v3.1)					
1 équipement	24	44	104	204	405
8 équipements	25	45	105	205	406
16 équipements	28	47	107	206	408
32 équipements	40	60	118	218	417

UC TSXP57304M avec module TSXETY5103

L'UC TSXP57304M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



La courbe du bas indique que les temps de réponse pour 1 à 8 équipements présentent un écart inférieur à 2 ms. Les temps de réponse pour 16 équipements augmentent de 3 à 4 ms. Pour 32 équipements, les temps de réponse sont plus longs de 10 à 16 ms environ.

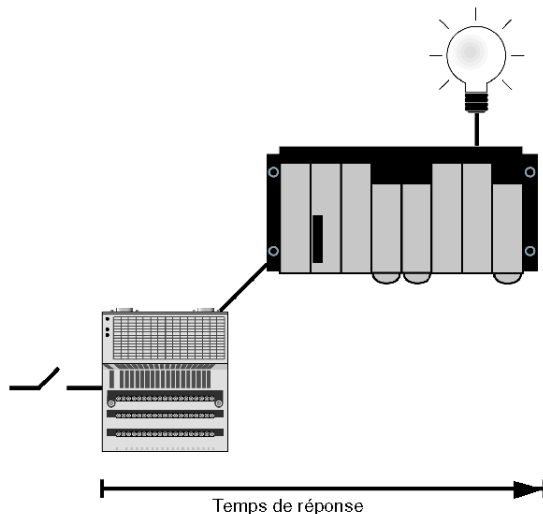
Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP57304M (v2.0) + ETY 5103 (v3.1)					
1 équipement	25	44	105	206	406
8 équipements	27	47	107	208	408
16 équipements	31	52	112	213	413
32 équipements	41	60	118	219	419

Temps de réponse du scrutateur d'E/S Premium : Entrée distante vers sortie locale

Configuration de la mesure

Les courbes ci-dessous illustrent les temps de réponse de l'automate Quantum lorsqu'un signal est envoyé d'un module d'entrée distant à un module de sortie Premium dans l'automate :



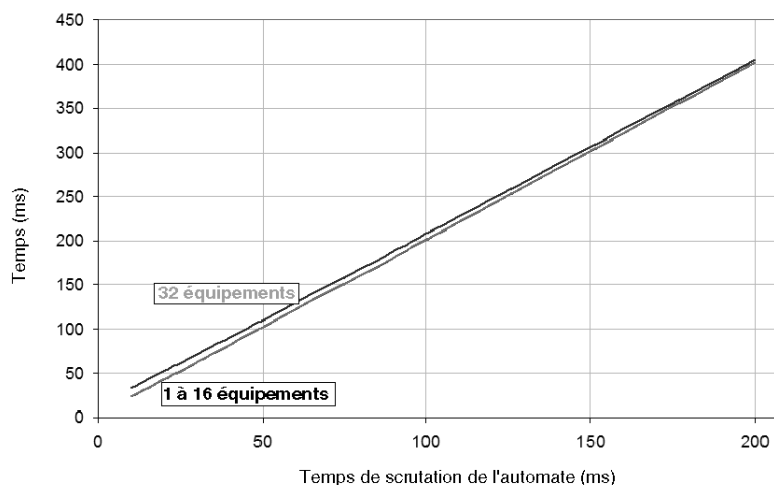
Le signal est :

- déclenché par un module d'entrée Momentum avec un temps de réponse d'environ 2 ms ;
- analysé dans l'automate Premium à une fréquence de répétition de 0 ms (*voir page 192*) ;
- copié dans une autre variable interne de l'automate ;
- inscrit dans un module de sortie Premium local.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

UC TSXP575634M avec port Ethernet intégré

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0, tout comme son port Ethernet intégré.



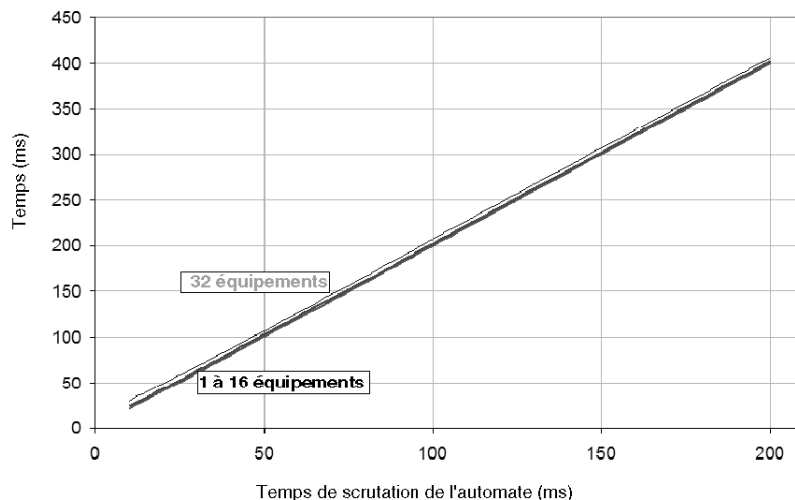
La courbe du bas indique que les temps de réponse pour 1 à 16 équipements présentent un écart inférieur à 1 ms. Les temps de réponse pour 32 équipements sont plus longs de 9 à 10 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse diminue.

Le tableau suivant indique les données utilisées pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634M (v2.0) + port Ethernet intégré (v2.0)					
1 équipement	23	42	102	201	402
8 équipements	23	42	102	201	402
16 équipements	24	43	103	202	403
32 équipements	33	52	110	208	405

UC TSXP575634M avec module TSXETY5103

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



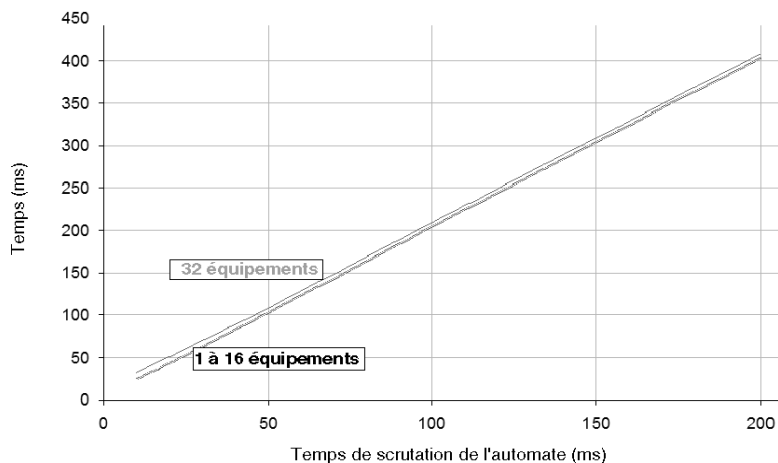
La courbe du bas indique que les temps de réponse pour 1 à 16 équipements présentent un écart inférieur à 3 ms. Les temps de réponse pour 32 équipements sont plus longs de 6 à 9 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse diminue.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634M (v2.0) + ETY5103 (v3.1)					
1 équipement	21	41	101	200	400
8 équipements	22	42	102	201	401
16 équipements	24	43	103	202	402
32 équipements	30	49	107	207	406

UC TSXP57304M avec module TSXETY5103

L'UC TSXP57304M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



La courbe du bas indique que les temps de réponse pour 1 à 16 équipements sont identiques ou présentent un écart inférieur à 1 ms. Les temps de réponse pour 32 équipements sont plus longs de 6 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse diminue lentement.

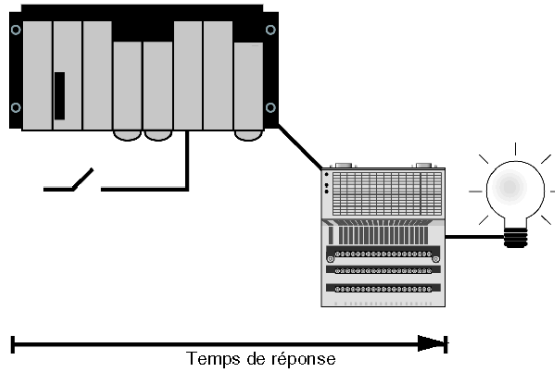
Le tableau suivant indique les données utilisées pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP57304M (v2.0) + ETY5103 (v3.1)					
1 équipement	24	43	103	204	404
8 équipements	24	43	103	204	404
16 équipements	24	43	103	204	404
32 équipements	32	51	108	209	409

Temps de réponse du scrutateur d'E/S Premium : Mémoire de l'automate vers sortie distante

Configuration de la mesure

La série de courbes ci-dessous illustre les temps de réponse de l'automate Quantum lorsqu'un signal est envoyé de l'automate à un module de sortie distant :

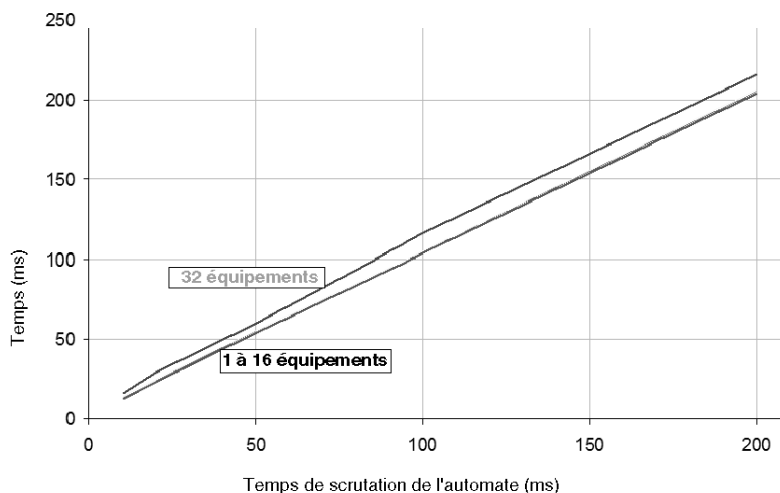


Le signal est écrit dans un module de sortie Momentum avec un temps de réponse d'environ 2 ms.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

UC TSXP575634M avec port Ethernet intégré

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0, tout comme son port Ethernet intégré.



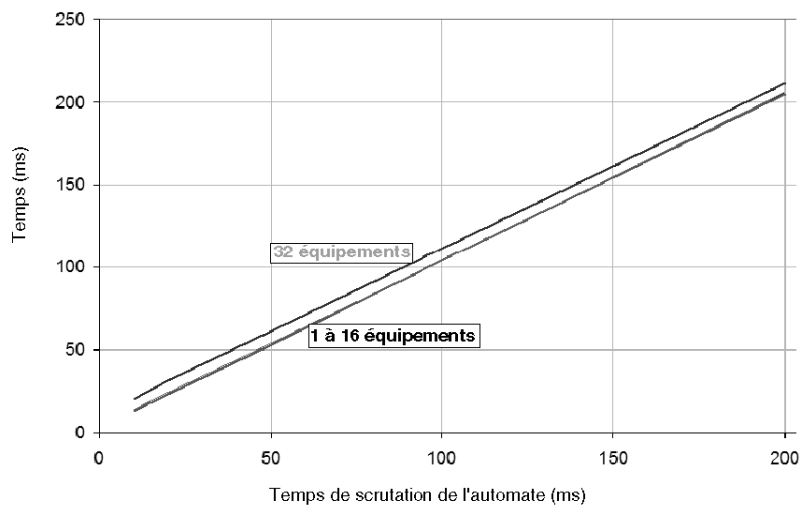
La courbe du bas indique que les temps de réponse pour 1 à 16 équipements varient de 1 à 2 ms selon les cas. Les temps de réponse pour 32 équipements sont plus longs de 2 à 4 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse s'amplifie.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre la mémoire de l'automate et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634M (v2.0) + port Ethernet intégré (v2.0)					
1 équipement	12	23	54	104	204
8 équipements	13	23	55	105	205
16 équipements	14	25	55	105	206
32 équipements	16	29	60	116	216

UC TSXP575634M avec module TSXETY5103

L'UC TSXP575634M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Son module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



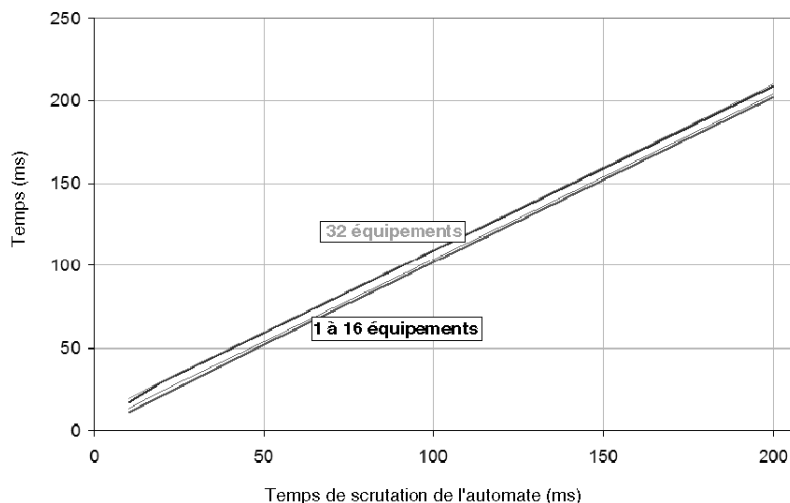
La courbe du bas indique que les temps de réponse pour 1 à 16 équipements varient de 1 à 4 ms selon les cas. Les temps de réponse pour 32 équipements sont plus longs de 6 à 9 ms.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre la mémoire de l'automate et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP575634M (v2.0) + ETY5103 (v3.1)					
1 équipement	13	23	53	104	205
8 équipements	13	23	53	104	205
16 équipements	14	24	54	104	206
32 équipements	20	31	61	111	211

UC TSXP57304M avec module TSXETY5103

L'UC TSXP57304M utilisée pour les mesures ci-dessous est au niveau de version 2.0. Son module de communication Ethernet TSXETY55103 est au niveau de version 3.1.



La courbe du bas indique que les temps de réponse pour 1 à 16 équipements sont identiques. Les temps de réponse pour 32 équipements sont plus longs de 8 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse se réduit.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre la mémoire de l'automate et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
TSXP57304M (v2.0) + ETY5103 (v3.1)					
1 équipement	11	21	52	102	202
8 équipements	13	24	54	104	204
16 équipements	17	29	59	109	209
32 équipements	19	30	60	110	210

A.2 Temps de réponse du scrutateur d'E/S des automates Quantum

Vue d'ensemble

Les courbes de temps de réponse système illustrées dans cette section sont basées sur des mesures effectuées sur des automates Quantum qui scrutent des équipements Momentum 170 ENT 110 00. Momentum a été utilisé car il fournit les meilleurs temps de réponse pour les applications Ethernet (entre 5 et 8 ms). Trois scénarios de temps de réponse sont présentés.

Contenu de ce sous-chapitre

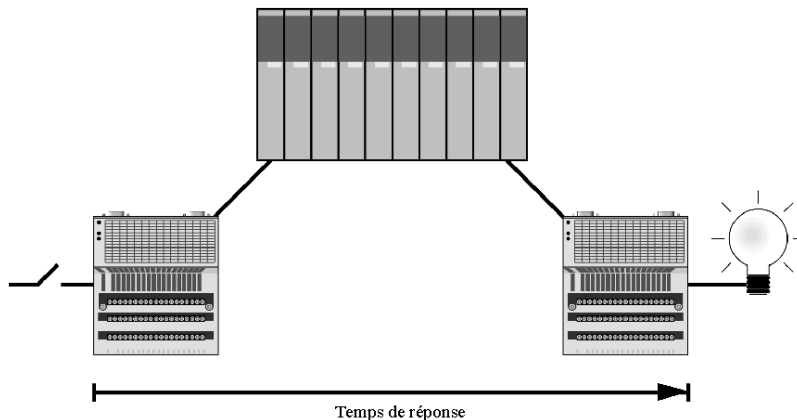
Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du scrutateur d'E/S Quantum : entrée distante vers sortie distante	428
Temps de réponse du scrutateur d'E/S Quantum : Entrée distante vers sortie locale	432
Temps de réponse du scrutateur d'E/S Quantum : Entrée locale vers sortie distante	436

Temps de réponse du scrutateur d'E/S Quantum : entrée distante vers sortie distante

Configuration de la mesure

Les courbes ci-dessous illustrent les temps de réponse de l'automate Quantum lorsqu'un signal est envoyé d'un module d'entrée distant à un module de sortie distant via l'automate :



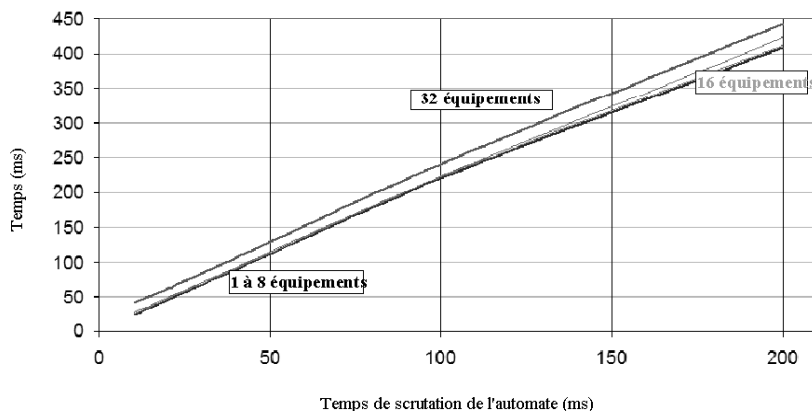
Le signal est :

- déclenché par un module d'entrée Momentum avec un temps de réponse d'environ 2 ms ;
- analysé dans l'automate Quantum à un taux de répétition de 0 ms (*voir page 192*) ;
- copié dans une autre variable interne de l'automate ;
- écrit dans un module de sortie Momentum avec un temps de réponse d'environ 2 ms.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

140CPU65150 avec port Ethernet intégré

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0, avec un port Ethernet au niveau de version 3.1.



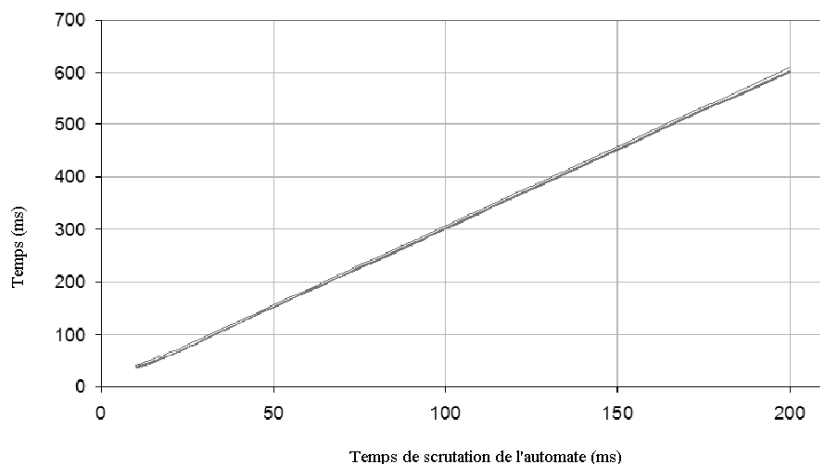
La courbe du bas indique que les temps de réponse pour 1 à 8 équipements varient de 1 à 3 ms selon les cas. Les temps de réponse pour 16 équipements sont plus longs de 2 à 4 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse s'amplifie (par exemple, 11 ms pour une fréquence de scrutation de 200 ms). Les temps de réponse pour 32 équipements sont plus longs de 13 à 17 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse s'amplifie (par exemple, 34 ms de plus pour une fréquence de scrutation de 200 ms).

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + port Ethernet intégré (v3.1)					
1 équipement	25	46	112	220	409
8 équipements	26	47	113	222	412
16 équipements	28	49	115	223	423
32 équipements	42	62	129	241	443

140CPU65150 avec module 140NOE771x1

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet 140NOE771x1 est au niveau de version 3.5.



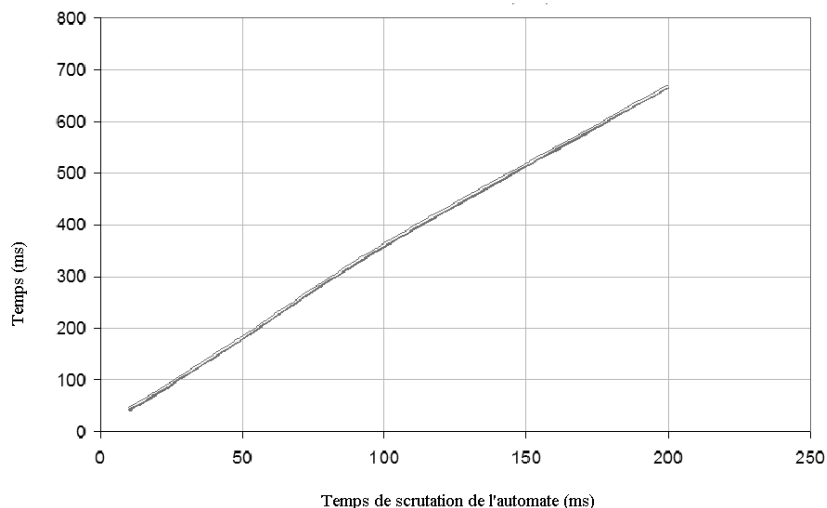
Les courbes ci-dessus indiquent que les temps de réponse présentent un écart compris entre 5 et 7 ms, quel que soit le nombre d'équipements.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + NOE771x1 (v3.5)					
1 équipement	35	61	153	302	602
8 équipements	36	62	154	303	603
16 équipements	38	64	155	305	606
32 équipements	40	66	157	307	609

140CPU43412A avec module 140NOE771x1

L'UC 140CPU43412A utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet 140NOE771x1 est au niveau de version 3.5.



Les courbes ci-dessus indiquent que les temps de réponse présentent un écart compris entre 5 et 6 ms, quel que soit le nombre d'équipements.

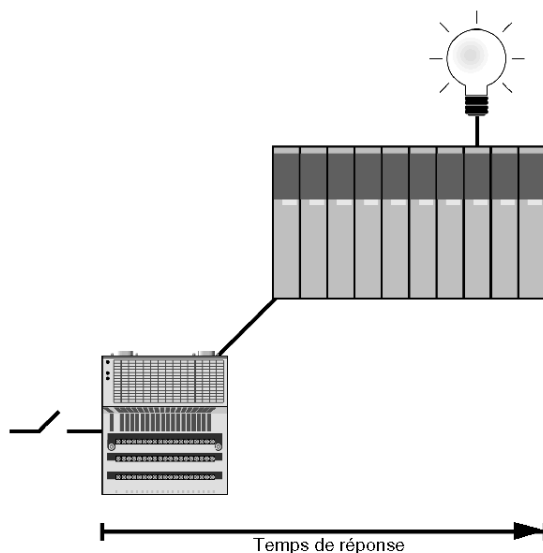
Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie de l'équipement scruté (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU43412A (v2.0) + NOE771x1 (v3.5)					
1 équipement	41	73	179	358	665
8 équipements	42	75	180	360	666
16 équipements	44	77	182	361	668
32 équipements	46	79	185	364	671

Temps de réponse du scrutateur d'E/S Quantum : Entrée distante vers sortie locale

Configuration de la mesure

Les courbes ci-dessous illustrent les temps de réponse de l'automate Quantum lorsqu'un signal est envoyé d'un module d'entrée distant à un module de sortie local dans l'automate :



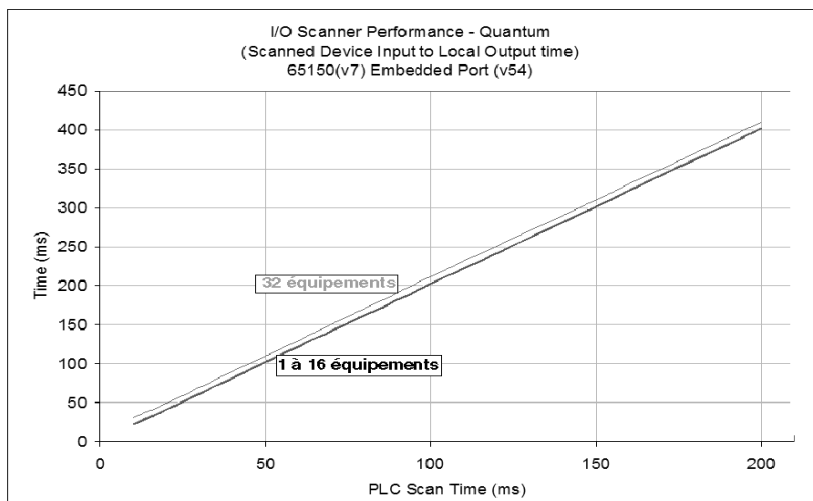
Le signal est :

- déclenché par un module d'entrée Momentum avec un temps de réponse d'environ 2 ms ;
- analysé dans l'automate Quantum à une fréquence de répétition de 0 ms (voir page 192) ;
- copié dans une autre variable interne de l'automate ;
- inscrit dans un module de sortie Quantum local.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

140CPU65150 avec port Ethernet intégré

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0, avec un port Ethernet au niveau de version 3.1.



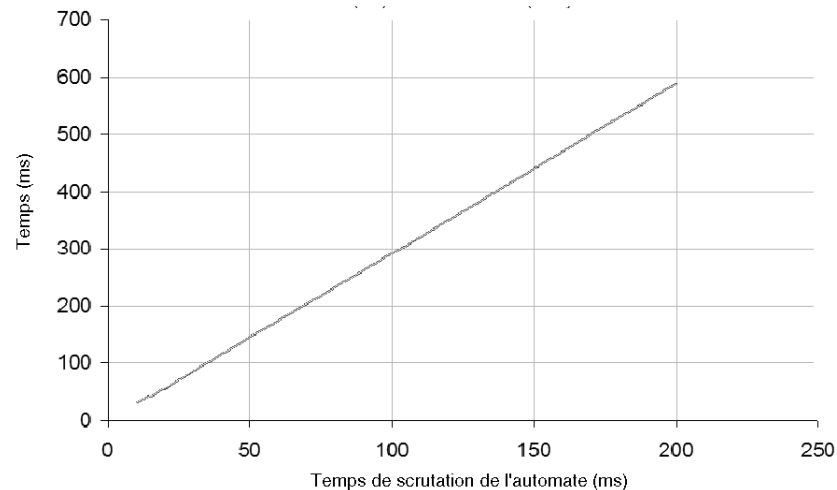
La courbe du bas indique que les temps de réponse pour 1 à 16 équipements présentent un écart inférieur à 2 ms, quel que soit le temps de scrutation de l'automate. La courbe du haut montre que les temps de réponse pour 32 équipements sont supérieurs de 7 à 8 ms.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + port Ethernet intégré (v3.1)					
1 équipement	22	41	102	202	402
8 équipements	23	42	103	204	403
16 équipements	24	43	104	204	404
32 équipements	31	49	110	211	410

140CPU65150 avec module 140NOE771x1

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0, avec un module de communication Ethernet 140NOE771x1 au niveau de version 3.5.



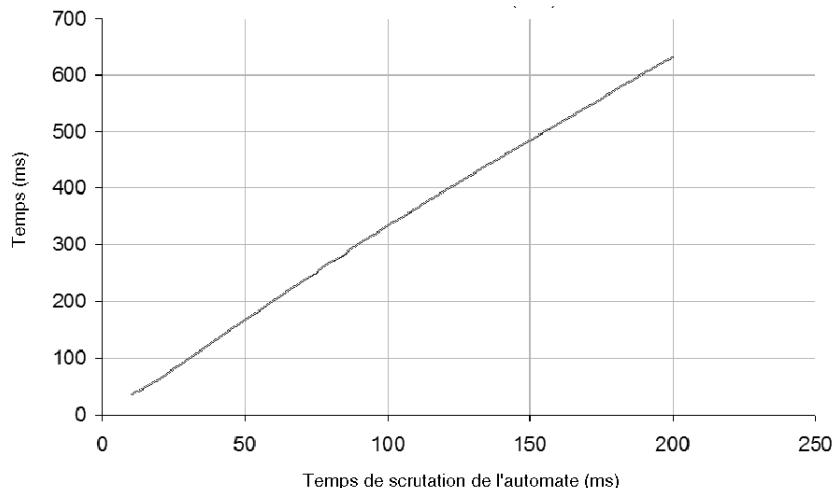
Les courbes ci-dessus montrent que les temps de réponse sont identiques pour 1, 8, 16 et 32 équipements.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + NOE771x1 (v3.5)					
1 équipement	31	56	145	292	590
8 équipements	31	56	145	292	590
16 équipements	31	56	145	292	590
32 équipements	31	56	145	292	590

140CPU43412A avec module 140NOE771x1

L'UC 140CPU43412A utilisée pour les mesures ci-dessous est au niveau de version 2.0, avec un module de communication Ethernet 140NOE771x1 au niveau de version 3.5.



Les courbes ci-dessus montrent que les temps de réponse sont identiques pour 1, 8, 16 et 32 équipements.

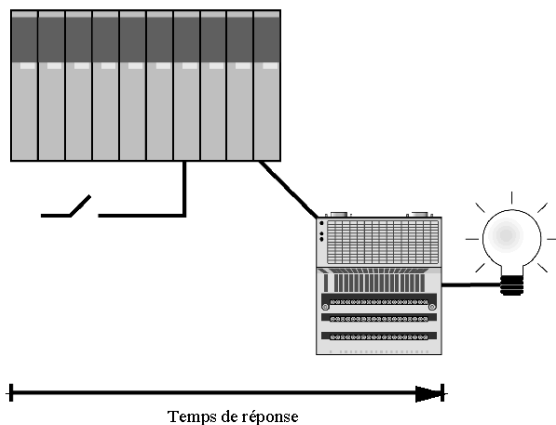
Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU43412A (v2.0) + NOE771x1 (v3.5)					
1 équipement	35	64	168	334	634
8 équipements	35	64	168	334	634
16 équipements	35	64	168	334	634
32 équipements	35	64	168	334	634

Temps de réponse du scrutateur d'E/S Quantum : Entrée locale vers sortie distante

Configuration de la mesure

Les courbes ci-dessous illustrent les temps de réponse de l'automate Quantum lorsqu'un signal est envoyé de l'automate local à un module de sortie distant :



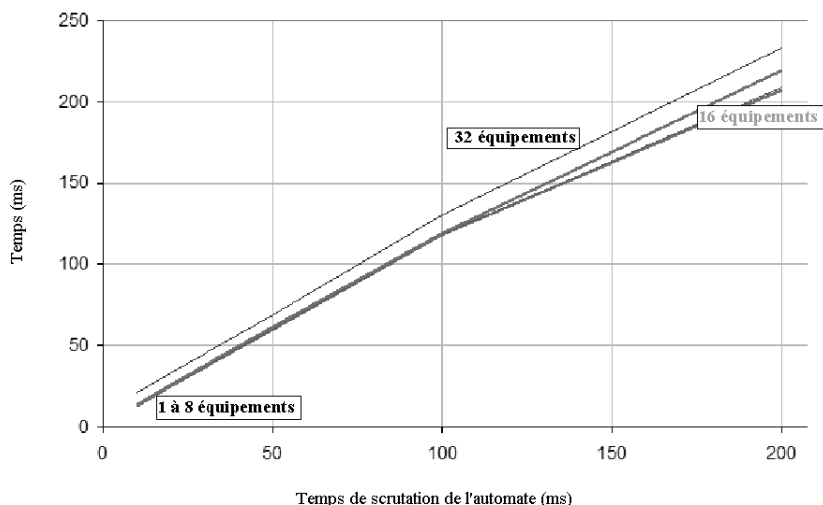
Le signal est :

- déclenché par un module d'entrée Quantum local ;
- analysé dans l'automate Quantum à une fréquence de répétition de 0 ms (*voir page 192*) ;
- copié dans une autre variable interne de l'automate ;
- écrit dans un module de sortie Momentum distant avec un temps de réponse d'environ 2 ms.

Les résultats sont tracés pour 1, 8, 16 et 32 équipements.

140CPU65150 avec port Ethernet intégré

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0. Son port Ethernet intégré est au niveau de version 3.5.



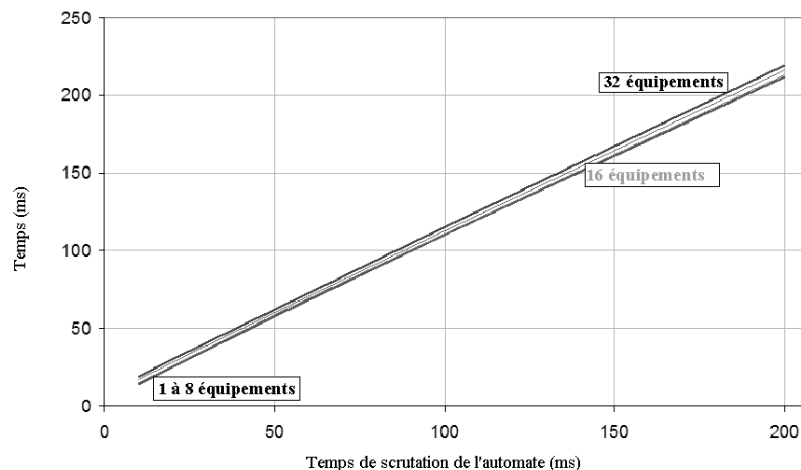
La courbe du bas indique que les temps de réponse pour 1 à 8 équipements sont pratiquement identiques, à l'exception d'une différence de 2 ms pour un temps de scrutation de 200 ms. Les temps de réponse pour 16 équipements sont plus longs de 1 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse s'amplifie jusqu'à atteindre 10 à 12 ms pour une fréquence de scrutation de 200 ms. Les temps de réponse pour 32 équipements sont plus longs de 7 à 8 ms. A mesure que le temps de scrutation augmente, la différence entre les temps de réponse s'amplifie (par exemple, de 14 à 16 ms de plus pour une fréquence de scrutation de 200 ms).

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + port Ethernet intégré (v3.1)					
1 équipement	13	25	60	118	207
8 équipements	13	25	60	118	209
16 équipements	14	26	61	119	219
32 équipements	21	33	69	130	233

140CPU65150 avec module Ethernet 140NOE771x1

L'UC 140CPU65150 utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet 140NOE771x1 est au niveau de version 3.5.



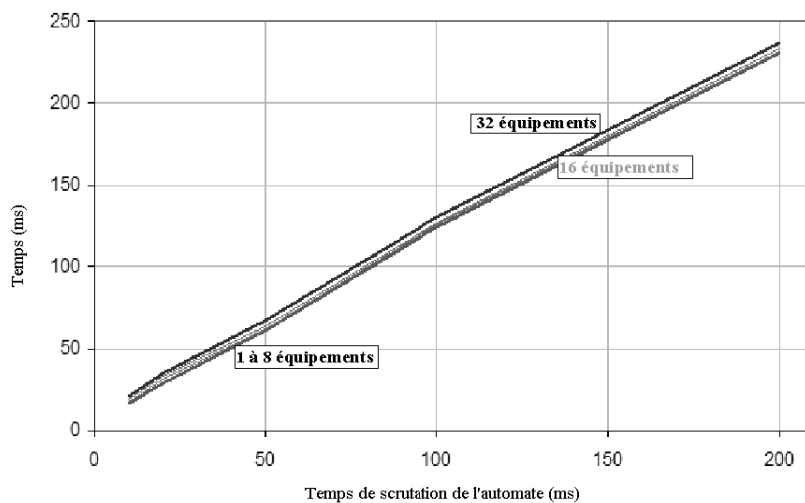
Les courbes ci-dessus indiquent que les temps de réponse présentent un écart compris entre 5 et 7 ms, quel que soit le nombre d'équipements.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU65150 (v2.0) + NOE771x1 (v3.5)					
1 équipement	14	25	58	110	212
8 équipements	15	26	59	111	213
16 équipements	17	28	60	113	216
32 équipements	19	30	62	115	219

140CPU43412A avec module Ethernet 140NOE771x1

L'UC 140CPU43412A utilisée pour les mesures ci-dessous est au niveau de version 2.0. Le module de communication Ethernet 140NOE771x1 est au niveau de version 3.5.



Les courbes ci-dessus indiquent que les temps de réponse présentent un écart compris entre 5 et 6 ms, quel que soit le nombre d'équipements.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Nombre d'équipements à scruter	Délai entre l'entrée de l'équipement scruté et la sortie locale (ms)				
	Scrutation de 10 ms	Scrutation de 20 ms	Scrutation de 50 ms	Scrutation de 100 ms	Scrutation de 200 ms
140CPU43412A (v2.0) + NOE771x1 (v3.5)					
1 équipement	16	29	61	124	231
8 équipements	17	31	62	126	232
16 équipements	19	33	64	127	234
32 équipements	21	35	67	130	237

Débit de serveurs Modbus



Vue d'ensemble

Cette annexe indique le débit de serveurs Modbus pour les systèmes Premium et Quantum qui utilisent un réseau Ethernet industriel.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

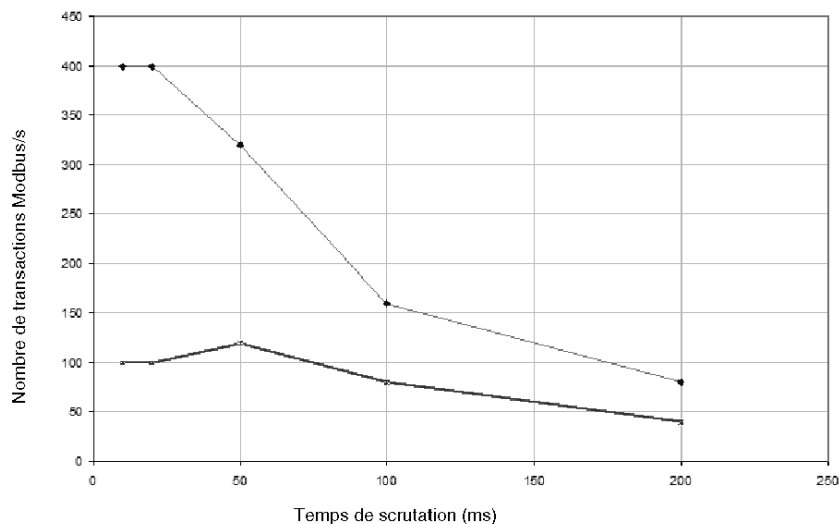
Sujet	Page
Débit des serveurs Modbus Quantum : Unity v2.0	442
Débit des serveurs Modbus Premium : Unity v2.0	444

Débit des serveurs Modbus Quantum : Unity v2.0

Mesures de performance

Le diagramme ci-dessous indique le nombre de requêtes de lecture de registre Modbus auxquelles les UC Quantum peuvent répondre en 1 s. (Une requête de lecture de registre est une commande de fonction Modbus de code 3.) Le délai minimum de réponse à une requête Modbus correspond à un cycle de scrutation d'un automate. Le débit de cinq systèmes est mesuré :

- une UC 140CPU65150 avec un module de communication Ethernet 140NOE77101 ;
- une UC 140CPU65150 avec un module de communication Ethernet 140NOE77111 ;
- une UC 140CPU43412A avec un module de communication Ethernet 140NOE77101 ;
- une UC 140CPU43412A avec un module de communication Ethernet 140NOE77111 ;
- une UC 140CPU65150 avec un port Ethernet intégré.



Les quatre courbes du bas (fondues en une même ligne car ayant des valeurs identiques) indiquent le débit des quatre UC qui utilisent les modules NOE. La courbe du haut indique le débit de l'UC équipée d'un port Ethernet intégré. A mesure que les temps de scrutation augmentent, la différence de débit (le nombre de transactions Modbus/messages) entre les UC équipées de modules NOE et celles disposant du port Ethernet intégré diminue.

Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

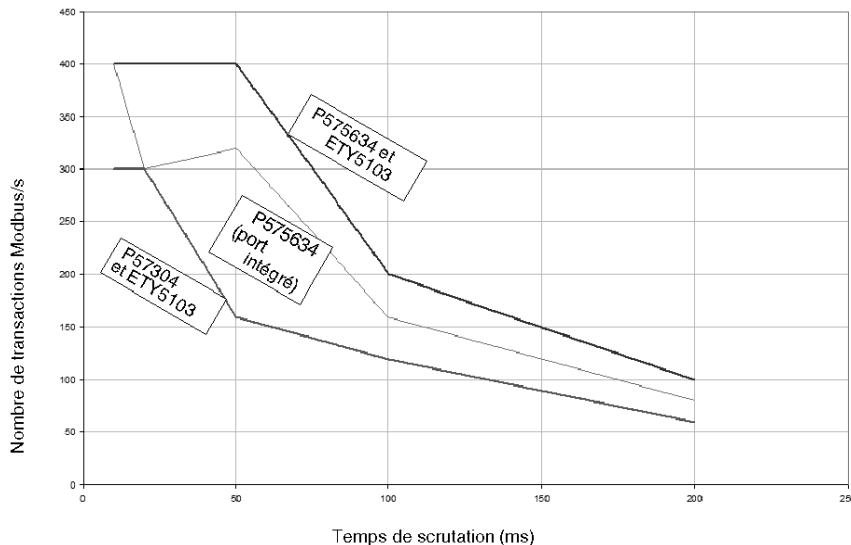
Temps de scrutation (ms)	65150 (port intégré)	65150 + NOE77101	65150 + NOE77111	43412A + NOE77101	43412A+ NOE77111
Temps de scrutation	Nombre de transactions Modbus/seconde				
10	400	100	100	100	100
20	400	100	100	100	100
50	320	120	120	120	120
100	160	80	80	80	80
200	80	40	40	40	40

Débit des serveurs Modbus Premium : Unity v2.0

Mesures de performance

Le diagramme ci-dessous indique le nombre de requêtes de lecture de registre Modbus auxquelles les UC Premium peuvent répondre en 1 cycle de processeur. (Une requête de lecture de registre est une commande de fonction Modbus de code 3.) Le délai minimum de réponse à une requête Modbus correspond à un cycle de scrutation d'un automate. Le débit de trois automates est mesuré :

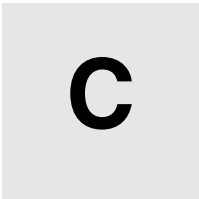
- une UC TSXP575634M équipée d'un module de communication Ethernet TSX ETY5103 ;
- une UC TSXP575634M avec un port Ethernet intégré ;
- une UC TSXP57304M équipée d'un module de communication Ethernet TSX ETY5103.



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

	P575634M (port intégré)	P575634M + ETY5103	P57304M + ETY5103
Temps de scrutation	Nombre de transactions Modbus/seconde		
10	400	400	300
20	300	400	300
50	320	400	160
100	160	200	120
200	80	100	60

Temps de réponse des clients Modbus



Vue d'ensemble

Cette annexe indique les temps de réponse des clients Modbus pour les systèmes Premium et Quantum qui utilisent un réseau Ethernet industriel.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du client Modbus : Premium TSXP575634M	448
Temps de réponse du client Modbus : Premium TSXP57304M	454
Temps de réponse du client Modbus : Quantum 140 CPU65150 avec port Ethernet intégré	461
Temps de réponse du client Modbus : Quantum 140 CPU65150 avec module de communication Ethernet 140 NOE77101	467
Temps de réponse du client Modbus : Quantum 140 CPU65150 avec module de communication Ethernet 140 NOE77111	473
Temps de réponse du client Modbus : Quantum 140 CPU43412A avec module de communication Ethernet 140 NOE77101	479
Temps de réponse du client Modbus : Quantum 140 CPU43412A avec module de communication Ethernet 140 NOE77111	485

Temps de réponse du client Modbus : Premium TSXP575634M

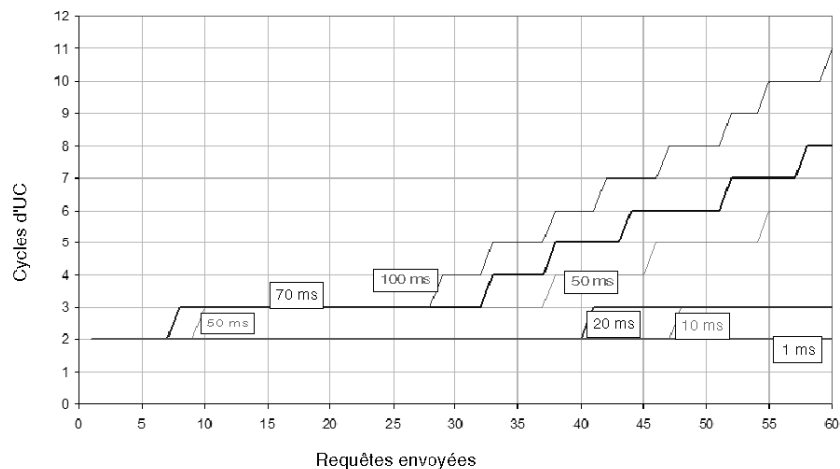
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse de l'UC Premium lorsqu'un bloc de requête client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'UC est un module Premium TSXP575634M équipé d'un module de communication Ethernet TSXETY5103 (EXEC v3.10). Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

Temps de scrutation d'UC de 200 ms

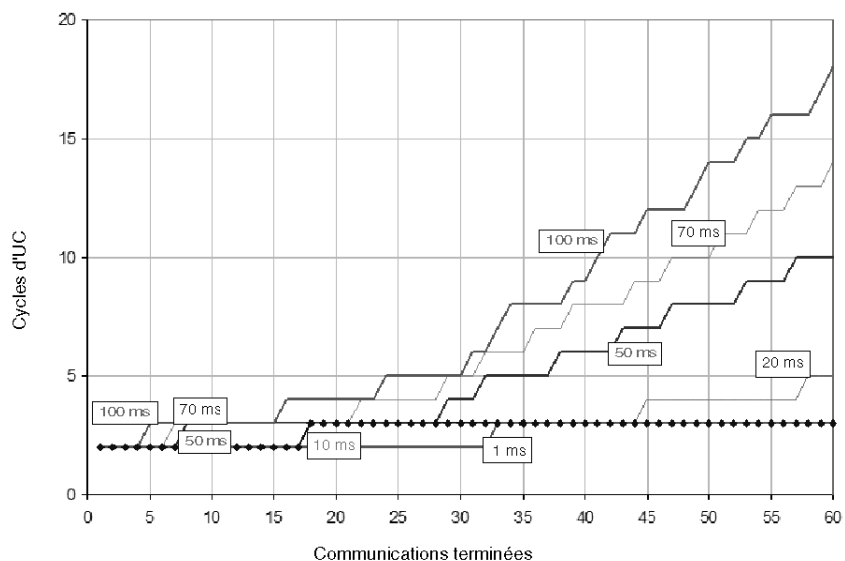


Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1 à 7	<1 à 100 ms	2 cycles
8	70 à 100 ms	3 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
10	50 ms	3 cycles
29	100 ms	4 cycles
33	70 ms	4 cycles
	100 ms	5 cycles
38	50 ms	4 cycles
	70 ms	5 cycles
	100 ms	6 cycles
41	20 ms	3 cycles
42	100 ms	7 cycles
46	50 ms	5 cycles
	70 ms	6 cycles
48	10 ms	3 cycles
55	50 ms	6 cycles
	70 ms	7 cycles
	100 ms	10 cycles
60	100 ms	11 cycles

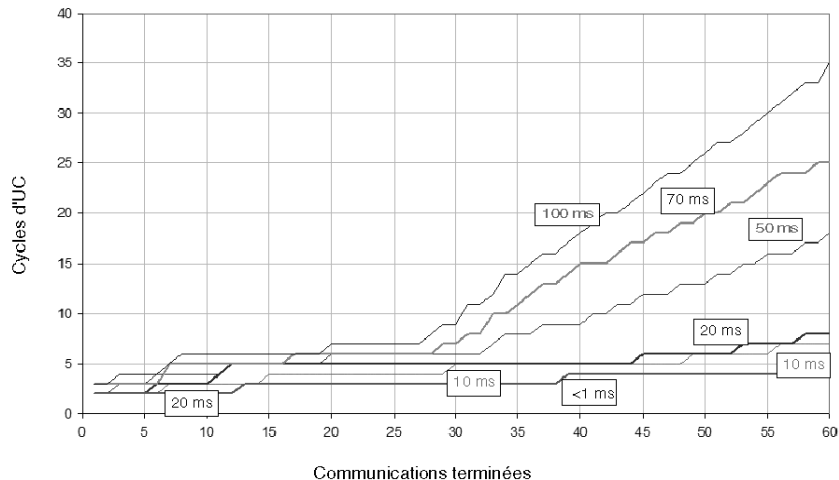
Temps de scrutation d'UC de 100 ms



Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1 à 4	<1 à 100 ms	2 cycles
5	100 ms	3 cycles
7	20 à 70 ms	3 cycles
16	100 ms	4 cycles
18	10 ms	3 cycles
22	70 ms	4 cycles
24	100 ms	5 cycles
29	50 ms	4 cycles
	70 ms	5 cycles
31	100 ms	6 cycles
33	<1 ms	3 cycles
	70 ms	6 cycles
	100 ms	7 cycles
34	100 ms	8 cycles
38	50 ms	6 cycles
39	70 ms	8 cycles
	100 ms	9 cycles
47	20 ms	4 cycles
	50 ms	8 cycles
	70 ms	10 cycles
	100 ms	12 cycles
60	20 ms	5 cycles
	50 ms	10 cycles
	70 ms	14 cycles
	100 ms	18 cycles

Temps de scrutation d'UC de 50 ms

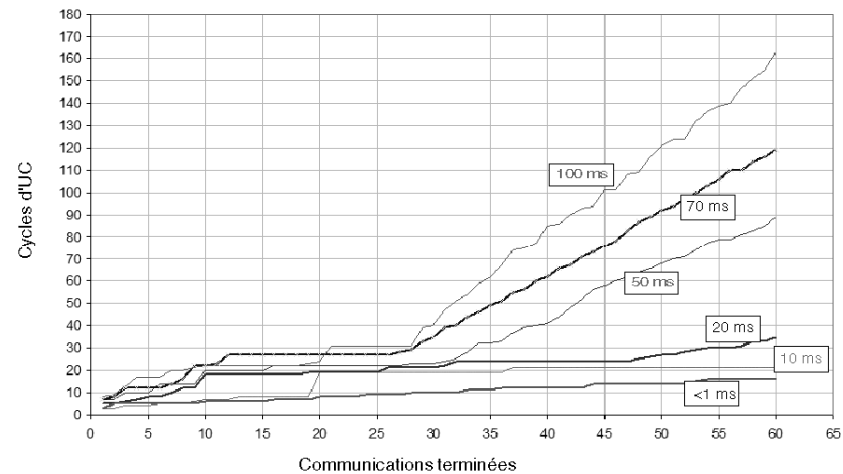


Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1 à 2	<1 à 50 ms	2 cycles
	70 à 100 ms	3 cycles
3	50 ms	3 cycles
	100 ms	4 cycles
7	10 à 20 ms	3 cycles
	50 ms	4 cycles
	70 à 100 ms	5 cycles
8	100 ms	6 cycles
15	10 ms	4 cycles
	20 à 70 ms	5 cycles
26	50 à 70 ms	6 cycles
	100 ms	7 cycles
31	70 ms	8 cycles
	100 ms	11 cycles
37	50 ms	9 cycles
	70 ms	13 cycles
	100 ms	16 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
39	<1 ms	4 cycles
	100 ms	17 cycles
50	10 à 20 ms	6 cycles
	50 ms	13 cycles
	70 ms	20 cycles
	100 ms	26 cycles
60	<1 ms	5 cycles
	10 ms	7 cycles
	20 ms	8 cycles
	50 ms	18 cycles
	70 ms	25 cycles
	100 ms	35 cycles

Temps de scrutation d'UC de 10 ms



Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1	<1 à 10 ms	3 cycles
	20 ms	5 cycles
	50 à 70 ms	7 cycles
	100 ms	8 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
3	<1 ms	5 cycles
	10 ms	4 cycles
	20 ms	6 cycles
	50 ms	10 cycles
	70 ms	12 cycles
	100 ms	13 cycles
10	<1 ms	6 cycles
	10 ms	7 cycles
	20 ms	18 cycles
	70 à 100 ms	22 ms
16	10 ms	8 cycles
	20 ms	18 cycles
	50 ms	22 cycles
	70 ms	27 cycles
	100 ms	22 cycles
21	<1 ms	8 cycles
	10 à 20 ms	19 cycles
	50 ms	22 cycles
	70 ms	27 cycles
	100 ms	31 cycles
33	<1 ms	11 cycles
	10 ms	19 cycles
	20 ms	24 cycles
	50 ms	25 cycles
	70 ms	44 cycles
	100 ms	54 cycles
39	<1 ms	4 cycles
	100 ms	17 cycles
45	<1 ms	14 cycles
	10 ms	21 cycles
	50 ms	58 cycles
	70 ms	76 cycles
	100 ms	101 cycles
60	<1 ms	16 cycles
	10 ms	21 cycles
	20 ms	35 cycles
	50 ms	89 cycles
	70 ms	119 cycles
	100 ms	163 cycles

Temps de réponse du client Modbus : Premium TSXP57304M

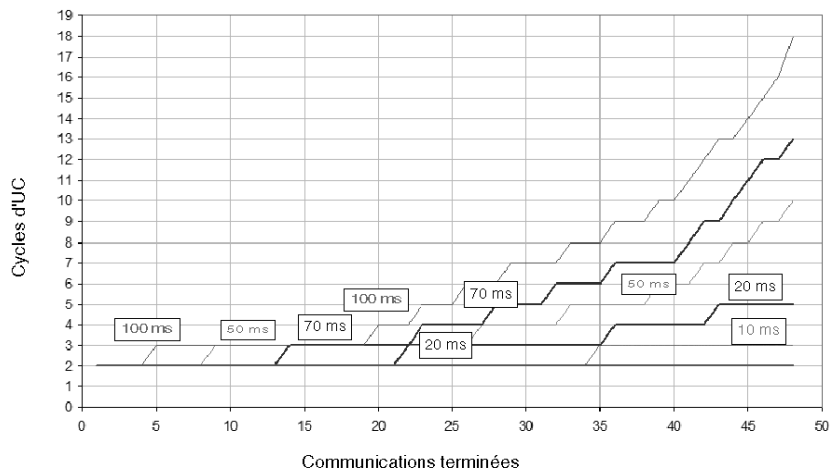
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse de l'UC Premium lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Premium TSXP57304M équipé d'un module de communication Ethernet ETY5103 (EXEC v3.10). Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

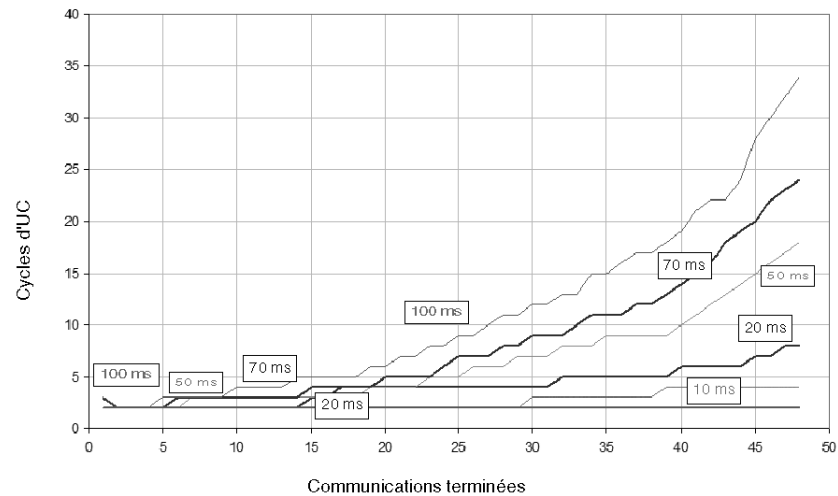
Temps de scrutation d'UC de 200 ms



Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1 à 4	<1 à 100 ms	2 cycles
5	100 ms	3 cycles
9	50 ms	3 cycles
14	70 ms	3 cycles
20	100 ms	4 cycles
23	20 ms	3 cycles
	70 ms	4 cycles
	100 ms	5 cycles
28	50 ms	4 cycles
	70 ms	5 cycles
	100 ms	6 cycles
36	10 ms	3 cycles
	20 ms	4 cycles
	50 ms	5 cycles
	70 ms	7 cycles
	100 ms	9 cycles
43	20 ms	5 cycles
	50 ms	7 cycles
	70 ms	9 cycles
	100 ms	13 cycles
48	50 ms	10 cycles
	70 ms	13 cycles
	100 ms	18 cycles

Temps de scrutation d'UC de 100 ms

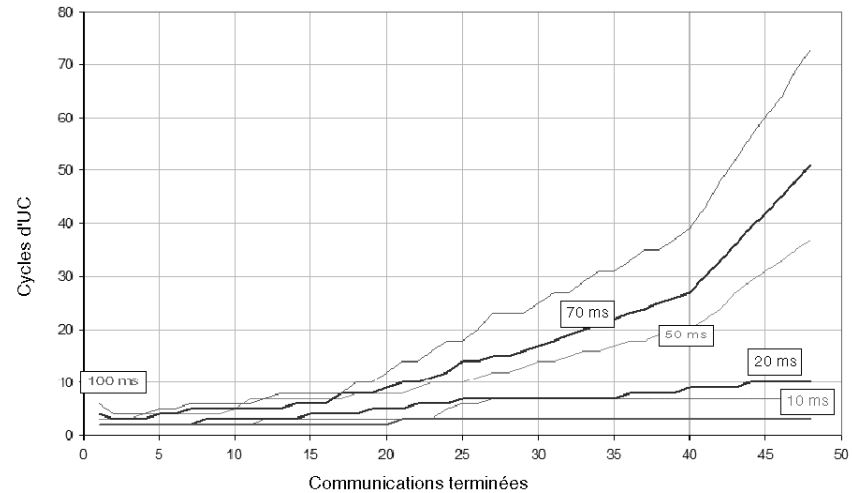


Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1	<1 à 50 ms	2 cycles
	70 à 100 ms	3 cycles
2 ... 4	<1 à 100 ms	2 cycles
5	100 ms	3 cycles
6	50 ... 70 ms	3 cycles
15	20 à 50 ms	3 cycles
	70 ms	3 cycles
	100 ms	5 cycles
18	20 ms	4 cycles
	50 ms	3 cycles
	70 ms	4 cycles
24	50 ms	5 cycles
	70 ms	3 cycles
	100 ms	5 cycles
32	10 ms	3 cycles
	20 ms	5 cycles
	50 ms	8 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
48	70 ms	9 cycles
	100 ms	13 cycles
	10 ms	4 cycles
	20 ms	8 cycles
	50 ms	18 cycles
	70 ms	24 cycles
	100 ms	34 cycles

Temps de scrutation d'UC de 50 ms

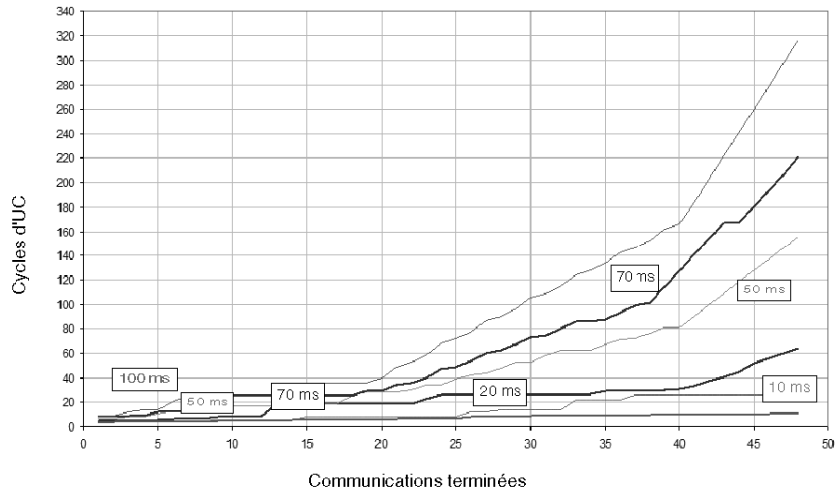


Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1	<1 à 20 ms	2 cycles
	50 ms	3 cycles
	70 ms	4 cycles
	100 ms	6 cycles
2	70 ms	3 cycles
	100 ms	4 cycles
4	50 ms	4 cycles
8	20 ms	3 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
	70 ms	5 cycles
	100 ms	6 cycles
15	10 ms	3 cycles
	20 ms	4 cycles
	50 ms	7 cycles
	70 ms	6 cycles
	100 ms	8 cycles
22	<1 ms	3 cycles
	20 ms	6 cycles
	50 ms	9 cycles
	70 ms	10 cycles
	100 ms	14 cycles
35	10 à 20 ms	7 cycles
	50 ms	17 cycles
	70 ms	22 cycles
	100 ms	31 cycles
48	20 ms	10 cycles
	50 ms	37 cycles
	70 ms	51 cycles
	100 ms	73 cycles

Temps de scrutation d'UC de 10 ms



Voici un échantillon des résultats représentés dans le graphique :

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
1	<1 à 10 ms	2 cycles
	20 ms	4 cycles
	50 ms	5 cycles
	70 ms	3 cycles
	100 ms	5 cycles
2	10 ms	3 cycles
3	<1 ms	3 cycles
	70 ms	4 cycles
	100 ms	6 cycles
11	<1 ms	4 cycles
	10 ms	5 cycles
	20 ms	6 cycles
	50 ms	15 cycles
	70 ms	12 cycles
18	100 ms	22 cycles
	<1 ms	5 cycles
	10 ms	6 cycles
	20 ms	13 cycles

Nombre de requêtes	Temps de réponse du serveur	Nombre de cycles d'UC requis
	50 ms	16 cycles
	70 ms	22 cycles
	100 ms	28 cycles
22	<1 ms	6 cycles
	10 ms	7 cycles
	20 ms	18 cycles
	50 ms	27 cycles
	70 ms	35 cycles
	100 ms	50 cycles
39	<1 ms	9 cycles
	10 ms	12 cycles
	20 ms	33 cycles
	50 ms	81 cycles
	70 ms	109 cycles
	100 ms	159 cycles
48	<1 ms	10 cycles
	20 ms	16 cycles
	20 ms	64 cycles
	50 ms	159 cycles
	70 ms	220 cycles
	100 ms	314 cycles

Temps de réponse du client Modbus : Quantum 140 CPU65150 avec port Ethernet intégré

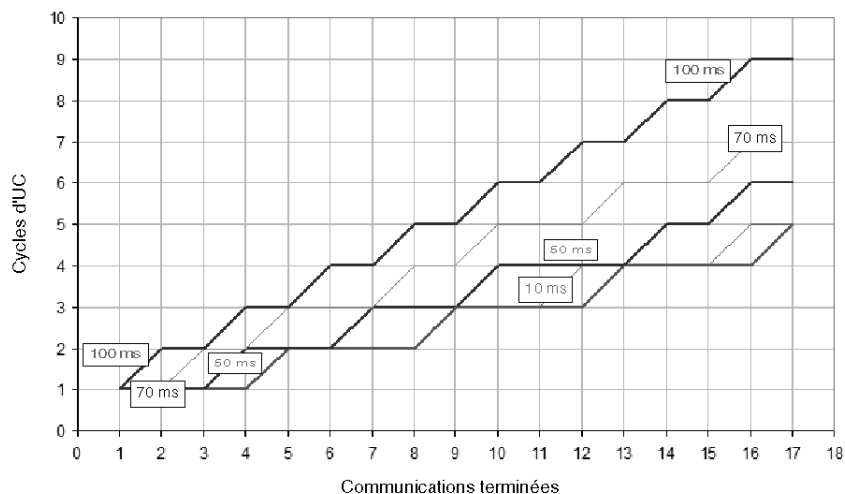
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse de l'automate Quantum lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Quantum 140 CPU65150 équipé d'un port Ethernet intégré. Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

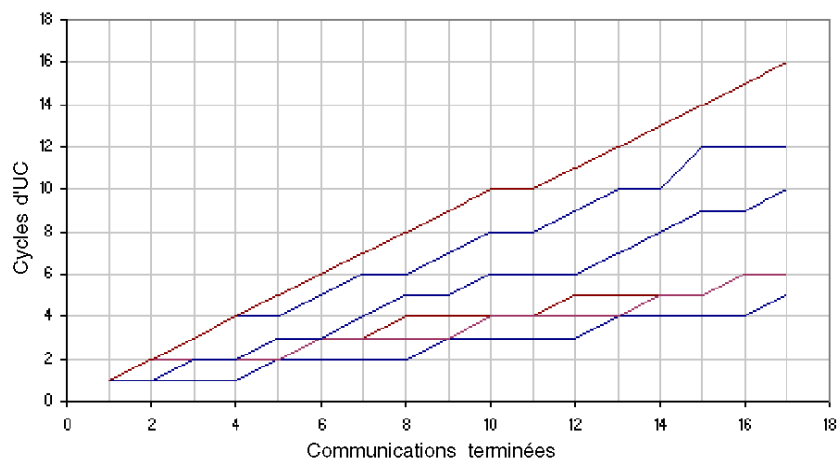
Temps de scrutation d'UC de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
200	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	2
3	1	1	1	1	2	2
4	1	1	1	2	2	3
5	2	2	2	2	3	3
6	2	2	2	2	3	4
7	2	2	2	3	3	4
8	2	2	2	3	4	5
9	3	3	3	3	4	5
10	3	3	3	4	5	6
11	3	3	3	4	5	6
12	3	4	3	4	5	7
13	4	4	4	4	6	7
14	4	4	4	5	6	8
15	4	4	4	5	6	8
16	4	5	4	6	7	9
17	5	5	5	6	7	9

Temps de scrutation d'UC de 100 ms

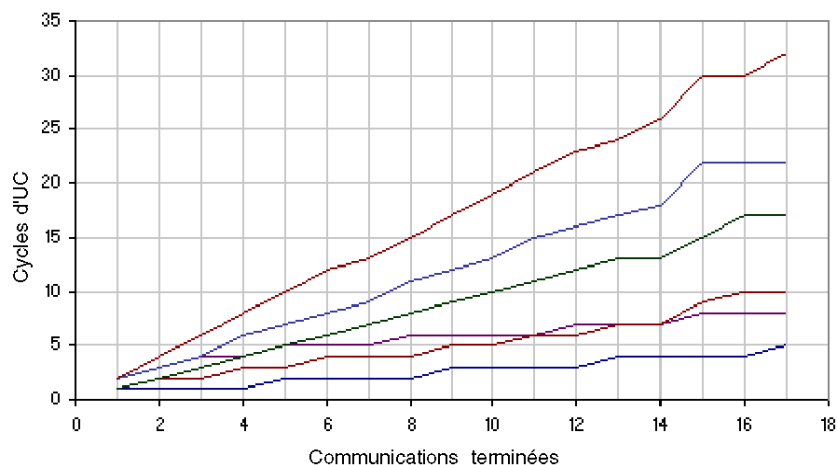


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	2	2	1	2	2
3	1	2	2	2	3	3
4	1	2	2	2	4	4
5	2	2	2	3	4	5
6	2	3	3	3	5	6
7	2	3	3	4	6	7
8	2	4	3	5	6	8
9	3	4	3	5	7	9
10	3	4	4	6	8	10
11	3	4	4	6	8	10
12	3	5	4	6	9	11
13	4	5	4	7	10	12
14	4	5	5	8	10	13
15	4	5	5	9	12	14

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
100	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
16	4	6	6	9	12	15
17	5	6	6	10	12	16

Temps de scrutation d'UC de 50 ms

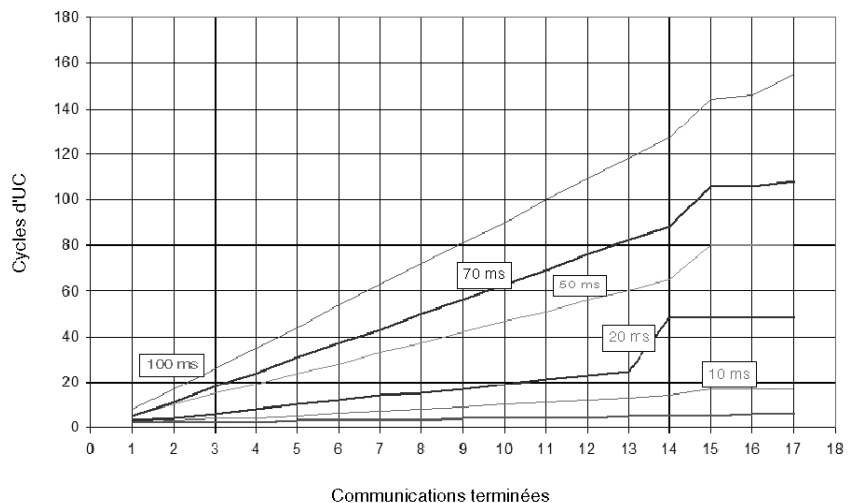


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	2	1	1	2	2
2	1	3	2	2	3	4
3	1	4	2	3	4	6
4	1	4	3	4	6	8
5	2	5	3	5	7	10
6	2	5	4	6	8	12
7	2	5	4	7	9	13
8	2	6	4	8	11	15
9	3	6	5	9	12	17
10	3	6	5	10	13	19

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
11	3	6	6	11	15	21
12	3	7	6	12	16	23
13	4	7	7	13	17	24
14	4	7	7	13	18	26
15	4	8	9	15	22	30
16	4	8	10	17	22	30
17	5	8	10	17	22	32

Temps de scrutation d'UC de 10 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	2	2	3	5	5	8
2	2	3	4	10	11	17
3	2	4	6	15	18	26
4	2	4	8	19	24	35
5	3	5	10	24	31	44
6	3	6	12	28	37	54
7	3	7	14	33	43	63
8	3	8	15	37	50	72
9	4	9	17	42	56	81
10	4	10	19	47	63	90
11	4	11	21	51	69	100
12	4	12	23	56	76	109
13	5	13	25	60	82	118
14	5	14	48	65	88	127
15	5	17	48	80	106	144
16	6	17	48	80	106	146
17	6	17	48	80	108	155

Temps de réponse du client Modbus : Quantum 140 CPU65150 avec module de communication Ethernet 140 NOE77101

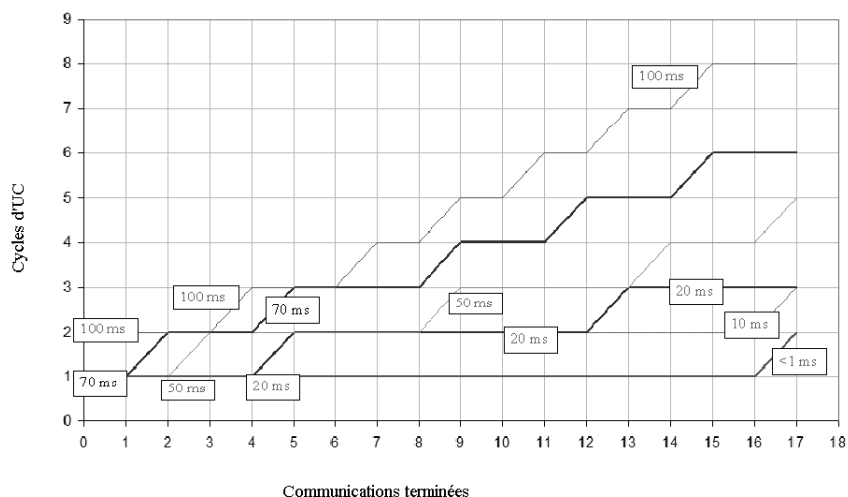
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse de l'automate Quantum lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Quantum 140 CPU65150 équipé d'un module de communication Ethernet 140 NOE77101. Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

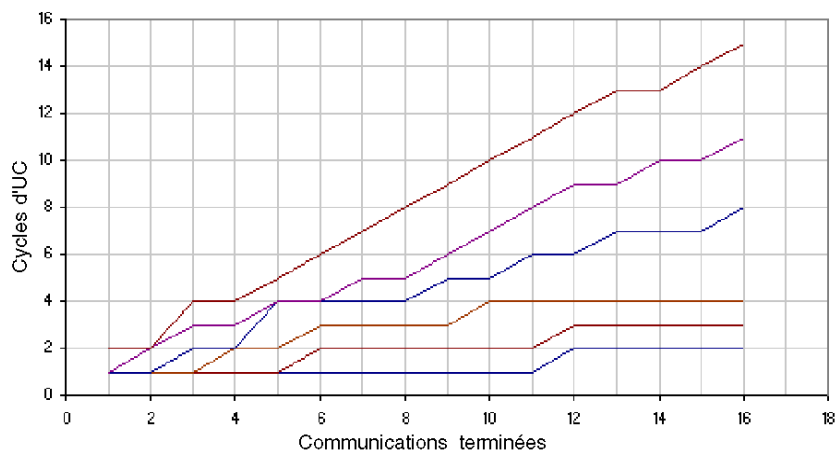
Temps de scrutation d'UC de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
200	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	2
2	1	1	1	1	2	2
3	1	1	1	2	2	2
4	1	1	1	2	2	3
5	1	2	2	2	3	3
6	1	2	2	2	3	3
7	1	2	2	2	3	4
8	1	2	2	2	3	4
9	1	2	2	3	4	5
10	1	2	2	3	4	5
11	1	2	2	3	4	6
12	1	2	2	3	5	6
13	1	2	3	3	5	7
14	1	2	3	4	5	7
15	1	2	3	4	6	8
16	1	2	3	4	6	8
17	2	3	3	5	6	8

Temps de scrutation d'UC de 100 ms

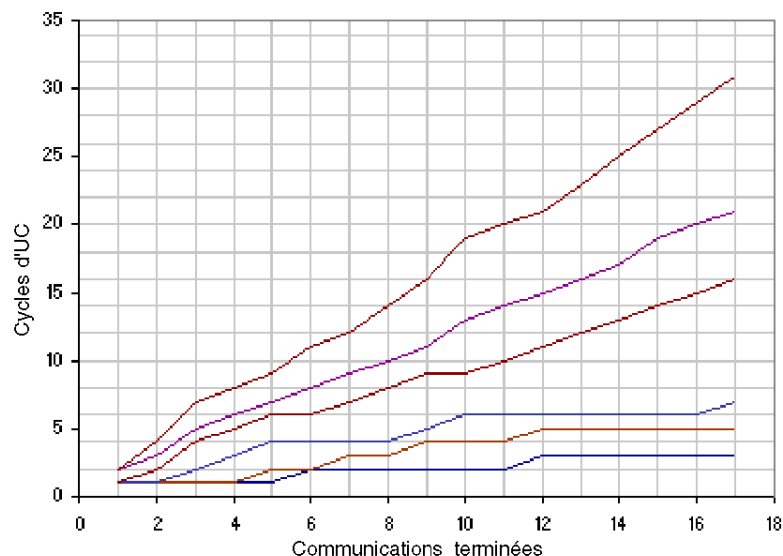


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	2
2	1	1	1	1	2	2
3	1	1	1	2	3	4
4	1	1	2	2	3	4
5	1	1	2	4	4	5
6	1	2	3	4	4	6
7	1	2	3	4	5	7
8	1	2	3	4	5	8
9	1	2	3	5	6	9
10	1	2	4	5	7	10
11	1	2	4	6	8	11
12	2	3	4	6	9	12
13	2	3	4	7	9	13
14	2	3	4	7	10	13
15	2	3	4	7	10	14

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
100	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
16	2	3	4	8	11	15
17	2	3	4	8	11	16

Temps de scrutation d'UC de 50 ms

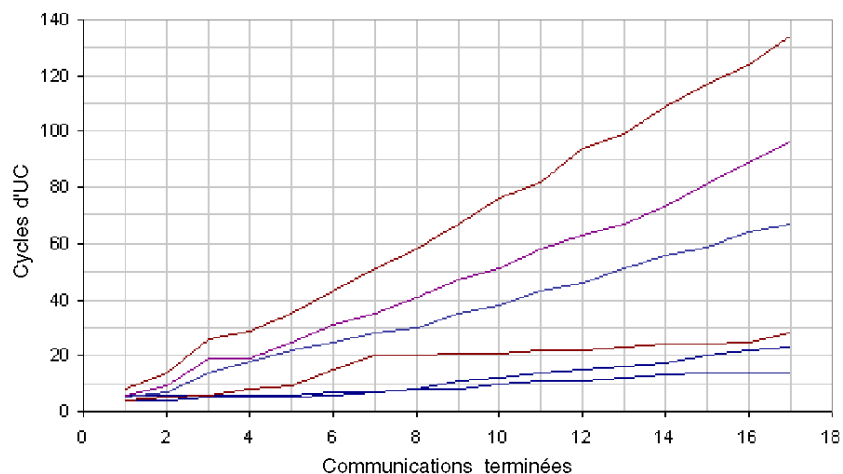


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	2	2
2	1	1	1	2	3	4
3	1	1	2	4	5	7
4	1	1	3	5	6	8
5	1	2	4	6	7	9
6	2	2	4	6	8	11
7	2	3	4	7	9	12

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
8	2	3	4	8	10	14
9	2	4	5	9	11	16
10	2	4	6	9	13	19
11	2	4	6	10	14	20
12	3	5	6	11	15	21
13	3	5	6	12	16	23
14	3	5	6	13	17	25
15	3	5	6	14	19	27
16	3	5	6	15	20	29
17	3	5	7	16	21	31

Temps de scrutation d'UC de 10 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	6	4	4	5	6	8
2	6	4	5	7	9	14
3	6	5	6	14	19	26
4	6	5	8	18	19	29
5	6	5	9	22	25	35
6	7	6	15	25	31	43
7	7	7	20	28	35	51
8	8	8	20	30	41	58
9	8	11	21	35	47	67
10	10	12	21	38	51	76
11	11	14	22	43	58	82
12	11	15	22	46	63	94
13	12	16	23	51	67	99
14	13	17	24	56	73	109
15	14	20	24	59	81	117
16	14	22	25	64	89	124
17	14	23	28	67	96	134

Temps de réponse du client Modbus : Quantum 140 CPU65150 avec module de communication Ethernet 140 NOE77111

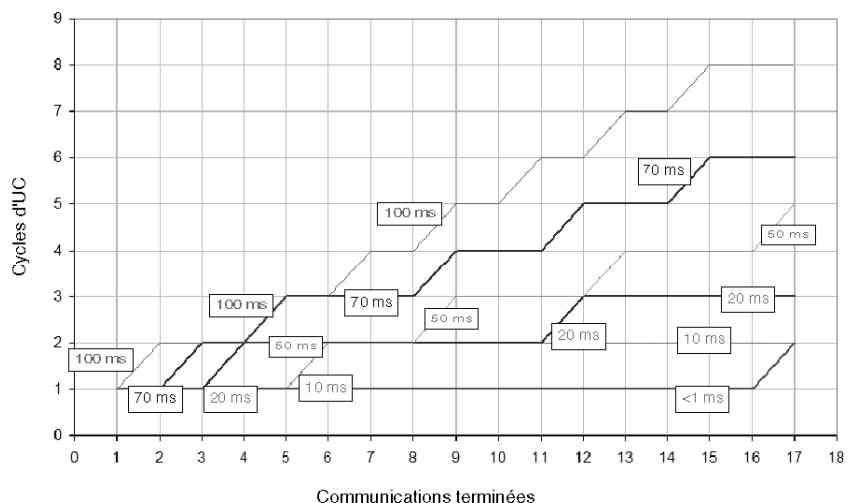
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse de l'automate Quantum lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Quantum 140 CPU65150 équipé d'un module de communication Ethernet 140 NOE77111. Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

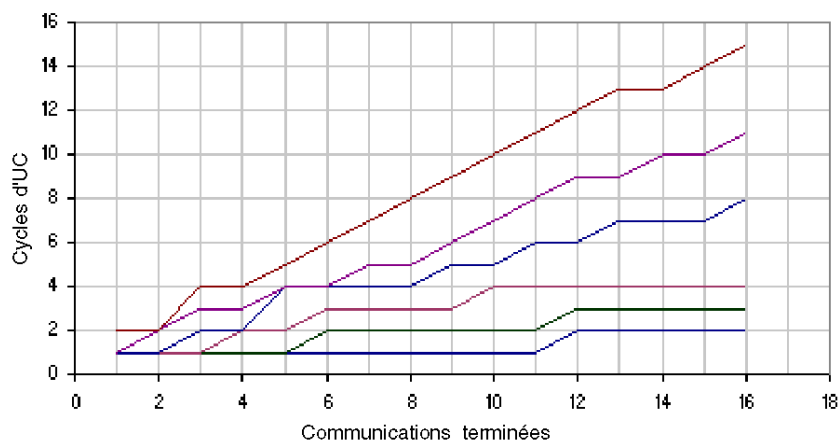
Temps de scrutation d'UC de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
200	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	2
3	1	1	1	2	2	2
4	1	1	2	2	2	2
5	1	1	2	2	3	3
6	1	2	2	2	3	3
7	1	2	2	2	3	4
8	1	2	2	2	3	4
9	1	2	2	3	4	5
10	1	2	2	3	4	5
11	1	2	2	3	4	6
12	1	2	3	3	5	6
13	1	2	3	4	5	7
14	1	2	3	4	5	7
15	1	2	3	4	6	8
16	1	2	3	4	6	8
17	2	2	3	5	6	8

Temps de scrutation d'UC de 100 ms

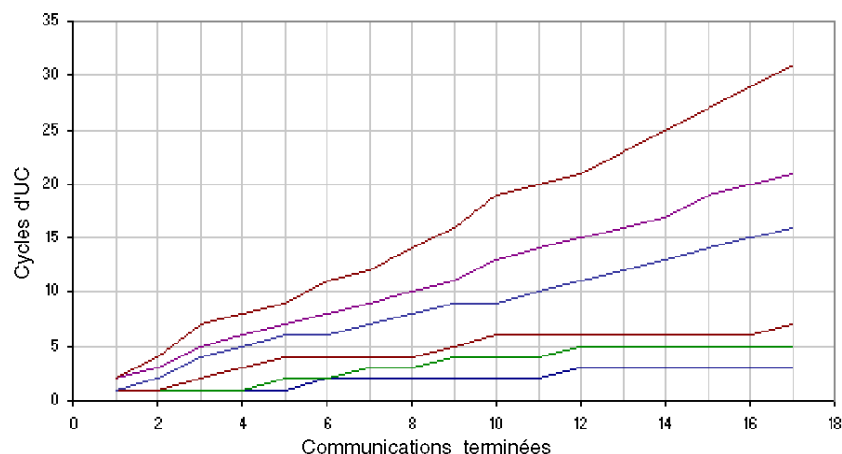


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	2
2	1	1	1	1	2	2
3	1	1	1	2	3	4
4	1	1	2	4	3	4
5	1	1	2	4	4	5
6	1	2	3	4	4	6
7	1	2	3	4	5	7
8	1	2	4	4	6	8
9	1	2	4	5	6	9
10	1	2	4	5	7	10
11	2	3	4	6	8	11
12	2	3	4	6	8	12
13	2	3	4	7	9	13
14	2	3	4	7	10	13
15	2	3	4	7	10	14

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
100	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
16	2	3	4	8	11	15
17	2	3	4	8	12	16

Temps de scrutation d'UC de 50 ms

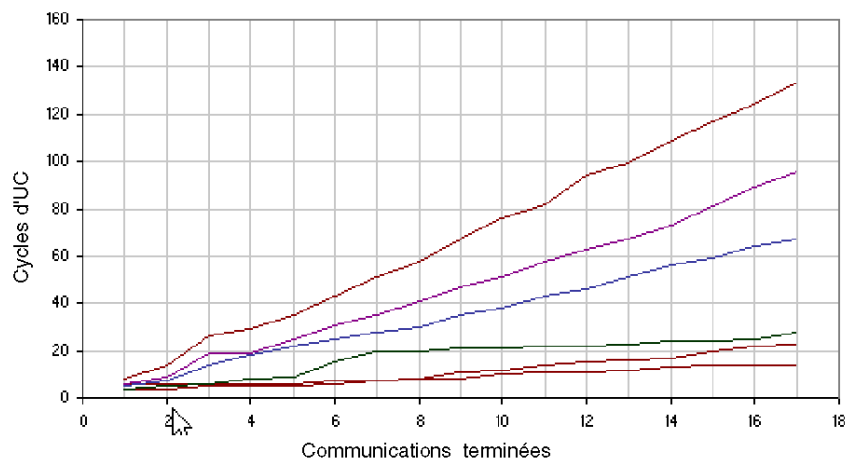


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	2	2
2	1	1	1	2	3	4
3	1	1	2	4	6	7
4	2	2	3	5	6	7
5	2	2	4	5	7	9
6	2	2	4	6	8	11
7	2	3	4	7	9	13
8	2	3	5	8	10	14
9	2	3	5	8	11	16
10	2	4	6	9	13	19

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
11	3	4	6	10	14	20
12	3	4	6	11	15	21
13	3	5	6	12	16	23
14	3	5	6	13	18	25
15	3	5	6	14	19	27
16	3	5	6	15	20	29
17	3	5	7	16	22	31

Temps de scrutation d'UC de 10 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	6	4	4	5	5	8
2	6	5	5	8	10	15
3	7	5	6	16	18	28
4	7	5	6	18	19	29
5	7	6	7	21	25	36

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
6	7	6	19	26	30	43
7	7	7	21	28	35	51
8	7	7	21	30	41	58
9	8	12	21	34	46	66
10	9	12	21	38	51	74
11	9	14	22	42	57	82
12	10	14	22	46	63	91
13	11	16	23	50	69	99
14	12	17	24	55	75	108
15	13	19	24	59	81	117
16	13	22	26	64	88	126
17	14	23	28	68	95	136

Temps de réponse du client Modbus : Quantum 140 CPU43412A avec module de communication Ethernet 140 NOE77101

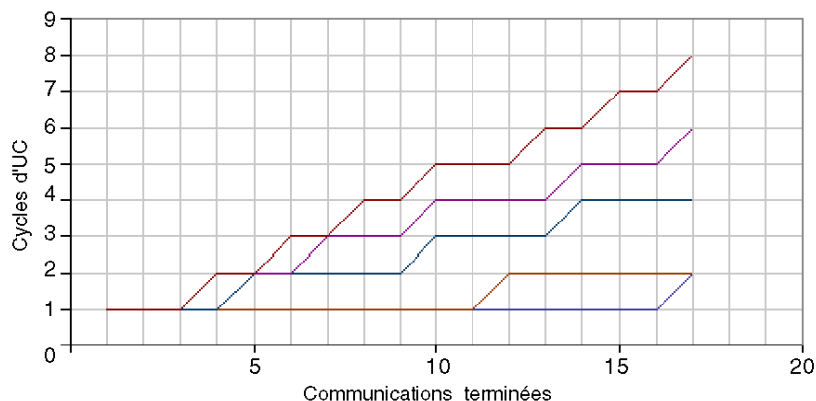
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse du client Modbus lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Quantum 140 CPU43412A équipé d'un module de communication Ethernet 140 NOE77101. Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

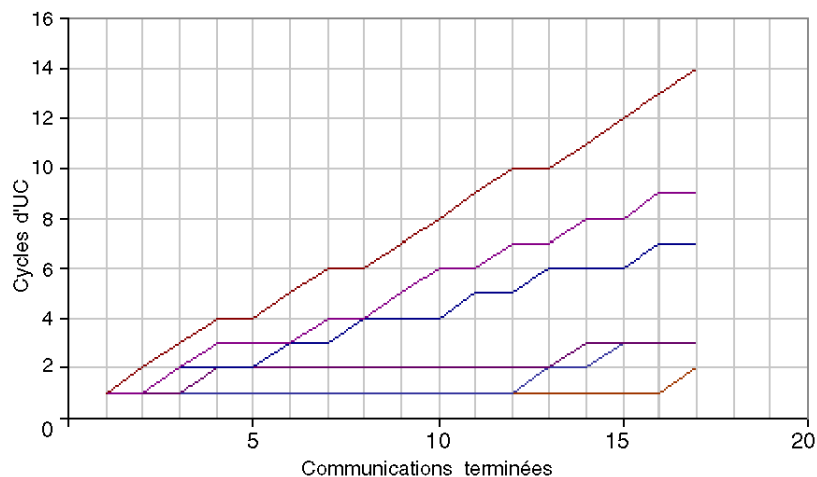
Temps de scrutation d'UC de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
200	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4	1	1	1	1	2	2
5	1	1	1	2	2	2
6	1	1	1	2	2	3
7	1	1	1	2	3	3
8	1	1	1	2	3	4
9	1	1	1	2	3	4
10	1	1	1	3	4	5
11	1	1	1	3	4	5
12	1	1	2	3	4	5
13	1	1	2	3	4	6
14	1	1	2	4	5	6
15	1	1	2	4	5	7
16	1	1	2	4	5	7
17	2	2	2	4	6	8

Temps de scrutation d'UC de 100 ms

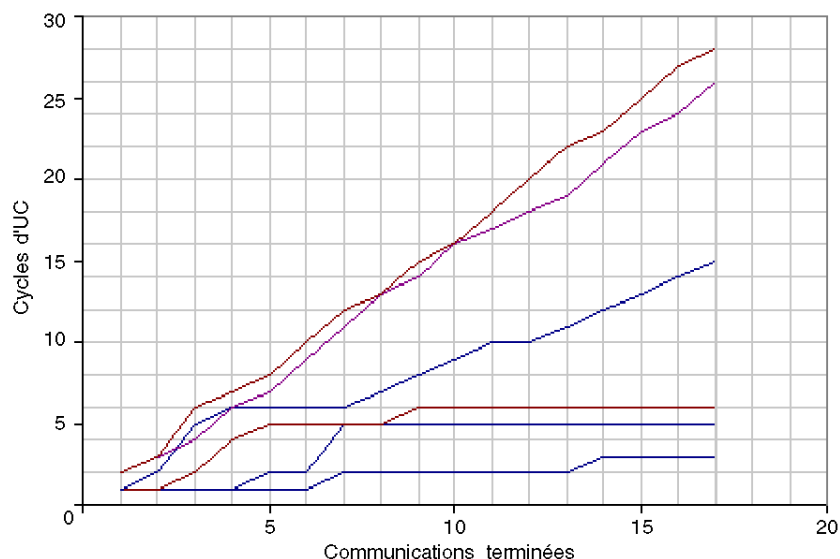


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	2
3	1	1	1	2	2	3
4	1	1	2	2	3	4
5	1	1	2	2	3	4
6	1	1	2	3	3	5
7	1	1	2	3	4	6
8	1	1	2	4	4	6
9	1	1	2	4	5	7
10	1	1	2	4	6	8
11	1	1	2	5	6	9
12	1	1	2	5	7	10
13	1	2	2	6	7	10
14	1	2	3	6	8	11
15	1	3	3	6	8	12

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
100	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
16	1	3	3	7	9	13
17	2	3	3	7	9	14

Temps de scrutation d'UC de 50 ms

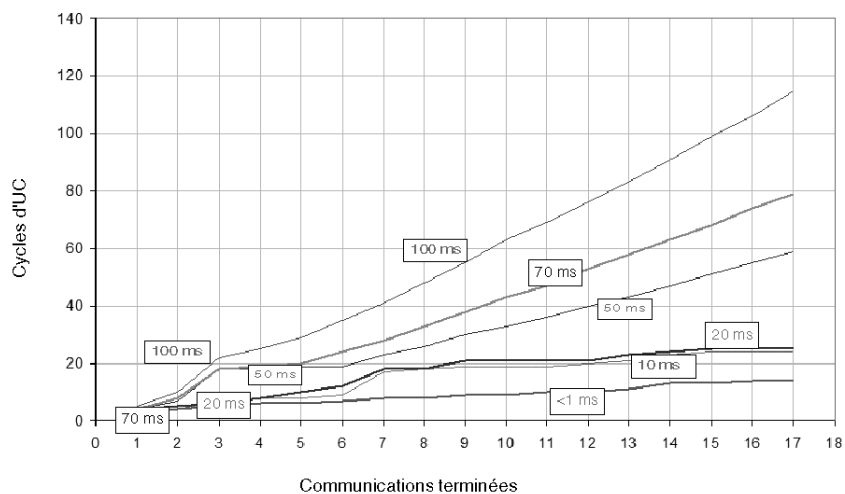


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	2	2
2	1	1	1	2	3	3
3	1	1	2	5	4	6
4	1	1	4	6	6	7
5	1	2	5	6	7	8
6	1	2	5	6	9	10
7	2	5	5	6	11	12

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
8	2	5	5	7	13	13
9	2	5	6	8	14	15
10	2	5	6	9	16	16
11	2	5	6	10	17	18
12	2	5	6	10	18	20
13	2	5	6	11	19	22
14	3	5	6	12	21	23
15	3	5	6	13	23	25
16	3	5	6	14	24	27
17	3	5	6	15	26	28

Temps de scrutation d'UC de 10 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	3	4	4	4	4	5
2	4	4	5	7	8	10
3	5	7	6	18	18	22
4	6	8	8	18	19	25
5	6	8	10	19	20	29
6	7	9	12	19	24	35
7	8	17	18	23	28	41
8	8	18	18	26	33	48
9	9	19	21	30	38	55
10	9	19	21	33	43	63
11	10	19	21	36	47	69
12	10	20	21	40	53	76
13	11	21	23	43	58	83
14	13	23	24	47	63	91
15	13	24	25	51	68	99
16	14	24	25	55	74	106
17	14	24	25	59	79	115

Temps de réponse du client Modbus : Quantum 140 CPU43412A avec module de communication Ethernet 140 NOE77111

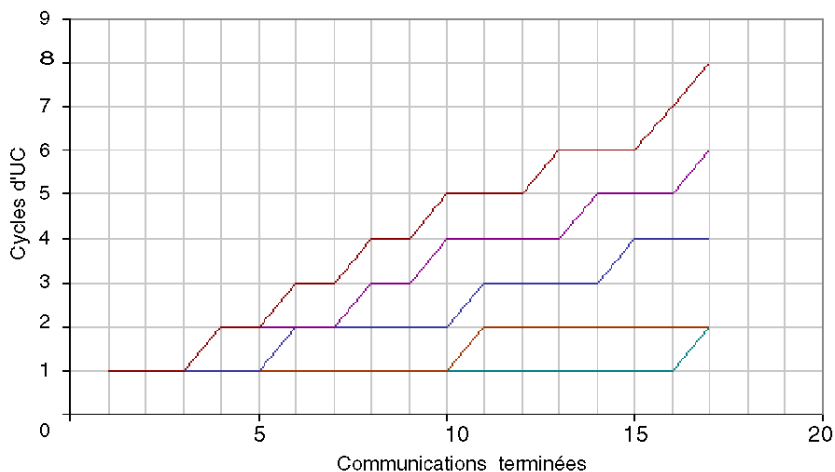
Configuration du test

Les graphiques ci-dessous indiquent les temps de réponse du client Modbus lorsque le bloc de requête du client est déclenché dans la logique de l'automate par la lecture de données sur un serveur Modbus. Ces graphiques représentent le nombre de cycles d'UC nécessaires à l'automate pour traiter toutes les demandes de client Modbus déclenchées. Dans tous les cas, l'automate est un Quantum 140 CPU43412A équipé d'un module de communication Ethernet 140 NOE77111. Les temps de scrutation de la logique de l'UC varient.

Les temps de réponse du client Modbus sont analysés par rapport à six temps de réponse du serveur Modbus :

- < 1 ms
- 10 ms
- 20 ms
- 50 ms
- 70 ms
- 100 ms

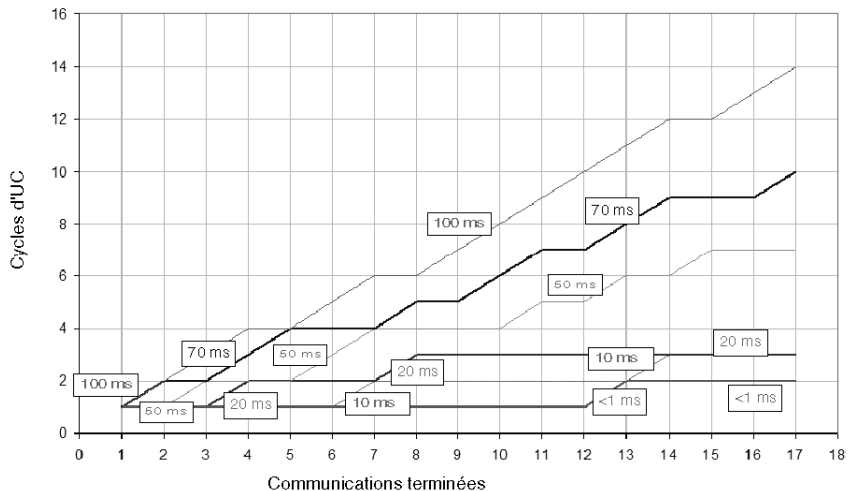
Temps de scrutation d'UC de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
200	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4	1	1	1	1	2	2
5	1	1	1	1	2	2
6	1	1	1	2	2	3
7	1	1	1	2	2	3
8	1	1	1	2	3	4
9	1	1	1	2	3	4
10	1	1	1	2	4	5
11	1	1	2	3	4	5
12	1	1	2	3	4	5
13	1	1	2	3	4	6
14	1	1	2	3	5	6
15	1	1	2	4	5	6
16	1	1	2	4	5	7
17	2	2	2	4	6	8

Temps de scrutation d'UC de 100 ms

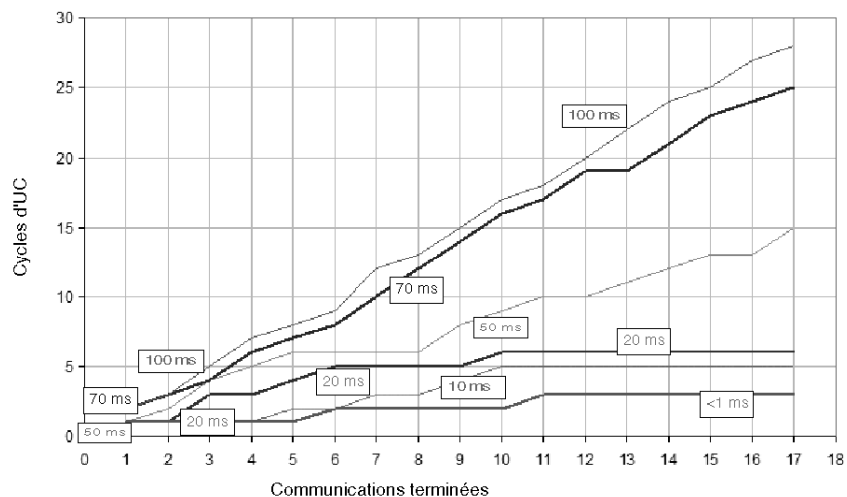


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
	<1	10	20	50	70	100
100						
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	1	1
2	1	1	1	1	1	2
3	1	1	1	1	2	3
4	1	1	1	2	2	3
5	1	1	1	2	3	4
6	1	1	2	3	3	5
7	1	1	2	3	4	6
8	1	1	2	3	4	6
9	1	1	2	4	5	7
10	1	1	2	4	6	8
11	1	1	2	4	6	9
12	1	2	2	5	7	9
13	1	2	2	6	7	10
14	1	2	2	6	8	11
15	1	3	3	6	9	12

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
100	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
16	1	3	3	6	9	13
17	2	3	3	7	9	14

Temps de scrutation d'UC de 50 ms

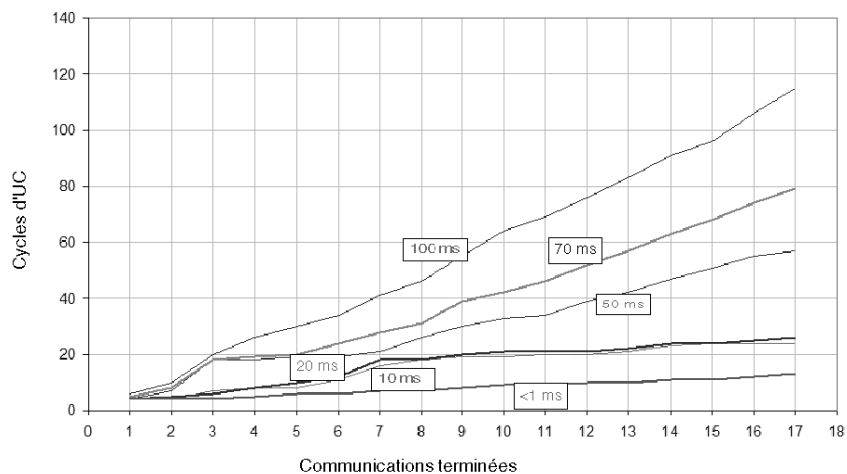


Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	1	1	1	1	2	2
2	1	1	1	2	3	3
3	1	1	3	4	4	5
4	1	1	3	5	6	7
5	1	2	4	6	7	8
6	2	2	5	6	8	9
7	2	3	5	6	10	12
8	2	3	5	6	12	13

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
50	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
9	2	4	5	8	14	15
10	2	5	6	9	16	17
11	3	5	6	10	17	18
12	3	5	6	10	19	20
13	3	5	6	11	19	22
14	3	5	6	12	21	24
15	3	5	6	13	23	25
16	3	5	6	13	24	27
17	3	5	6	15	25	28

Temps de scrutation d'UC de 10 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Scrutation de l'automate (ms)	Temps de réponse du serveur (ms)					
10	<1	10	20	50	70	100
Requêtes envoyées	Cycles d'automate avant réception de la réponse					
1	4	4	4	4	5	6
2	4	4	5	7	8	10
3	4	7	6	18	18	20
4	5	8	8	18	19	26
5	6	8	10	19	20	30
6	6	11	12	19	24	34
7	7	16	18	21	28	41
8	7	18	18	26	31	46
9	8	19	20	30	39	55
10	9	19	21	33	42	64
11	9	20	21	34	46	69
12	10	20	21	39	52	76
13	10	21	22	42	57	83
14	11	23	24	47	63	91
15	11	24	24	51	68	96
16	12	24	25	55	74	106
17	13	24	26	57	79	115

Mesures du timeout et du temps de réponse de la passerelle

D

Vue d'ensemble

Cette annexe illustre certaines mesures de performances pour les équipements avec divers temps de réponse lorsqu'ils communiquent sur un réseau via une passerelle série EGX200, EGX400 ou 174CEV30020. Des mesures distinctes sont données pour les équipements qui communiquent correctement, et pour ces mêmes équipements dans le cas d'un simple échec de requête.

Contenu de ce chapitre

Ce chapitre contient les sous-chapitres suivants :

Sous-chapitre	Sujet	Page
D.1	Mesures du timeout et du temps de réponse du serveur série de passerelles EGX200	492
D.2	Mesures du timeout et du temps de réponse du serveur série de passerelles EGX400	503
D.3	Mesures du timeout et du temps de réponse du serveur série de passerelles 174CEV30020	514

D.1 Mesures du timeout et du temps de réponse du serveur série de passerelles EGX200

Vue d'ensemble

Les performances des équipements série avec des temps de réponse de 50 ms, 100 ms, 200 ms et 500 ms sont mesurées dans le cadre d'une communication réseau via une passerelle Modbus vers Ethernet EGX200. Ces mesures sont prises à des débits réseau de 9 600 et 19 200 bauds. En outre, ces mesures sont prises dans le cas de communications établies avec succès, mais également dans le cas d'un simple échec de requête suivi d'une tentative de rétablissement de communication réussie.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du serveur série EGX200	493
Mesures des réponses du serveur série EGX200 avec timeout de la requête	498

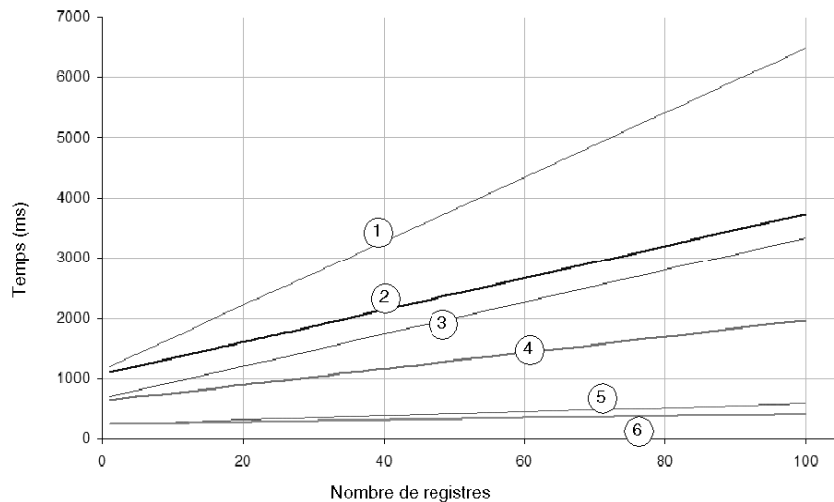
Temps de réponse du serveur série EGX200

Configuration du test

Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle EGX200 côté série. Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur la quantité de données (c.-à-d., le nombre de registres) requise. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

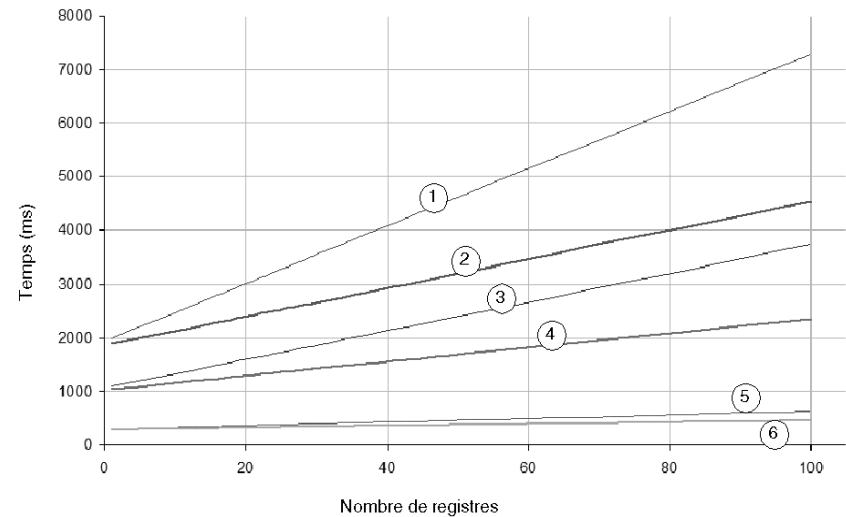
Equipements série avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Équipement	Temps de réponse du serveur série = 50						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	250.8333333	694.1666667	1200.833333	244.1666667	640.8333333	1094.166667	
16	300.8333333	1094.166667	2000.833333	269.1666667	840.8333333	1494.166667	
32	354.1666667	1520.833333	2854.166667	295.8333333	1054.1666667	1920.833333	
64	460.8333333	2374.166667	4560.833333	349.1666667	1480.833333	2774.166667	
100	580.8333333	3334.166667	6480.833333	409.1666667	1960.833333	3734.166667	187.5

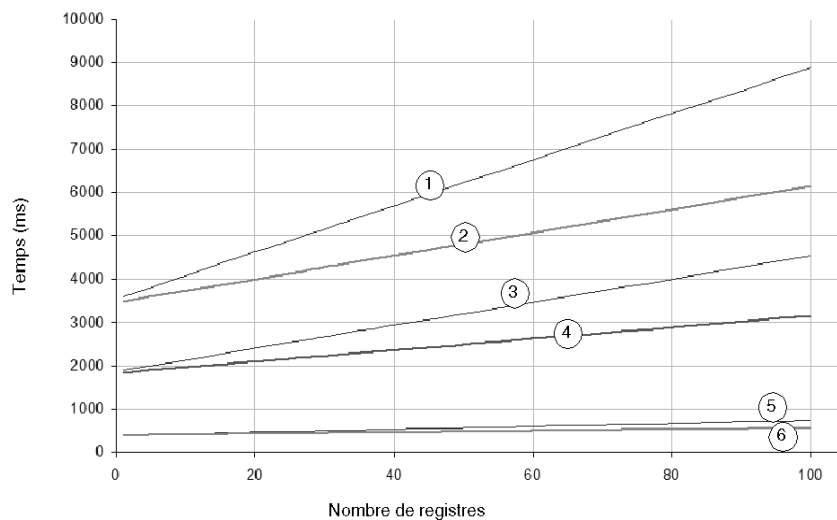
Equipements série avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	300.8333333	1094.166667	2000.833333	294.1666667	1040.833333	1894.166667	
16	350.8333333	1494.166667	2800.833333	319.1666667	1240.833333	2294.166667	
32	404.1666667	1920.833333	3654.166667	345.8333333	1454.166667	2720.833333	
64	510.8333333	2774.166667	5360.833333	399.166667	1880.833333	3574.166667	
100	630.8333333	3734.166667	7280.833333	459.166667	2360.833333	4534.166667	187.5

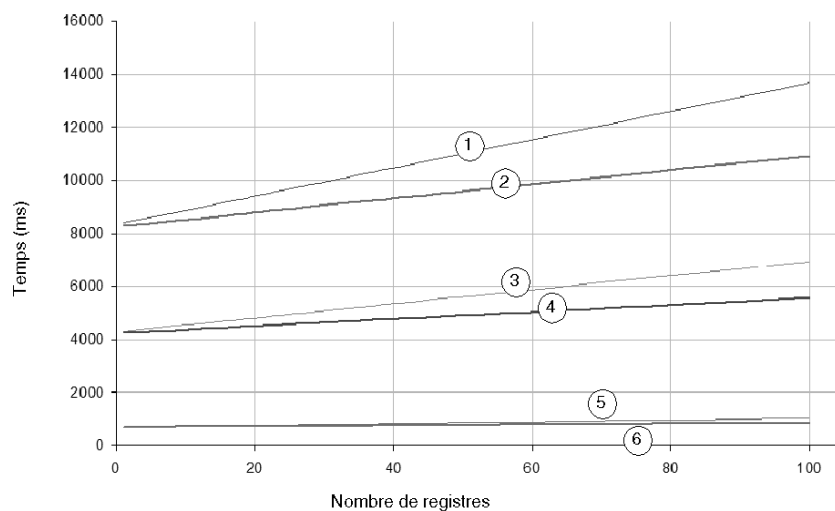
Equipements série avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	400.8333333	1894.166667	3600.833333	394.1666667	1840.833333	3494.166667	
16	450.8333333	2294.166667	4400.833333	419.1666667	2040.833333	3894.166667	
32	504.1666667	2720.833333	5254.166667	445.8333333	2254.166667	4320.833333	
64	610.8333333	3574.166667	6960.833333	499.1666667	2680.833333	5174.166667	
100	730.8333333	4534.166667	8880.833333	559.1666667	3160.833333	6134.166667	187.5

Equipements série avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 500						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	700.8333333	4294.16667	8400.833333	694.1666667	4240.833333	8294.166667	
16	750.8333333	4694.16667	9200.833333	719.1666667	4440.833333	8694.166667	
32	804.1666667	5120.83333	10054.16667	745.8333333	4654.166667	9120.833333	
64	910.8333333	5974.16667	11760.83333	799.1666667	5080.833333	9974.166667	
100	1030.833333	6934.16667	13680.83333	859.1666667	5560.833333	10934.16667	

Mesures des réponses du serveur série EGX200 avec timeout de la requête

Configuration du test

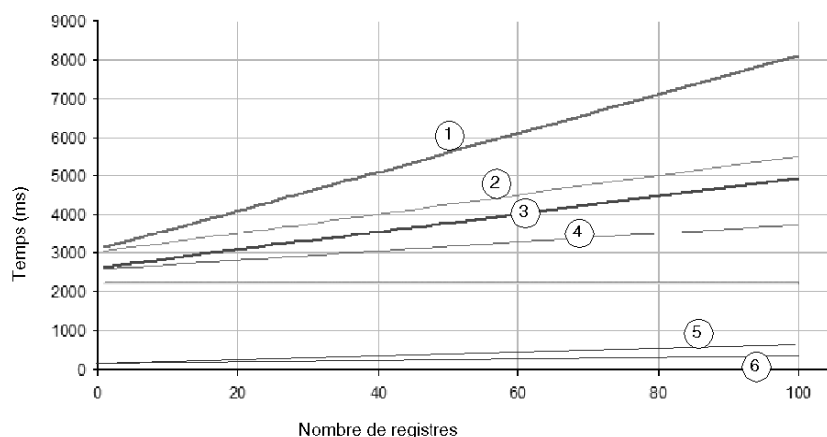
Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle EGX200 côté série, en cas d'erreur d'une requête de communication (par exemple, un équipement série déconnecté). Cet échec entraîne un timeout de 1 000 ms sur la requête initiale suivi par une nouvelle tentative de la requête.

NOTE : Un échec de requête augmente les temps de réponse pour toutes les requêtes.

Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur une quantité de données (c.-à-d., le nombre de registres) requise. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

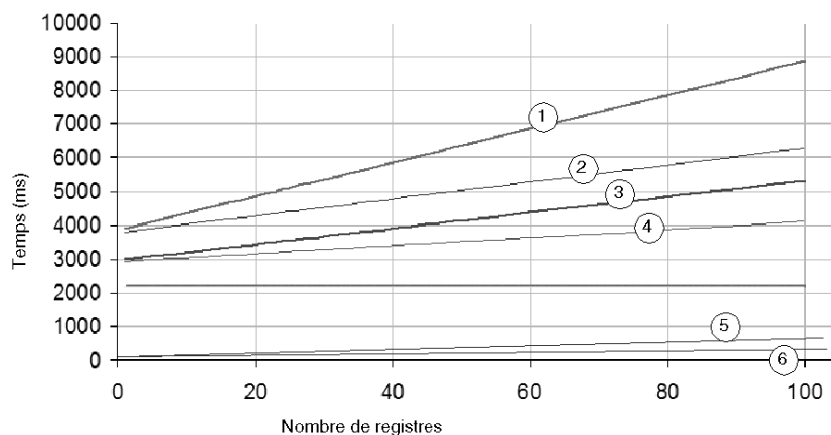
Equipements série avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 50						Timeout
EGX200	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2200.83	2644.163333	3150.83	2194.17	2590.836667	3044.17	187.5
16	2200.83	2994.163333	3900.83	2194.17	2765.836667	3419.17	187.5
32	2200.83	3367.496667	4700.83	2194.17	2952.503333	3819.17	187.5
64	2200.83	4114.163333	6300.83	2194.17	3325.836667	4619.17	187.5
100	2200.83	4954.163333	8100.83	2194.17	3745.836667	5519.17	187.5

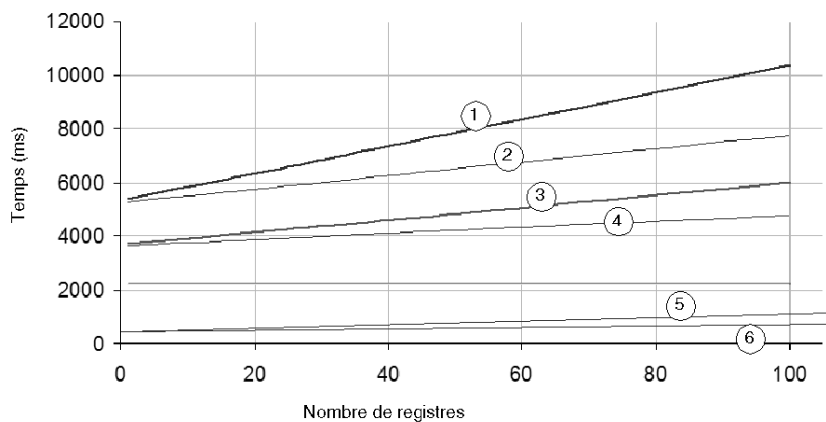
Equipements série avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						Timeout
EGX200	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2200.83	2994.163333	3900.83	2194.17	2940.836667	3794.17	187.5
16	2200.83	3344.163333	4650.83	2194.17	3115.836667	4169.17	187.5
32	2200.83	3717.496667	5450.83	2194.17	3302.503333	4569.17	187.5
64	2200.83	4464.163333	7050.83	2194.17	3675.836667	5369.17	187.5
100	2200.83	5304.163333	8850.83	2194.17	4095.836667	6269.17	187.5

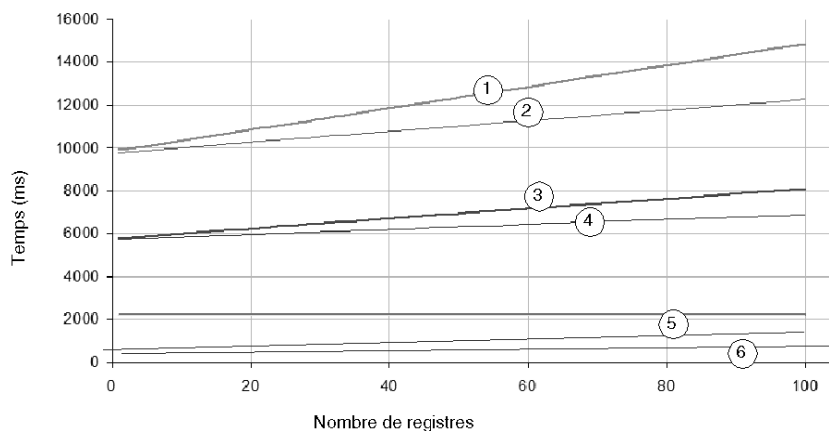
Equipements série avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						Timeout
EGX200	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2200.83	3694.163333	5400.83	2194.17	3640.836667	5294.17	187.5
16	2200.83	4044.163333	6150.83	2194.17	3815.836667	5669.17	187.5
32	2200.83	4417.496667	6950.83	2194.17	4002.503333	6069.17	187.5
64	2200.83	5164.163333	8550.83	2194.17	4375.836667	6869.17	187.5
100	2200.83	6004.163333	10350.83	2194.17	4795.83667	7769.17	187.5

Equipements série avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 500						Timeout 1 000 ms 1 tentative
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2200.83	5794.163333	9900.83	2194.17	5740.836667	9794.17	187.5
16	2200.83	6114.163333	10650.83	2194.17	5915.836667	10169.17	187.5
32	2200.83	6517.496667	11450.83	2194.17	6102.50333	10569.17	187.5
64	2200.83	7264.163333	13050.83	2194.17	6475.836667	11369.17	187.5
100	2200.83	8104.163333	14850.83	2194.17	6895.83667	12269.17	187.5

D.2 Mesures du timeout et du temps de réponse du serveur série de passerelles EGX400

Vue d'ensemble

Les performances des équipements série avec des temps de réponse de 50 ms, 100 ms, 200 ms et 500 ms sont mesurées dans le cadre d'une communication réseau via une passerelle Modbus vers Ethernet EGX400. Ces mesures sont prises à des débits réseau de 9 600 et 19 200 bauds. En outre, ces mesures sont prises dans le cas de communications établies avec succès, mais également dans le cas d'un simple échec de requête suivi d'une tentative de rétablissement de communication réussie.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du serveur série de passerelles EGX400	504
Mesures des réponses du serveur série EGX400 avec timeout de la requête	509

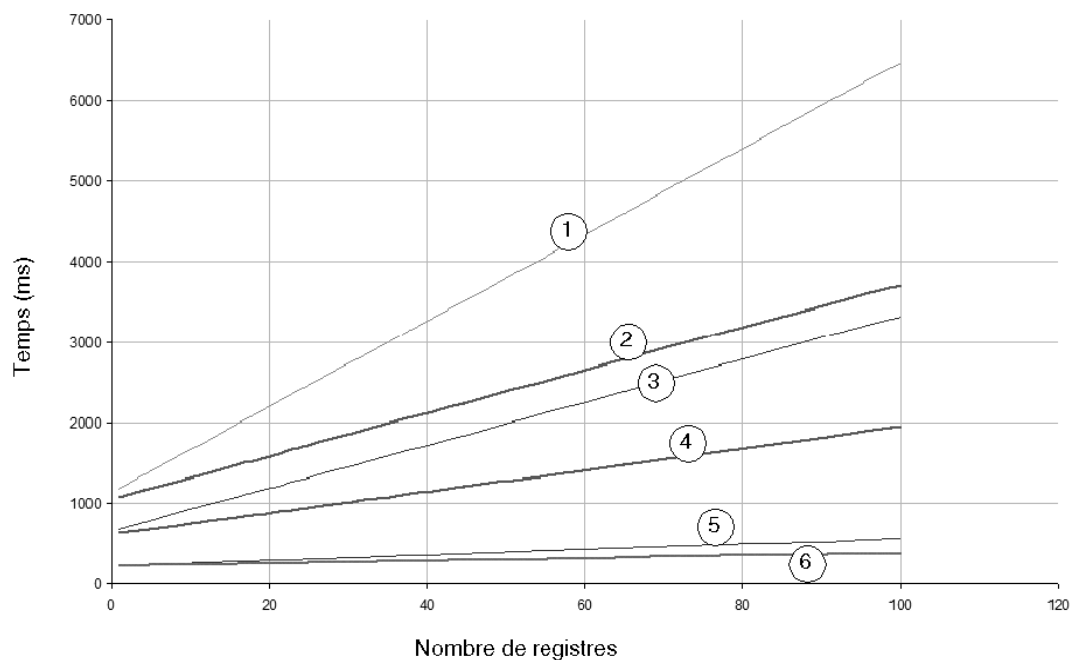
Temps de réponse du serveur série de passerelles EGX400

Configuration du test

Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle EGX400 côté série. Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur la quantité de données (c.-à-d., le nombre de registres) requise. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

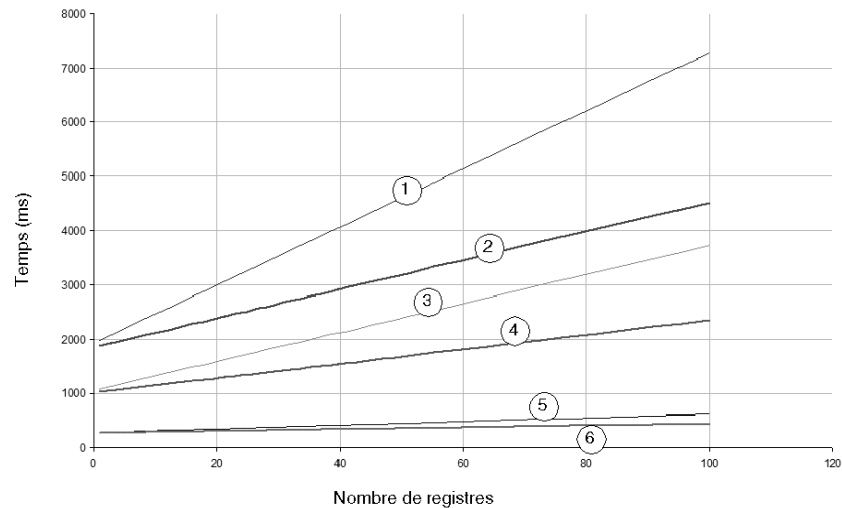
Equipements série avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 50						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	235.3333333	678.6666667	1185.333333	228.6666667	625.3333333	1078.666667	
16	285.3333333	1078.666667	1985.333333	253.6666667	825.3333333	1478.666667	
32	338.6666667	1505.333333	2838.666667	280.3333333	1038.666667	1905.333333	
64	445.3333333	2358.666667	4545.333333	333.6666667	1465.333333	2758.666667	
100	565.3333333	3318.666667	6465.333333	393.6666667	1945.333333	3718.666667	

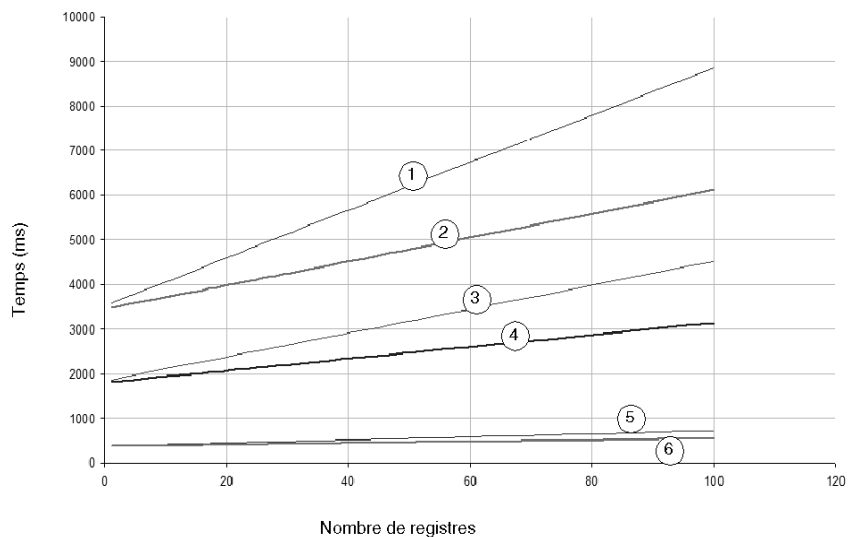
Equipements série avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	285.3333333	1078.666667	1985.333333	278.6666667	1025.3333333	1878.666667	172
16	335.3333333	1478.666667	2785.333333	303.6666667	1225.3333333	2278.666667	172
32	388.6666667	1905.333333	3638.666667	330.3333333	1438.666667	2705.333333	172
64	495.3333333	2758.666667	5345.333333	383.6666667	1865.333333	3558.666667	172
100	615.3333333	3718.666667	7265.333333	443.6666667	2345.333333	4518.666667	172

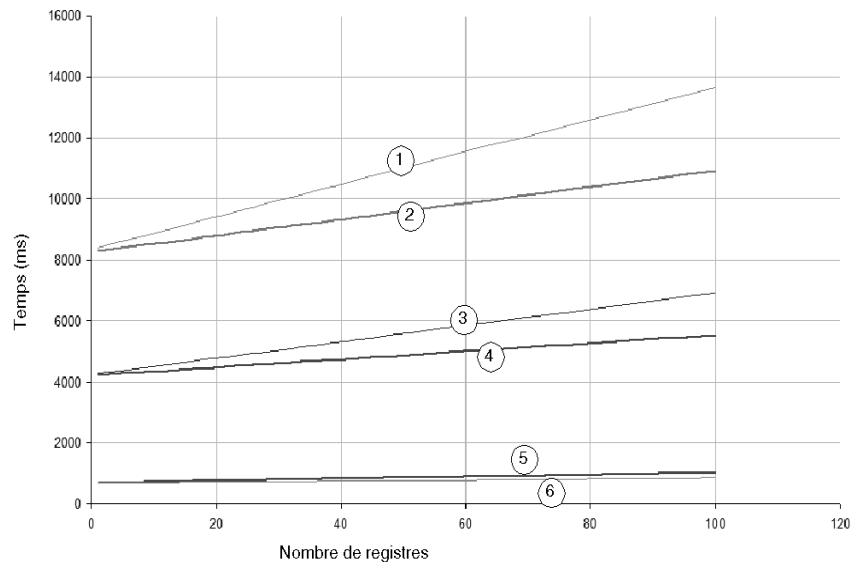
Equipements série avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	385.3333333	1878.666667	3585.333333	378.666667	1825.333333	3478.666667	172
16	435.3333333	2278.666667	4385.333333	403.666667	2025.333333	3878.666667	172
32	488.6666667	2705.333333	5238.666667	430.333333	2238.666667	4305.333333	172
64	595.3333333	3558.666667	6945.333333	483.666667	2665.333333	5158.666667	172
100	715.3333333	4518.666667	8865.333333	543.666667	3145.333333	6118.666667	172

Equipements série avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 500						
EGX200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	685.3333333	4278.666667	8385.333333	678.6666667	4225.333333	8278.666667	172
16	735.3333333	4678.666667	9185.333333	703.6666667	4425.333333	8678.666667	172
32	788.6666667	5105.333333	10038.66667	730.3333333	4638.666667	9105.333333	172
64	895.3333333	5958.666667	11745.33333	783.6666667	5065.333333	9958.666667	172
100	1015.333333	6918.666667	13665.33333	843.6666667	5545.333333	10918.66667	172

Mesures des réponses du serveur série EGX400 avec timeout de la requête

Configuration du test

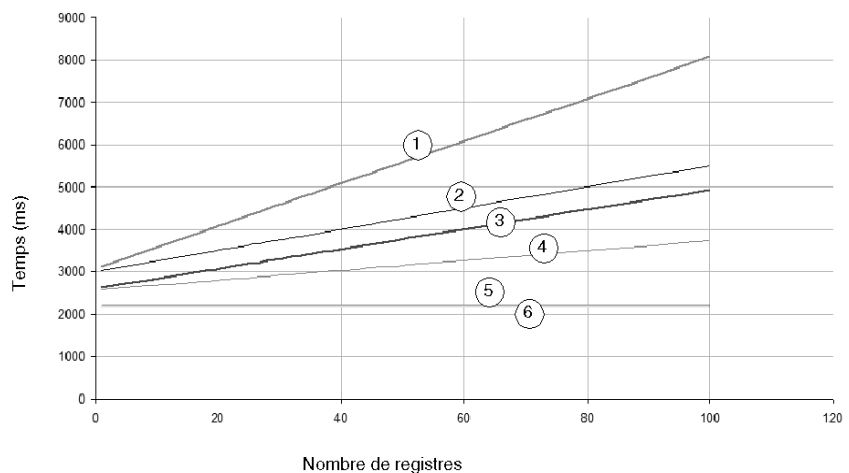
Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle EGX400 côté série, en cas d'erreur d'une requête de communication (par exemple, un équipement série déconnecté). Cet échec entraîne un timeout de 1 000 ms sur la requête initiale suivi par une nouvelle tentative de la requête.

NOTE : Un échec de requête augmente les temps de réponse pour toutes les requêtes.

Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur une quantité de données (c.-à-d., le nombre de registres) requise. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

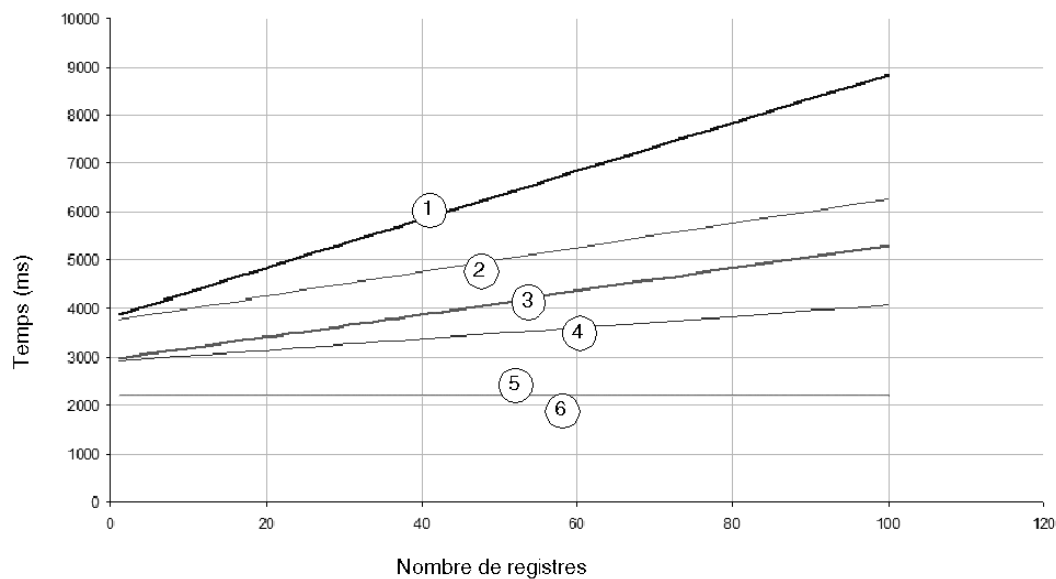
Equipements série avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 50						Timeout
EGX400	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2185.33	2628.663333	3135.33	2178.67	2575.336667	3028.167	172
16	2185.33	2978.663333	3885.33	2178.67	2750.336667	3403.167	172
32	2185.33	3351.996667	4685.33	2178.67	2937.003333	3803.67	172
64	2185.33	4098.663333	6285.33	2178.67	3310.336667	4603.67	172
100	2185.33	4938.663333	8085.33	2178.67	3730.336667	5503.67	172

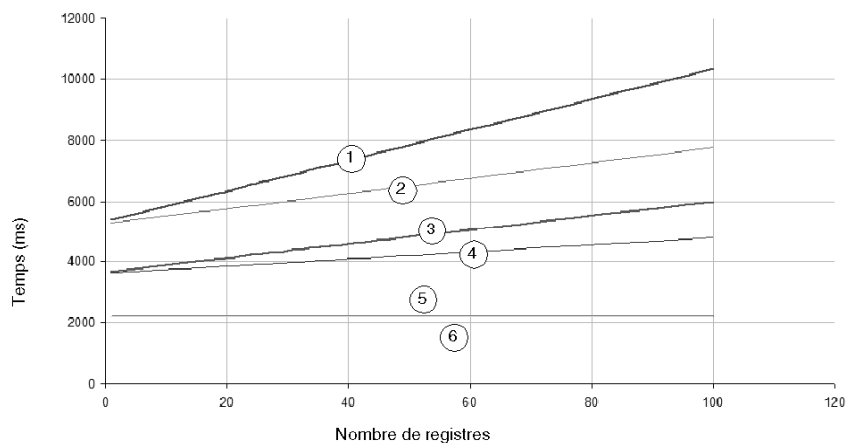
Equipements série avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						Timeout
EGX400	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2185.33	2978.663333	3885.33	2178.67	2925.336667	3778.67	172
16	2185.33	3328.663333	4635.33	2178.67	3100.336667	4153.67	172
32	2185.33	3701.996667	5435.33	2178.67	3287.003333	4553.67	172
64	2185.33	4448.663333	7035.33	2178.67	3660.336667	5353.67	172
100	2185.33	5288.663333	8835.33	2178.67	4080.336667	6253.67	172

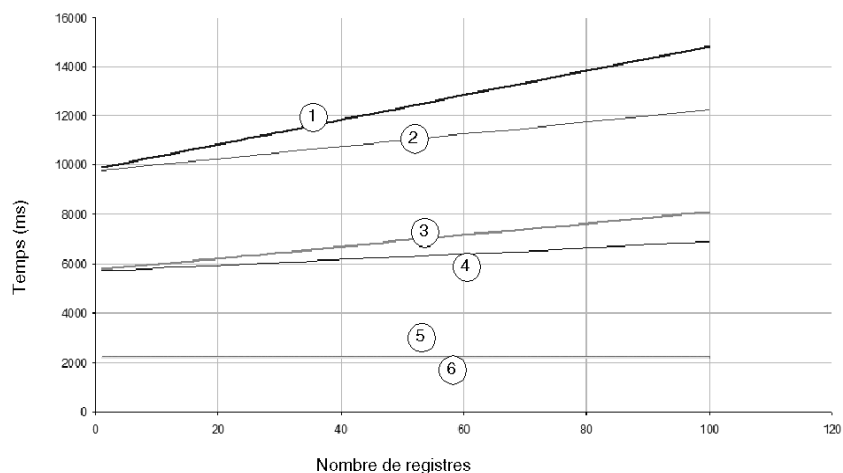
Equipements série avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						Timeout 1 000 ms 1 tentative
EGX400	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2185.33	3678.663333	5385.33	2178.67	3625.336667	5278.67	172
16	2185.33	4028.663333	6135.33	2178.67	3800.336667	5653.67	172
32	2185.33	4401.996667	6935.33	2178.67	3987.003333	6053.67	172
64	2185.33	5148.663333	8535.33	2178.67	4360.336667	6853.67	172
100	2185.33	5988.663333	10335.33	2178.67	4780.336667	7753.67	172

Equipements série avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 500						Timeout
EGX400	Durée pour accomplir toutes les requêtes						1 000 ms 1 tentative
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2185.33	5778.663333	9885.33	2178.67	5725.336667	9778.67	172
16	2185.33	6128.663333	10635.33	2178.67	5900.336667	10153.67	172
32	2185.33	6501.996667	11435.33	2178.67	6087.003333	10553.67	172
64	2185.33	7248.663333	13035.33	2178.67	6460.336667	11353.67	172
100	2185.33	8088.663333	14835.33	2178.67	6880.336667	12253.67	172

D.3 Mesures du timeout et du temps de réponse du serveur série de passerelles 174CEV30020

Vue d'ensemble

Les performances des équipements série avec des temps de réponse de 50 ms, 100 ms, 200 ms et 500 ms sont mesurées dans le cadre d'une communication réseau via une passerelle Modbus vers Ethernet 174CEV30020. Ces mesures sont prises à des débits réseau de 9 600 et 19 200 bauds. En outre, ces mesures sont prises dans le cas de communications établies avec succès, mais également dans le cas d'un simple échec de requête suivi d'une tentative de rétablissement de communication réussie.

Contenu de ce sous-chapitre

Ce sous-chapitre contient les sujets suivants :

Sujet	Page
Temps de réponse du serveur série de passerelles 174CEV30020	515
Mesures des réponses du serveur série 174CEV30020 avec timeout de la requête	520

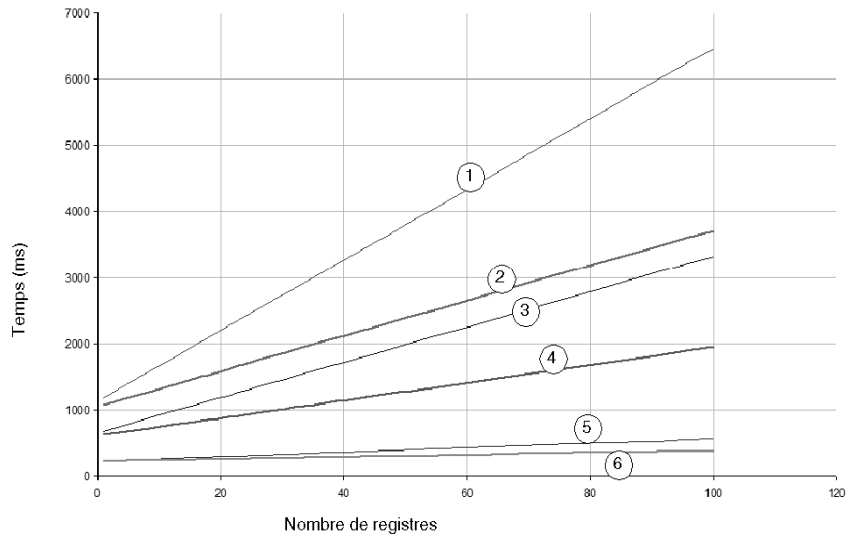
Temps de réponse du serveur série de passerelles 174CEV30020

Configuration du test

Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle 174CEV30020, côté série. Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur des quantités de données (c-à-d, le nombre de registres) précises. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

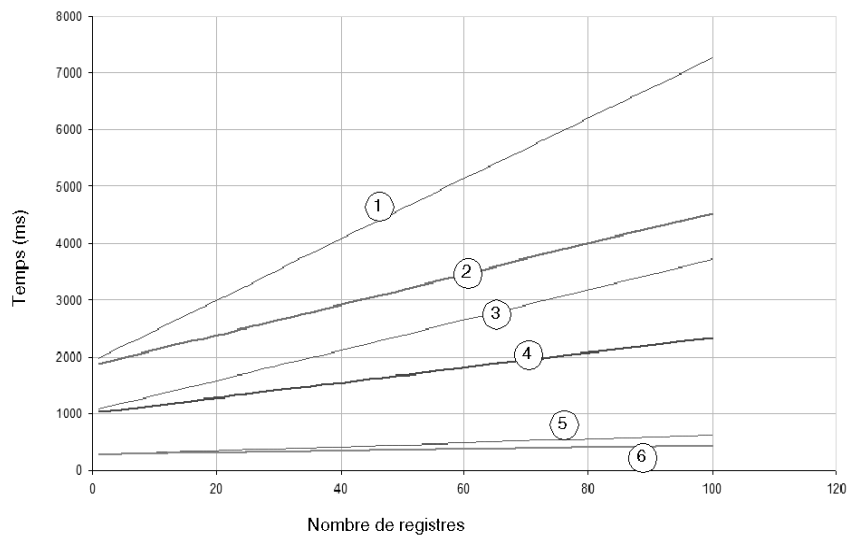
Equipements série avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Équipement	Temps de réponse du serveur série = 50						
CEV300200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	201,3333333	644,6666667	1 151,833333	194,6666667	591,8333333	1 044,166667	
16	251,3333333	1 044,666667	1 951,833333	219,6666667	791,8333333	1 444,166667	
32	304,6666667	1 471,333333	2 804,166667	246,3333333	1 004,166667	1 871,833333	
64	411,3333333	2 324,666667	4 511,833333	299,6666667	1 431,833333	2 724,166667	
100	531,3333333	3 284,666667	6 431,833333	359,6666667	1 911,833333	3 684,166667	

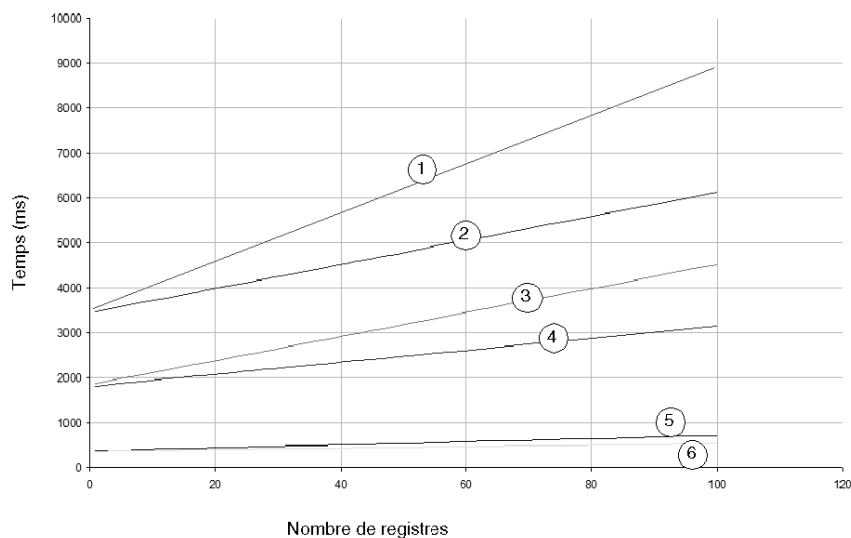
Équipements série avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						
CEV300200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	251,33333	1 044,66667	1 951,333333	244,66667	991,333333	1 844,666667	138
16	301,33333	1 444,6667	2 751,333333	269,66667	1 191,33333	2 244,666667	138
32	354,66667	1 871,33333	3 604,666667	296,33333	1 404,66667	2 671,333333	138
64	461,33333	2 724,66667	5 311,333333	349,66667	1 831,33333	3 524,666667	138
100	581,33333	3 684,66667	7 231,333333	409,66667	2 311,33333	4 484,666667	138

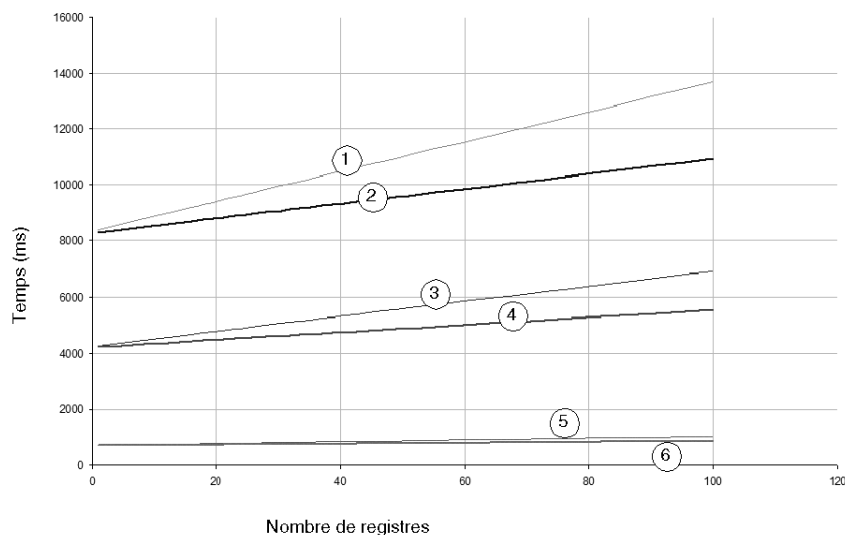
Equipements série avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Équipement	Temps de réponse du serveur série = 200						
CEV300200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	351,33333	1 844,66667	3 551,333333	344,66667	1 791,333333	3 444,666667	138
16	401,33333	2 244,66667	4 351,333333	369,66667	1 991,33333	3 844,666667	138
32	454,66667	2 671,33333	5 204,666667	396,33333	2 204,66667	4 271,333333	138
64	561,33333	3 524,66667	6 911,333333	449,66667	2 631,33333	5 124,666667	138
100	681,33333	4 484,66667	8 831,333333	509,66667	3 111,33333	6 084,666667	138

Équipements série avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 500						
CEV300200	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	651,33333	4 244,66667	8 351,333333	644,66667	4 191,333333	8 244,666667	138
16	701,33333	4 644,66667	9 151,333333	669,66667	4 391,33333	8 644,666667	138
32	754,66667	5 071,33333	10 004,66667	696,33333	4 604,66667	9 071,333333	138
64	861,33333	5 924,66667	11 711,33333	749,66667	5 031,33333	9 924,666667	138
100	981,33333	6 884,66667	13 631,33333	809,66667	5 511,33333	10 884,66667	138

Mesures des réponses du serveur série 174CEV30020 avec timeout de la requête

Configuration du test

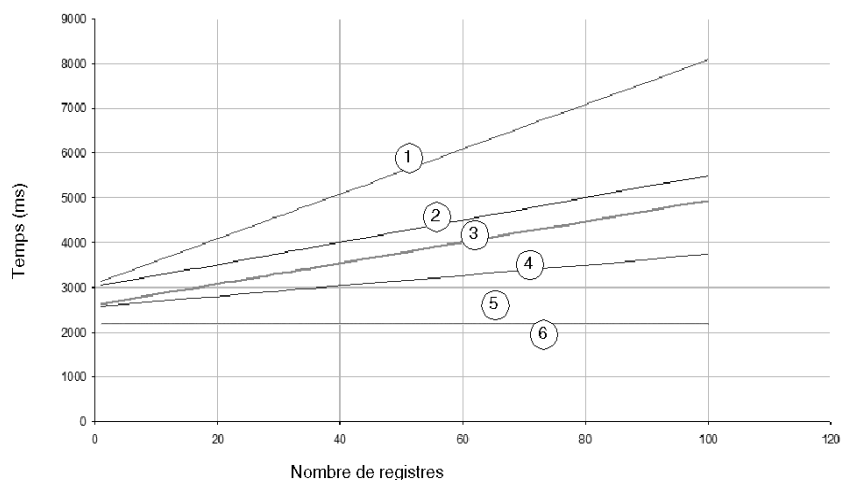
Les graphiques ci-dessous vérifient le temps nécessaire pour obtenir une réponse après un certain nombre de requêtes envoyées à des équipements connectés à la passerelle 174CEV30020, côté série, en cas d'erreur d'une requête de communication (par exemple, un équipement série déconnecté). Cet échec entraîne un timeout de 1 000 ms sur la requête initiale suivi par une nouvelle tentative de la requête.

NOTE : Un échec de requête augmente les temps de réponse pour toutes les requêtes.

Les performances sont basées sur des débits réseau de 9 600 et 19 200 bauds et sur des quantités de données (c-à-d, le nombre de registres) précis. Le tableau suivant décrit les débits en bauds testés et le nombre de requêtes envoyées pour les quatre graphiques ci-dessous :

Courbe	Nombre de requêtes	Débit en bauds
1	16	9 600
2		19 200
3	8	9 600
4		19 200
5	1	9 600
6		19 200

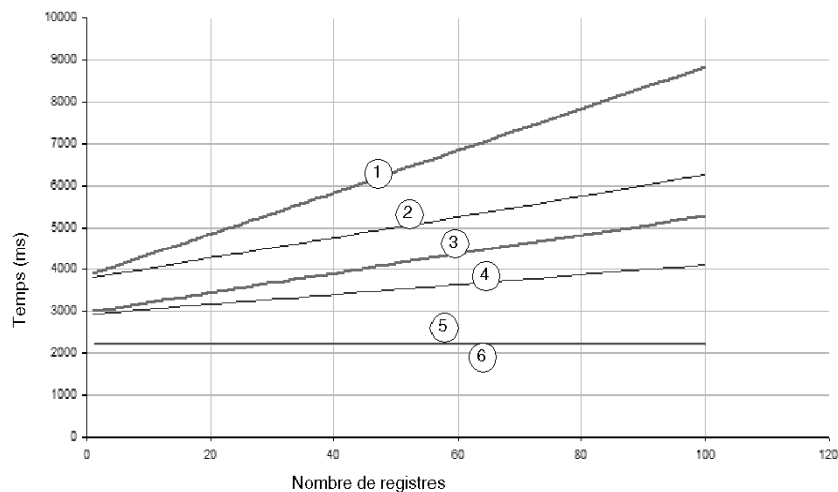
Equipements séries avec un temps de réponse de 50 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 50						
CEV30020	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2 151,33	2 594,663333	3 101,33	2 144,67	2 541,336667	2 994,67	138
16	2 151,33	2 944,663333	3 851,33	2 144,67	2 716,336667	3 369,167	138
32	2 151,33	3 317,333333	4 651,33	2 144,67	2 903,166667	3 769,67	138
64	2 151,33	4 064,996667	6 251,33	2 144,67	3 276,336667	4 569,67	138
100	2 151,33	4 904,663333	8 051,33	2 144,67	3 696,336667	5 469,67	138

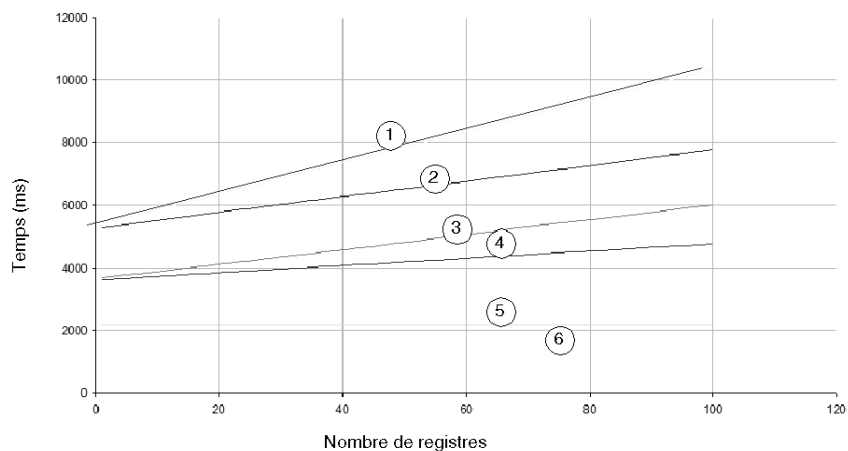
Equipements séries avec un temps de réponse de 100 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 100						
CEV30020	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2 151,33	2 944,663333	3 851,33	2 144,67	2 891,336667	3 744,67	138
16	2 151,33	3 294,663333	4 601,33	2 144,67	3 066,336667	4 119,67	138
32	2 151,33	3 667,333333	5 401,33	2 144,67	3253.003333	4 519,67	138
64	2 151,33	4 414,996667	7 001,33	2 144,67	3 626,336667	5 319,67	138
100	2 151,33	5 254,663333	8 801,33	2 144,67	4 046,336667	6 219,67	138

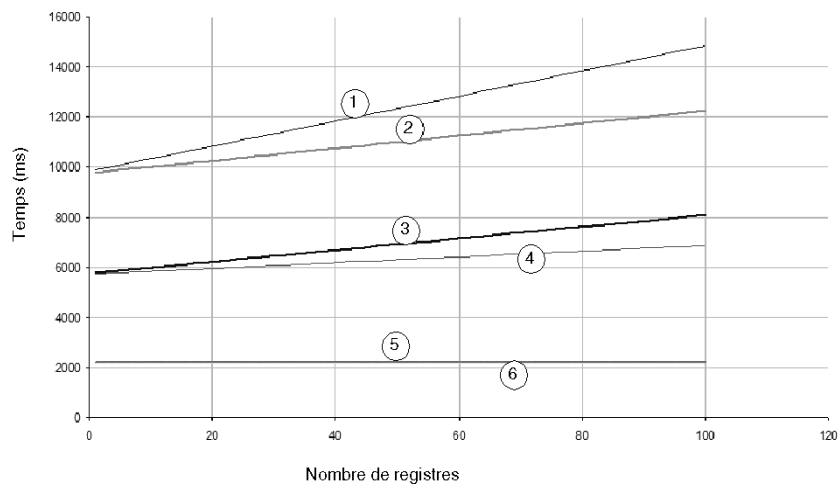
Equipements séries avec un temps de réponse de 200 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						
CEV30020	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	Durée du routage
1	2 151,33	3 644,663333	5 351,33	2 144,67	3 591,336667	5 244,67	138
16	2 151,33	3 994,663333	6 101,33	2 144,67	3 766,336667	5 619,67	138
32	2 151,33	4 367,333333	6 901,33	2 144,67	3 953,003333	6 019,67	138
64	2 151,33	5 114,996667	8 501,33	2 144,67	4 326,336667	6 819,67	138
100	2 151,33	5 954,663333	10 301,33	2 144,67	4 746,336667	7 719,67	138

Equipements séries avec un temps de réponse de 500 ms



Le tableau suivant indique les points de données utilisés pour générer le graphique représenté ci-dessus.

Equipement	Temps de réponse du serveur série = 200						
CEV30020	Durée pour accomplir toutes les requêtes						
Débit en bauds	9 600			19 200			Durée du routage
Nombre de registres	1 requête	8 requêtes	16 requêtes	1 requête	8 requêtes	16 requêtes	
1	2 151,33	5 744,663333	9 851,33	2 144,67	5 691,336667	9 744,67	
16	2 151,33	6 094,663333	10 601,33	2 144,67	5 866,336667	10 119,67	
32	2 151,33	6 467,333333	11 401,33	2 144,67	6 053,003333	10 519,67	
64	2 151,33	7 214,996667	13 001,33	2 144,67	6 426,336667	11 319,67	
100	2 151,33	8 054,663333	14 801,33	2 144,67	6 846,336667	12 219,67	138

Normes et autres considérations relatives aux réseaux Ethernet industriel



Vue d'ensemble

Cette annexe fournit des informations complémentaires sur les normes et les informations de planification présentées au Chapitre 2 (*voir page 29*).

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Normes et organisations	526
Compatibilité électromagnétique	536
Activités de normalisation des connecteurs en cuivre	541
Conformité aux normes	542
Conformité du réseau Ethernet industriel Transparent Ready	544

Normes et organisations

Organisations de normalisation

Plusieurs organisations de normalisation sont chargées de définir des exigences de câblage générales. Par exemple, Electronics Industries Alliance (EIA) et Telecommunications Industry Association (TIA) élaborent et approuvent les normes régissant les câbles LAN. D'autres organisations ont en charge l'élaboration de normes réseau spécifiques aux caractéristiques de câblage.

Organisation de normalisation	Site Web	Description	Zone d'application
EIA	www.eia.org	Association qui regroupe les industries de matériel électronique et de télécommunications : TIA, CEMA, ECA, EIG, GEIA, JEDEC et EIF.	Etats-Unis et Canada
TIA	www.tiaonline.org	Association regroupant essentiellement des entreprises nord-américaines fournissant des produits haute technologie, matériaux, systèmes, services de distribution et services professionnels dans le domaine des communications et de l'information.	Etats-Unis et Canada
CEI (Commission électrotechnique internationale)	www.iec.ch	Organisme international de normalisation et d'évaluation de la conformité dans tous les domaines de l'électro-technologie, y compris l'électricité et l'électronique.	Mondiale
ISO (Organisation internationale de normalisation)	www.iso.org	Réseau fédérateur d'instituts nationaux de normalisation de 146 pays. Les normes de câblage ne représentent qu'une partie infime des activités globales de l'ISO.	Mondiale
CENELEC (Comité Européen de Normalisation Electrotechnique)	www.cenelec.org	Développe des normes électrotechniques pour le marché européen/l'espace économique européen. La majorité des normes de câblage développées par le CENELEC sont modelées, à quelques exceptions près, sur les normes ISO.	Europe
CSA (Association Canadienne de Normalisation)	www.csa.ca	Organisme indépendant élaborant des normes de sécurité à l'échelle mondiale pour les produits et services, par le biais d'essais, de certification, de contrôle de sécurité et de performance, y compris les essais CEM et CEI.	Canada
IEEE 802.3 (International Electrical and Electronics Engineers)	www.ieee.org	Groupe de travail développant des normes pour les réseaux locaux basés CSMA/CD (Ethernet), y compris les réseaux 1000Base-T et 100Base-T.	Mondiale

Organisation de normalisation	Site Web	Description	Zone d'application
ANSI	www.ansi.org	Organisme chargé de l'élaboration des normes nationales aux Etats-Unis. L'ANSI est le seul représentant et membre cotisant des Etats-Unis au sein des deux principales organisations internationales de normalisation, l'ISO et la CEI (via l'USNC, le Comité national américain). Avec l'ANSI, les Etats-Unis bénéficient d'un accès direct aux processus de développement des normes ISO et CEI.	Mondiale
IETF (Internet Engineering Task Force)	www.ietf.org	L'IETF est une communauté étendue et ouverte d'experts internationaux du Web (concepteurs de réseaux, opérateurs, fournisseurs et chercheurs), soucieux de contribuer à l'évolution de son architecture et à son bon fonctionnement. C'est elle qui a la charge de la suite des protocoles Internet (TCP/IP).	Mondiale
IANA (Internet Assigned Numbers Authority)	www.iana.org	Organisation dont la mission est de préserver les fonctions de coordination centrales de l'Internet dans l'intérêt du bien public : affectation des numéros IP, des noms de domaine, etc.	Mondiale

D'autres organisations Ethernet industriel fournissent des recommandations et soutiennent ces organisations de normalisation, mais elles ne sont pas accréditées à développer des normes.

Suite de normes TCP/IP Internet

L'IETF est une communauté d'experts informatiques qui gère la suite TCP/IP, et notamment l'évolution des protocoles, tels que TCP, IP, UDP, SNMP, HTTP et FTP.

Requirements for Internet Hosts - Communication Layers	RFC 1122 IETF Network Working Group, R. Branden, Ed., RFC-1122 (STD-0003), Octobre 1989
--	---

Norme relative au protocole d'application industrielle Modbus

Modbus Application Protocol Specification	Modbus-IDA - Version 1.1a, Juin 2004IEC PAS
---	---

Norme TIA/EIA-568-A

La norme TIA/EIA-568-A est l'une des premières normes de câblage. Développée conjointement par le TIA et l'EIA, cette norme définit le système de câblage dans les réseaux voix et données, sous la forme d'un réseau structuré et hiérarchique en topologie en étoile, dans lequel des câbles haute vitesse (à fibre optique) alimentent des réseaux périphériques plus lents. Elle a été intégrée à la norme TIA/EIA-568-B en 2000.

Norme	Domaine	Description
TIA/EIA-568-A-1995	Télécommunications des immeubles commerciaux	Réglemente les systèmes de câblage des immeubles commerciaux gérant les réseaux Voix Données Vidéo. Elle définit également des critères techniques et de performance pour le câblage.
	Normes de câblage	
TIA/EIA-568-A (1998-1999)	Mises à jour	A1 spécifie les paramètres de temps de propagation et de différence de temps de propagation. A2 couvre des modifications diverses. A3 définit les exigences applicables aux câbles en faisceaux et hybrides. A4 définit les exigences de paradiaphonie et de perte par retour pour les câbles de raccordement. A5 spécifie les exigences de performance applicables à la catégorie 5 améliorée (CAT5e).
TIA/EIA-568-B.1-2000	Télécommunications des immeubles commerciaux	Regroupe, dans une nouvelle version, toutes les mises à jour précédentes et recommande le câble catégorie 5e en raison de ses performances. Plusieurs amendements fournissent des informations techniques sur le câblage à paire torsadée, le câblage à paire torsadée blindé et le câblage à fibre optique 100 Ω .
	Normes de câblage	
ANSI/TIA/EIA-568-B.2	Norme de câblage pour câble à paire torsadée 100 Ω	
ANSI/TIA/EIA-568-B.3	Norme sur les fibres optiques	
TIA/EIA-569-A-1995	Norme des immeubles commerciaux pour les voies d'accès et les espaces de télécommunications	Réglemente la conception des voies d'accès et des espaces des supports de télécommunications.
TIA/EIA-606-1994	Norme de gestion des infrastructures d'immeubles	Définit des directives de conception pour la gestion des installations de télécommunications.
TIA/EIA-607-1995	Exigences de mise à la masse et de liaison	Définit les exigences de mise à la masse et de liaison equipotentielle pour le câblage et les équipements de télécommunication.
ANSI/EIA/TIA-570-A	Norme de câblage résidentiel pour les télécommunications	

Les normes TIA/EIA définissent un système de câblage structuré conçu et monté dans plusieurs blocs. Ces blocs sont intégrés dans un réseau hiérarchique afin de créer un système de communication unifié. Les réseaux LAN constituent des blocs avec des exigences de faible performance, alors que les blocs de réseaux fédérateurs, nécessitant des câbles à fibre optique hautement performants, servent à connecter les blocs entre eux dans une topologie en étoile. Ces normes définissent également les exigences des câbles à fibre optique (monomode et multimode), STP et UTP.

En résumé, la norme de câble TIA/EIA 568 fournit :

- des spécifications pour un système de câblage générique des télécommunications des immeubles commerciaux ;
- des spécifications pour les supports, topologies réseau, terminaisons et points de connexion (mise à la masse), et la gestion des systèmes de câblage ;
- un support pour les environnements utilisant des produits et des fournisseurs différents ;
- des informations sur la planification et l'installation d'un réseau de télécommunication pour les immeubles.

Normes ISO/CEI IS 11801 et EN 50173

Les normes ISO/CEI 11081 et EN 50173 définissent la structure et la configuration des systèmes de câblage pour les bureaux et les campus. Elles sont pratiquement identiques en termes de champ d'application et de contenu, de terminologie employée et d'informations techniques fournies. Le système de câblage générique spécifié n'est basé sur aucune application spécifique et consiste en un système de composants de câblage ouvert, facile à implémenter. Le système de câblage décrit dans la norme prend en charge une variété de services comprenant la voix, les données, les images et la vidéo.

Le tableau ci-dessous répertorie les mises à jour de la norme ISO/CEI-11801.

Norme		Description
ISO/CEI-11801:1995	Câblage générique des locaux du client	Basée sur la norme de câblage TIA/EIA-568, cette norme définit un système de câblage de télécommunications pour les bureaux et les campus.
ISO/CEI-11801:2000	Câblage générique des locaux du client, 2ème Edition	Editée en 2000 - mise à jour de la norme précédente reflétant les nouvelles versions de la norme TIA/EIA-568.
Administration, documentation, rapports		ISO/CEI 14763-1
Pratiques de planification et d'installation		ISO/CEI 14763-2

Norme		Description
Essais des câblages à fibre optique		ISO/CEI 14763-3
Essais des câblages cuivre		CEI 61935-1

Le tableau ci-dessous répertorie la norme EN 50173 et les normes associées.

Documents de normalisation européens	Référence
Phase de conception de construction	
Application de liaison équipotentielle et de mise à la masse dans les locaux contenant des équipements de technologie de l'information	EN 50310
Phase de conception de codage	
Technologie de l'information – Systèmes de câblage génériques	EN 50173 (et/ou EN 50098-1 ou -2) :
Phase de conception de planification	
Spécification et assurance qualité	EN 50174-1
Planification et pratiques d'installation à l'intérieur des bâtiments	EN 50174-2
Planification et pratiques d'installation à l'extérieur des bâtiments	EN 50174-3
Essais des câblages installés	EN 50346
Application de liaison équipotentielle et de mise à la masse dans les locaux avec équipements de technologie de l'information	EN 50310
Phase de conception d'implémentation	
Spécification et assurance qualité	EN 50174-1
Planification et pratiques d'installation à l'intérieur des bâtiments	EN 50174-2
Planification et pratiques d'installation à l'extérieur des bâtiments	EN 50174-3
Essais des câblages installés	EN 50346
Application de liaison équipotentielle et de mise à la masse dans les locaux avec équipements de technologie de l'information	EN 50310
Essais des câblages installés	EN 50346
Phase d'opération	
Spécification et assurance qualité	EN 50174 Partie 1

La norme ISO/CEI-11801:2000 spécifie les systèmes de câblage pour les propriétés commerciales pouvant inclure un ou plusieurs bâtiments sur un campus. Elle définit les exigences relatives aux câbles en cuivre et à fibre optique. Même si cette norme couvre les immeubles de bureaux, les principes énoncés s'appliquent également aux autres types d'installations.

En résumé, la norme ISO/CEI-11801 fournit :

- la structure et la configuration minimale pour un système de câblage générique ;
- les exigences de performance de chaque liaison par câble ;
- les exigences de conformité et procédures de vérification ;
- les exigences liées à une installation.

Cette norme ne couvre pas les spécifications des câbles utilisés pour connecter les équipements spécifiques aux applications à un système de câblage. Les lignes directrices énoncées couvrent uniquement les performances et la longueur des câbles, car ces deux paramètres sont les plus susceptibles d'affecter la qualité de transmission. La sécurité et la compatibilité électromagnétique ne sont pas abordées dans cette norme. Toutefois, les informations connexes contenues dans la norme ISO/CEI 11801 peuvent permettre de mieux comprendre les réglementations énoncées dans les autres documents de normalisation. Pour qu'une installation de câblage soit conforme à la norme CEI 11801, la configuration doit connecter les sous-systèmes suivants pour créer une structure de câblage générique :

- Réseau fédérateur campus – via un répartiteur campus
- Réseau fédérateur bâtiment – via un répartiteur bâtiment pour chaque bâtiment
- Câblage horizontal – via des répartiteurs sol

Normes de compatibilité électromagnétique (CEM)

Les principales organisations de normalisation CEM sont :

- CEI - Commission électrotechnique internationale (Genève)
- CENELEC - Comité Européen de Normalisation Electrotechnique (Bruxelles)

Il existe deux normes internationales importantes réglementant l'émission électromagnétique et l'immunité :

- CEI 61000-6-2:1999 Compatibilité électromagnétique (CEM) - Partie 6-2 : Normes génériques – Immunité pour les environnements industriels
- CEI 61000-6-4:1997 Compatibilité électromagnétique (CEM) - Partie 6 : Normes génériques - Section 4 : Norme sur l'émission pour les environnements industriels

Le tableau ci-dessous répertorie les normes et publications décrivant les exigences liées à la compatibilité électromagnétique (*voir page 536*).

Le tableau ci-dessous précise, après chaque référence de publication CEI, le document de normalisation européen équivalent, entre crochets.

Publications CEI		Description
Généralités		
CEI 1000-1-1 (1992)		Application et interprétation de définitions et termes fondamentaux.
Environnement		
CEI 1000-2-1 (1990)		Environnement électromagnétique pour les perturbations conduites basses fréquences et la transmission de signaux sur les réseaux publics d'alimentation.
CEI 1000-2-2 (1990)		Niveaux de compatibilité pour les perturbations conduites à basse fréquence et la transmission des signaux sur les réseaux publics d'alimentation basse tension.
CEI 1000-2-3 (1992)		Phénomènes rayonnés et conduits à des fréquences autres que celle du réseau.
CEI 1000-2-4 (1994)		Niveaux de compatibilité dans les installations industrielles pour les perturbations conduites à basse fréquence.
CEI 1000-2-5 (1995)		Classification des environnements électromagnétiques.
Limites		
552-2	CEI 1000-3-2 (1995) [EN 61000-3-2 (1995)]	Limites pour les émissions de courant harmonique (courant appelé par les appareils < 16 A par phase).
552-3	CEI 1000-3-3 (1994) [EN 61000-3-3 (1995)]	Limitation des fluctuations de tension et du papillotement dans les réseaux basse tension, pour les matériels ayant un courant assigné inférieur ou égal à 16 A.
	CEI 1000-3-5 (1994)	Limitation des fluctuations de tension et du papillotement dans les réseaux basse tension pour les équipements ayant un courant appelé supérieur à 16 A.
Guides d'installation et d'atténuation		
CEI 1000-5-1		Considérations générales
CEI 1000-5-2		Mise à la terre et câblage
CEI 1000-5-3		Concepts de protection

Norme CEI 1000-4

La norme CEI 1000-4 (préalablement CEI-801) établit une "référence commune pour l'évaluation de la performance des instruments de mesure et de contrôle des procédés industriels, lorsque ceux-ci sont exposés à des perturbations électriques ou électromagnétiques".

Cette norme couvre uniquement les types de perturbations provoquées par des sources externes à l'équipement. Elle décrit les essais de sensibilité aux perturbations destinés à démontrer l'aptitude de l'équipement à fonctionner correctement dans son environnement normal. L'essai approprié est déterminé en fonction du type de perturbations auxquelles l'équipement est soumis à son emplacement d'installation, en prenant en compte le circuit électrique (plus précisément, la façon dont le circuit et les blindages sont reliés à la prise de terre), la qualité du blindage et l'environnement.

La norme CEI 1000-4 est divisée en six sections.

Techniques d'essai et de mesure		
801-1	CEI 1000-4-1 (1992-12) [EN 61000-4 (1994-08)]	Vue d'ensemble des essais d'immunité
801-2	CIE 1000-4-2 (1995-01) [EN 61000-4-2]	Essais d'immunité aux décharges électrostatiques.
801-3	CEI 1000-4-3 (1995-02) [ENV 50140 (1993)]	Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques.
801-4	CIE 1000-4-4 (1995-01) [EN 61000-4-4]	Essais d'immunité aux transitoires électriques rapides en salves.
801-5	CIE 1000-4-5 (1995-02) [EN 61000-4-5]	Essais d'immunité aux ondes de choc.
	pr CEI 1000-4-6 [ENV 50141 (1993)]	Immunité aux perturbations conduites, induites par les champs radioélectriques.
	CEI 1000-4-7 (1991-07) [EN 61000-4-7 (1993-03)]	Guide général relatif aux mesures d'harmoniques et d'interharmoniques, ainsi qu'à l'appareillage de mesure, applicable aux réseaux d'alimentation et aux appareils qui y sont raccordés.
	CEI 1000-4-8 (1993-06) [EN 61000-4-8 (1993-09)]	Essai d'immunité au champ magnétique à la fréquence du réseau.
	CEI 1000-4-9 (1993-06) [EN 61000-4-9 (1993-09)]	Essai d'immunité au champ magnétique impulsionnel.
	CEI 1000-4-10 (1993-06) [EN 61000-4-10 (1993-09)]	Essai d'immunité au champ magnétique oscillatoire amorti.

Techniques d'essai et de mesure		
	CEI 1000-4-11 (1994-06) [EN 61000-4-11 (1994-09)]	Essais d'immunité aux creux de tension, coupures brèves et variations de tension.
	pr CEI 1000-4-12	Essai d'immunité aux ondes oscillatoires.

Normes sur les automates programmables

Automates programmables Partie 2 : Exigences et essais des équipements	CEI 61131-2
---	-------------

Normes TIA/EIA 568

La norme TIA/EIA-568-A, développée conjointement par TIA et EIA, est l'une des premières normes de câblage. Cette norme définit le système de câblage dans les réseaux voix et données sous la forme d'un réseau structuré et hiérarchique en topologie en étoile dans lequel des câbles haute vitesse (à fibre optique) alimentent des réseaux périphériques plus lents. Elle a été intégrée à la norme TIA/EIA-568-B en 2000.

Le tableau ci-dessous répertorie les mises à jour de la norme TIA/EIA-568.

Norme		Description
TIA/EIA-568-A-1995	Norme de câblage des télécommunications des immeubles commerciaux	Réglemente les systèmes de câblage des immeubles commerciaux gérant les réseaux Voix Données Vidéo. Elle définit également des critères techniques et de performance pour le câblage.
TIA/EIA-568-A (1998-1999)	Mises à jour	A1 spécifie les paramètres de temps de propagation et de différence de temps de propagation.
		A2 couvre des modifications diverses.
		A3 définit les exigences applicables aux câbles en faisceaux et hybrides.
		A4 définit les exigences de paradiaphonie et de perte par retour pour les câbles de raccordement.
		A5 spécifie les exigences de performance applicables à la catégorie 5 améliorée (CAT5e).

Norme		Description
TIA/EIA-568-B.1-2000	Norme de câblage des télécommunications des immeubles commerciaux	Regroupe, dans une nouvelle version, toutes les mises à jour précédentes et recommande le câble catégorie 5e en raison de ses performances. Plusieurs amendements fournissent des informations techniques sur le câble à paire torsadée, le câble à paire torsadée blindé et le câble à fibre optique 100 ohms.
TIA/EIA-569-A-1995	Norme des immeubles commerciaux pour les voies d'accès et les espaces de télécommunications	Réglemente la conception des voies d'accès et des espaces des supports de télécommunications.
TIA/EIA-606-1994	Norme de gestion des infrastructures d'immeubles	Définit des directives de conception pour la gestion des installations de télécommunications.
TIA/EIA-607-1995	Exigences de mise à la masse et de liaison	Définit les exigences de mise à la masse et de liaison equipotentielle pour le câblage et les équipements de télécommunication.

Les normes TIA/EIA définissent un système de câblage structuré conçu et monté dans plusieurs blocs. Ces blocs sont intégrés dans un réseau hiérarchique afin de créer un système de communication unifié. Les réseaux locaux constituent des blocs avec des exigences de faible performance, alors que les blocs de réseaux fédérateurs, nécessitant des câbles à fibre optique hautement performants, servent à connecter les blocs entre eux dans une topologie en étoile. Ces normes définissent également les exigences des câbles à fibre optique (monomode et multimode), STP et UTP. En résumé, la norme de câble TIA/EIA 568 fournit :

- des spécifications pour un système de câblage générique des télécommunications des immeubles commerciaux ;
- des spécifications pour les supports, topologies réseau, terminaisons et points de connexion (mise à la masse), et la gestion des systèmes de câblage ;
- un support pour les environnements utilisant des produits et des fournisseurs différents ;
- des informations sur la planification et l'installation d'un réseau de télécommunication pour les immeubles commerciaux.

Compatibilité électromagnétique

Introduction

Les interférences électromagnétiques (EMI) se caractérisent soit par des parasites électromagnétiques, soit par un signal brouilleur ou encore un changement du milieu de propagation, pouvant dégrader les performances des appareils et équipements de tout un système. Elles constituent l'une des premières causes de dysfonctionnement des réseaux de communication en environnement industriel. Les EMI ont un impact variable sur les applications industrielles, allant d'une simple influence acceptable à la dégradation des composants du système. Au cours de l'installation, vous devez donc connaître les conditions d'EMI et respecter les procédures qui garantissent la compatibilité électromagnétique et un environnement sûr.

Les paragraphes qui suivent fournissent des informations de base sur les types et les sources d'interférences électromagnétiques et proposent des solutions permettant de réduire ces interférences dans les environnements où doivent coexister machines industrielles et réseaux de communication. Vous trouverez également des explications sur la terminologie et les classifications utilisées.

Définitions

La compatibilité électromagnétique (*CEM*) est la capacité d'un appareil, équipement ou système à fonctionner correctement dans son environnement électromagnétique, sans introduire de perturbations intolérables dans cet environnement ou un autre équipement. Pour cela, le niveau d'émission d'interférences des appareils ou équipements dans un système doit être suffisamment bas pour ne pas interférer avec d'autres appareils ou équipements situés dans le même environnement électromagnétique. Etant donné que les équipements et les câblages réseau peuvent être sensibles aux EMI et en émettre eux-mêmes, le niveau d'immunité des équipements et des appareils doit donc être suffisant pour éviter que ceux-ci ne perturbent ou ne soient perturbés par d'autres équipements dans l'environnement.

Les interférences *EMI* constituent un phénomène électromagnétique capable de dégrader les performances d'un appareil, d'un équipement ou d'un système. Dans certains cas, ces interférences peuvent être suffisamment importantes pour endommager définitivement les équipements. Dans les réseaux de communication, les EMI sont simplement un signal électrique brouilleur qui vient s'ajouter au signal utile. Ce signal brouilleur est émis par les conductions des conducteurs ou par le rayonnement dans l'air.

Perturbation et interférence

Les termes *EMI* et *perturbation* ont globalement le même sens. Une perturbation peut être générée par un phénomène électromagnétique, tel qu'une tension électrique, un courant électrique ou des champs magnétiques ou électriques. Elle présente une large amplitude et plage de fréquences sur des durées de temps variables et réduit la capacité des équipements sensibles à fonctionner correctement.

Influence électromagnétique

L'influence électromagnétique se produit chaque fois qu'une perturbation est transmise d'une source d'interférences vers un équipement sensible en passant par un ou plusieurs mécanismes de couplage. La source d'interférences peut être n'importe quel appareil ou équipement émettant une perturbation électromagnétique, comme un câblage électrique, des câbles et équipements de communication, des régulateurs et relais ou des moteurs électriques.

L'équipement sensible peut être n'importe quel composant d'équipement ou d'appareil susceptible d'être influencé par les interférences EMI. Il présente donc un *niveau d'immunité faible* aux EMI.

Mécanismes de couplage

Le *couplage* représente la propagation des EMI depuis leur source vers d'autres appareils ou équipements sensibles. Il existe cinq types de mécanismes de couplage.

Mécanismes de couplage	Description
Galvanique	Couplage via un circuit commun
Inductif	Couplage via un champ magnétique
Capacitif	Couplage via un champ électrique – également appelé couplage électrostatique
Influence du rayonnement	Couplage via un champ électromagnétique
Influence des ondes	Couplage via un champ électromagnétique

Les interférences peuvent être transmises sous forme conduite (*énergie guidée*), le long d'un fil par exemple, ou dans l'air (*énergie non guidée/rayonnée*). Elles se présentent généralement sous la forme d'interférences rayonnées et guidées en ligne. En règle générale, les lois physiques qui s'appliquent au transfert d'énergie dans des champs électromagnétiques valent également pour le couplage des interférences.

Pour installer une application Ethernet industriel, vous devez comprendre les phénomènes d'interférences électromagnétiques, les mécanismes de couplage et les influences et connaître les mesures préventives applicables, avant toute installation. Il existe plusieurs façons de réduire les EMI et améliorer la CEM dans votre installation, décrites ci-après.

Méthodes de réduction des EMI

Selon le type de couplage d'interférences, vous avez le choix entre plusieurs méthodes permettant de réduire ou de neutraliser les EMI. Le tableau ci-dessous répertorie les méthodes adaptées à chaque type de couplage.

Méthodes	Couplage galvanique	Couplage inductif	Couplage capacitif	Influence du rayonnement	Influence des ondes
Mise à la terre	X	-	-	-	-
Isolation électrique	X	-	-	-	-
Circuits d'équilibrage	-	X	X	X	-
Transposition des lignes de départ/de retour	-	X	X	X	-
Placement des fils	-	X	X	X	-
Placement des équipements	-	X	X	X	-
Blindage	-	X	X	X	-
Filtrage	X	X	X	X	X
Sélection des câbles	X	-	X	X	X
Disposition des fils	X	X	X	X	X

NOTE : Les méthodes de réduction des EMI les plus efficaces sont le blindage et la disposition des fils. Ces deux méthodes sont décrites plus en détails dans ce chapitre.

Veillez à prendre les mesures appropriées visant à :

- réduire la transmission de perturbations électromagnétiques depuis les sources d'interférences ;
- limiter la propagation de ces perturbations électromagnétiques.

Types d'interférences électromagnétiques

Types d'interférences électromagnétiques

- Basse fréquence
- Haute fréquence

Les interférences basse fréquence se présentent principalement sous forme conduite, comme la conduction dans les câbles. Elles sont souvent émises pendant une longue période, plus d'une douzaine de millisecondes, et peuvent parfois être continues (harmonique). L'énergie conduite peut être élevée et provoquer un dysfonctionnement, voire la destruction des équipements connectés. L'intervalle de fréquence est égal à ≤ 1 à 5 Hz.

Les interférences haute fréquence se présentent principalement sous forme rayonnée, comme les décharges électrostatiques dans l'air. L'énergie rayonnée est généralement basse et peut provoquer le dysfonctionnement des équipements et des appareils à proximité. Les interférences haute fréquence sont transmises avec un temps de montée d'impulsion inférieur à 10 ns. Elles peuvent être continues, notamment dans les redresseurs et les horloges. L'intervalle de fréquence est égal à ≥ 30 MHz.

Les interférences haute fréquence peuvent également se présenter sous une forme conduite, comme un courant ou une tension transitoire. Un transitoire est une oscillation temporaire qui se produit dans un circuit suite à une variation soudaine de la tension ou de la charge. Par exemple, il pourrait être provoqué par la foudre ou une panne électrique. Les perturbations de type décharges électrostatiques peuvent également être conduites le long de conducteurs et ensuite facilement injectées dans d'autres conducteurs, par rayonnement.

Interférences basse et haute fréquence

Le tableau ci-dessous répertorie les différentes sources d'interférences basse fréquence.

Type	Sources possibles	Effets des EMI
Interférences harmoniques	Inverseurs, hacheurs Redresseurs en pont, électrolyse, machines à souder, etc. Fours à arc Fours à induction Starter électronique Régulateurs de vitesse électroniques pour moteurs cc Convertisseurs de fréquence pour moteurs à induction et synchrones Appareils électroménagers, tels que téléviseurs, lampes à décharge de gaz et lampes fluorescentes	Dysfonctionnement des équipements connectés Destruction éventuelle des équipements connectés

Type	Sources possibles	Effets des EMI
Interférences secteur basse tension	Fluctuations de tension, coupures brèves, creux de tension et surtensions transitoires Variations de fréquence Harmoniques de forme d'onde, transitoires, courants porteurs Phases, dissymétrie Courts-circuits de puissance, surcharges (effets sur la tension)	Dysfonctionnement des équipements connectés, comme une interruption de relais haute vitesse pendant les creux de tension Perte de puissance Destruction éventuelle du matériel électronique

Le tableau ci-dessous répertorie les différentes sources d'interférences haute fréquence.

Type	Sources	Effets des EMI
Transitoires	Foudre Défauts à la terre Défauts de commutation dans les circuits inductifs (bobines de chantier, électrovannes, etc.)	Dysfonctionnement des équipements à proximité
Décharge électrostatique	Entre une personne et un objet Entre des objets chargés électrostatiquement Pour exemple, échange d'électrons entre le corps et un tissu lorsqu'une personne marche sur un tapis ou entre le corps et des vêtements portés par un opérateur assis sur une chaise.	Dysfonctionnement des équipements à proximité Destruction éventuelle des équipements

Le tableau suivant récapitule les différentes méthodes de réduction des EMI pour les interférences basse fréquence et haute fréquence.

Mesures préventives pour les phénomènes basse fréquence	Mesures préventives pour les phénomènes haute fréquence
Systèmes de protection Filtrage Longueurs de câble appropriées	Liaison équipotentielle des parties conductrices exposées (interconnexions) Routage correct des câbles Sélection de câbles de qualité Connexions adaptées aux conditions de basse fréquence Blindage des câbles
Les systèmes de protection sont extrêmement importants.	Les pratiques d'installation sont extrêmement importantes.

Activités de normalisation des connecteurs en cuivre

Activités en cours

Le sous-comité SC 48B de la CEI est chargé de la normalisation des connecteurs électriques, sur la base des exigences établies par les différents comités de la CEI, tels que l'ISO/CEI JTC 1 SC 25 (normes pour les environnements de bureau et similaires) et son groupe de travail sur le câblage des locaux industriels. Ces groupes travaillent conjointement avec le sous-comité SC 65C (Communications numériques), regroupés en un groupe de travail mixte, appelé SC65C/JWG10.

La mission du groupe de travail SC65C/JWG10 consiste à définir les règles de câblage d'un réseau Ethernet dans des environnements industriels. Précisons qu'il existe déjà des normes spécifiant les caractéristiques des connecteurs. L'utilisation de ces connecteurs dans des applications Ethernet industriel reste toutefois à normaliser. Plusieurs organisations de réseau (Modbus-IDA, IAONA, PNO, ODVA) ont émis des recommandations sur le type de connecteurs en cuivre à utiliser dans les différents environnements industriels. A l'heure actuelle, il ne s'agit que de recommandations et non pas de normes.

Recommandations applicables aux connecteurs de l'industrie légère

Pour les environnements industriels légers, le marché a autorisé l'utilisation de connecteurs RJ45, conformément à la norme CEI 60603-7. Certaines organisations ont proposé l'usage de boîtiers de protection pour le RJ45 (définies par la norme CEI 61076-3-106). Cette proposition fait actuellement l'objet d'âpres discussions, du fait de l'existence de plusieurs modèles de connecteurs RJ45 étanches non compatibles. Ces boîtiers s'adaptent à une variété de dimensions d'assemblage (rondes ou rectangulaires), de mécanismes de fermeture (à vis, à baïonnette, à levier de blocage, pousser/tirer) et autres caractéristiques spéciales. Les variantes différentes ne sont pas assemblables.

Recommandations applicables aux connecteurs de l'industrie lourde

Pour les environnements industriels lourds, le choix semble s'orienter vers le connecteur circulaire M12, défini par la norme CEI 61076-2-101. Le type de connecteur M12 à utiliser reste encore à débattre, les Européens préférant le modèle à 4 broches au modèle à 8 broches en vigueur aux Etats-Unis. Les connecteurs à 4 broches sont plus répandus en Europe, pratique qui s'explique par l'utilisation de câbles à 2 paires dans les réseaux Ethernet européens, au lieu des câbles à 4 paires spécifiés par l'organisation de normalisation américaine des télécommunications, la TIA.

Conformité aux normes

Introduction

Pour le moment, il n'existe pas de norme internationale pour la planification et l'installation d'un réseau Ethernet industriel. Toutefois, des recommandations émises par des organisations Ethernet industriel ainsi que les activités continues ont conduit à la création d'un projet de norme. Cette norme devrait être publiée sous le nom ISO/CEI 24702 à la fin de 2006.

ISO/CEI 24702 et ISO/CEI 11801

Etant donné que le projet de norme ISO/CEI 24702 est basé sur la norme ISO/CEI 11801, les normes existantes peuvent être utilisées comme références jusqu'à la publication de la norme ISO/CEI 24702.

La norme ISO/CEI 11801 inclut les informations suivantes :

Thème	Chapitre (Clause)	Description
Structure du système de câblage générique	5	Décrit les éléments fonctionnels d'un système de câblage générique (répartiteur campus, répartiteur bâtiment, point de transition, etc.) et leur mode de connexion les uns aux autres.
Implémentation	6	Spécifie une conception de câblage qui, lorsqu'elle est correctement installée, est conforme aux exigences de la norme internationale. Cette section définit également les longueurs maximales.
Spécifications relatives aux voies et aux liaisons permanentes	7	Définit les exigences de performance des voies et des liaisons permanentes des systèmes de câblage générique installés. Cette section définit : ● les spécifications de performance du câblage de chaque voie et liaison permanente ; ● les spécifications de performance de deux différents types de support (câbles équilibrés et fibre optique) ; ● les voies et liaisons permanentes et leur classification (5 classes, la classe D étant adaptée à une application jusqu'à 100 MHz) ; ● les spécifications de performance de la liaison/voie en fonction de l'application (performances en matière d'impédance, de perte par retour, d'affaiblissement, etc.).
Exigences relatives aux câbles	8	Fournit les exigences relatives au câble utilisé dans les sous-systèmes de câblage de réseau fédérateur et horizontal.
Exigences relatives au matériel de connexion	9	Fournit des instructions et des exigences pour le matériel de connexion utilisé dans les systèmes de câblage générique.
Pratiques de blindage	10	Fournit des informations de base sur le blindage.
Administration	11	Explique les méthodes d'identification, d'enregistrement et de documentation d'un système de câblage générique.

La norme ISO/CEI 24702 finale empruntera les chapitres suivants à la norme ISO/CEI 11801 :

- Chapitre 7 – Classes de transmission des liaisons et des voies pour un câblage équilibré et à fibre optique.
- Chapitres 7, 8 et 9 – Performances de transmission des composants pour un câblage équilibré et à fibre optique.

Elle apportera également les informations suivantes, conformément aux exigences industrielles :

- modification des spécifications de structure de câblage de la norme ISO/CEI 11801, Chapitre 5 ;
- classification environnementale (la norme ISO/CEI 11801, Chapitre 10, contient des informations limitées à ce sujet.) ;
- composants appropriés ;
- nouveaux concepts éventuels.

Conformité des installations de câblage à la norme ISO/CEI 11801

La norme ISO/CEI 11801 définit la conformité des installations de câblage comme suit. Pour qu'une installation de câblage soit conforme à cette norme internationale, elle doit remplir les conditions suivantes :

- a** La configuration doit être conforme aux exigences stipulées à la clause 5.
- b** Les interfaces du câblage doivent être conformes aux exigences stipulées à la clause 9.
- c** Le système entier doit être composé de liaisons répondant au niveau de performance requis par la clause 7. Cela requiert donc l'installation de composants conformes aux exigences stipulées aux clauses 8 et 9, conformément aux paramètres de conception stipulés à la clause 6, ou la conception et l'implémentation d'un système garantissant le respect de la classe de performances stipulée à la clause 7 et des exigences de fiabilité stipulées à la clause 9.
- d** L'administration du système doit être conforme aux exigences stipulées à la clause 11.
- e** Les réglementations locales concernant la sécurité et la norme CEM doivent être respectées.

La norme ISO/CEI 11801 spécifie en outre :

Les performances de liaison stipulées à la clause 7 doivent être conformes à la clause 6 (installation). Les performances de liaison sont respectées lorsque les composants spécifiés aux clauses 8 et 9 sont installés de manière professionnelle et conformément aux instructions du concepteur et du fournisseur, sur des distances ne dépassant pas celles spécifiées à la clause 6. Dans ce cas, il n'est pas exigé de tester les caractéristiques de transmission de la liaison. La conformité aux spécifications à la clause 7 doit être testée dans les cas suivants :

- a. conception de liaisons avec des longueurs dépassant celles spécifiées à la clause 6 ;
- b. conception de liaisons avec des composants différents de ceux décrits aux clauses 8 et 9 ;
- c. évaluation du câblage installé afin de déterminer sa capacité à supporter un certain groupe d'applications ;
- d. vérification des performances, comme requis, d'un système installé conçu conformément aux clauses 6, 8 et 9.

Conformité du réseau Ethernet industriel Transparent Ready

Classes d'application

Les classes d'application sont définies par la norme ISO/CEI 11801. Chaque application possède une plage de fréquences propre, et à chaque plage d'application correspond une catégorie de câble recommandée. Le tableau ci-dessous répertorie chacune des classes avec son application associée et sa catégorie de câble recommandée.

Classe	Éléments inclus dans la classe d'application	Liaison permanente et voie	Catégorie ANSI/TIA/EIA-568
A	Applications de bande téléphonique et basse fréquence Liaisons permanentes et voies de câblage en cuivre Les applications de support Classe A font référence, respectivement, aux liaisons permanentes de classe A et aux voies de classes A.	Jusqu'à 100 kHz	-
B	Applications de données à débit binaire moyen Liaisons permanentes et voies de câblage en cuivre Les applications de support Classe B font référence, respectivement, aux liaisons permanentes de classe B et aux voies de classes B.	Jusqu'à 1 MHz	-
C	Applications de données à débit binaire élevé Liaisons permanentes et voies de câblage en cuivre Les applications de support Classe C font référence, respectivement, aux liaisons permanentes de classe C et aux voies de classes C.	Jusqu'à 16 MHz	Catégorie 3
D	Applications de données à débit binaire très élevé Liaisons permanentes et voies de câblage en cuivre Les applications de support Classe D font référence, respectivement, aux liaisons permanentes de classe D et aux voies de classes D.	Jusqu'à 100 MHz	Catégorie 5 (n'est plus reconnue par la TIA/EIA) Catégorie 5e (catégorie minimale recommandée pour toutes les nouvelles installations par : TIA/EIA, IEEE, Active Equipment Manufacturers).
Classe optique	Applications de données à débit binaire élevé et très élevé Liaisons permanentes et voies de câblage à fibre optique Les applications de support Classe optique font référence, respectivement, aux liaisons permanentes de classe optique et aux voies de classes optique.	Prévues pour supporter des applications à 10 MHz et au-delà	-

Longueurs de voie maximales

Le tableau ci-dessous répertorie les longueurs de voie maximales par catégorie de câble et par classe, conformément à la norme ISO/CEI 11801.

Longueurs de voie maximales ISO/CEI par catégorie de câble et par classe							
Support	Classe A	Classe B	Classe C	Classe D	Classe E	Classe F	Optique
CAT 3	2 km	200 m	100 m	-	-	-	-
CAT 4	3 km	260 m	150 m	-	-	-	-
CAT 5e	3 km	260 m	160 m	-	-	-	-
CAT 6	-	-	-	-	100 m	100 m	-
CAT 7	3 km	290 m	180 m	120 m	-	-	-
150 ohms	3 km	400 m	250 m	150 m	-	-	-
	-	-	-	-	-	-	-
Câble	-	-	-	-	-	-	-
62,5/125 et 50/125 mm	-	-	-	-	-	-	2 km
Fibre optique	-	-	-	-	-	-	-
Monomode	-	-	-	-	-	-	3 km

Les limites de performance des liaisons de classe D sont spécifiées à l'Annexe A des normes EN 50173:2002 et ISO/CEI 11801:2002. Les limites de mesure sont décrites dans la norme prEN 50346:2001.

Procédures de mise à la terre (masse)



Vue d'ensemble

Cette annexe décrit les procédures de mise à la terre (mise à la masse).

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Sujet	Page
Connexions de mise à la terre (masse) adéquates	548
Réalisation d'une connexion de terre	549
Options de connexion des blindages de câble	555
Procédures de test des réseaux Ethernet en cuivre	557
Paramètres de performance	558
Définition des paramètres de performance	560

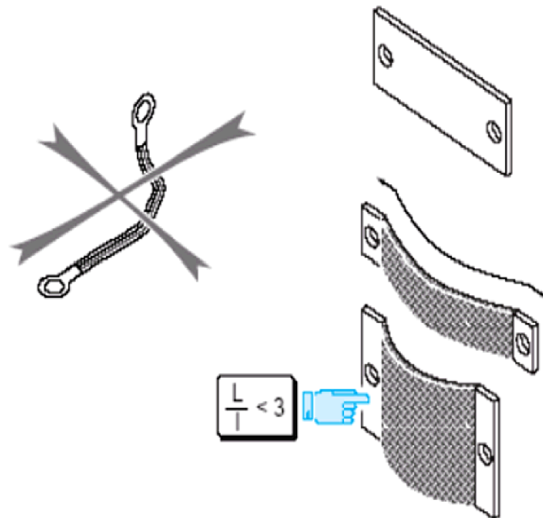
Connexions de mise à la terre (masse) adéquates

Introduction

Lorsque vous raccordez des structures et des équipements métalliques à un système de mise à la terre, la qualité des connexions de mise à la terre est déterminante pour la protection de vos équipements et leur compatibilité CEM. Les connexions de terre utilisent des bandes conductrices, des barres, des vis et des attaches de câble pour interconnecter les composants métalliques des machines, des équipements, des armoires, des blindages de câble et d'autres objets conducteurs à votre système de mise à la terre.

Type et longueur des connexions

Lorsque vous choisissez un type de connexion, les connexions de terre du châssis doivent à chaque fois être les plus courtes et les plus larges possible.



NOTE : Veillez à ce que les connexions soient correctement établies et à ce que les composants métalliques exposés soient correctement mis à la masse. Une connexion adéquate affichera les propriétés de conduction en basse et haute fréquence requises et garantira une durée de vie optimale de vos équipements.

Réalisation d'une connexion de terre

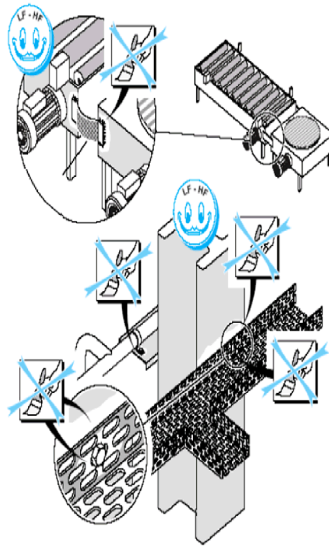
Introduction

Vous pouvez réaliser deux types de connexion de terre :

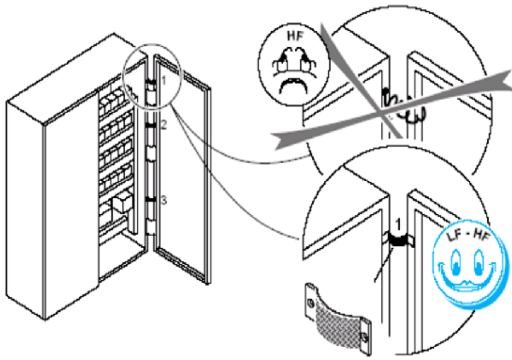
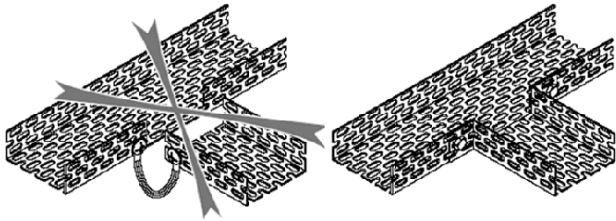
- entre deux surfaces métalliques ;
- entre un câblage blindé et une surface métallique.

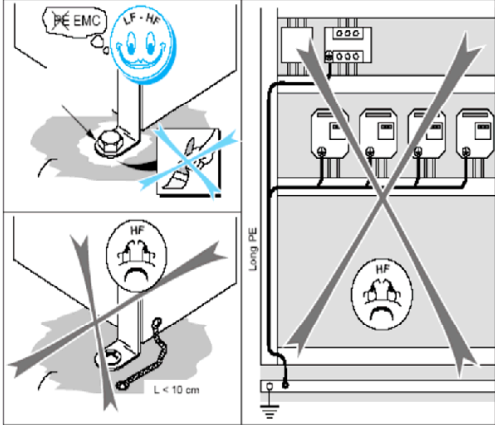
Réalisation d'une connexion entre deux surfaces métalliques

Assurez-vous que les plaques de plan de terre ne sont pas enrobées d'une couche de peinture ou de tout autre type de revêtement isolant. Ces matériaux empêchent le contact direct avec d'autres surfaces métalliques dans un système de mise à la terre :



Procédez comme suit pour réaliser une connexion compatible CEM entre deux surfaces métalliques.

Etape	Action	Commentaires
1	Sélectionnez des matériaux de connexion conducteurs appropriés pour obtenir un contact optimal. Utilisez des bandes torsadées ou des vis pour connecter les surfaces métalliques. Même si leur usage est déconseillé, des plaques ou des barres métalliques peuvent néanmoins être utilisées en l'absence de bandes torsadées. N'utilisez pas de conducteurs à fil jaune/vert.	Le schéma suivant illustre une connexion à bandes torsadées :  Le schéma suivant illustre une connexion à vis, écrou et rondelle : 
2	Préparez la surface pour les connexions métalliques au niveau de tous les points de contact. Retirez la peinture ou les revêtements isolants de la surface des points de contact métalliques.	Ceci inclut les surfaces entre deux connexions continues appariées, telles que deux barres ou feuilles métalliques plates.
3	Fixez les surfaces de connexion à l'aide de bandes torsadées ou d'écrous, de vis et de rondelles.	Assurez-vous que la connexion entre les surfaces en contact est bien ferme, en utilisant un système de vis à rondelle.

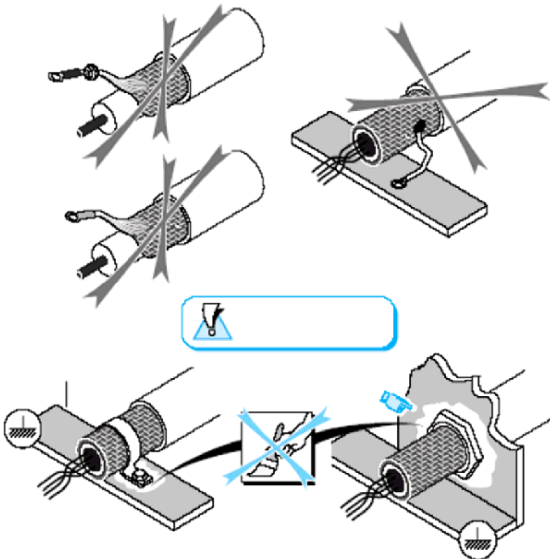
Etape	Action	Commentaires
4	Assurez-vous que tous les composants métalliques sont connectés entre eux et reliés à un système de mise à la terre.	Vérifiez de nouveau vos connexions afin de vous assurer qu'elles créent un système de mise à la terre local relié au connecteur de terre principal de votre bâtiment (voir page 106). 
5	Appliquez une couche de peinture ou de graisse sur les écrous et les vis au niveau de chaque point de contact, afin de les protéger contre la corrosion.	Maintenez la connexion tout le long.

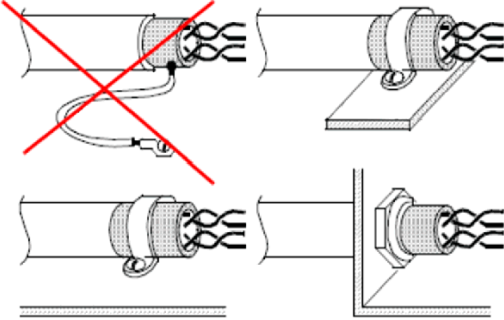
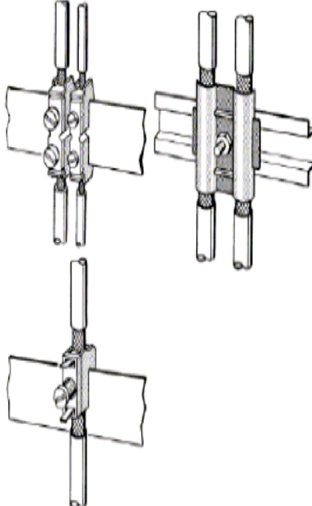
Remarques relatives aux connexions

- La peinture, les adhésifs frein-filet et le ruban Teflon agissent comme des matériaux isolants et empêchent un contact franc entre les surfaces métalliques aux points de connexion. Si une armoire ou une surface métallique, y compris la plaque du fond, est peinte, retirez la peinture avant de réaliser une connexion. Une fois la connexion effectuée, vous pouvez peindre les matériaux de connexion pour éviter toute corrosion.
- Assurez-vous que tous les composants et unités métalliques exposés qui se trouvent dans une armoire sont vissés directement sur la plaque de plan de terre.

Réalisation d'une connexion entre un blindage de câble et des surfaces métalliques

Etant donné que le réseau Ethernet fonctionne à des fréquences supérieures à 10 MHz, vous devez relier à la terre le blindage du câble à chaque extrémité, afin d'obtenir un maximum d'efficacité CEM. Si votre site ne dispose pas de liaison équipotentielle, vous pouvez réaliser une connexion à une seule extrémité et garantir un fonctionnement acceptable, mais pas aussi efficace. Procédez comme suit pour créer une connexion de qualité entre un blindage de câble et une surface métallique.

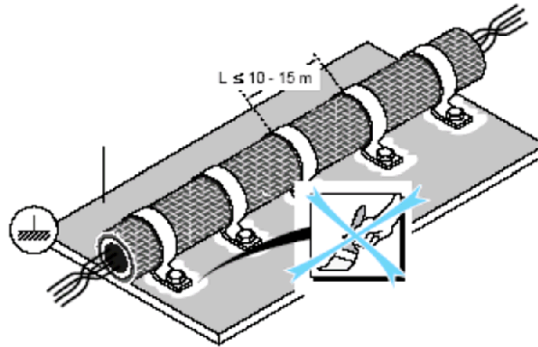
Etape	Action	Commentaires
1	Sélectionnez le câble approprié pour une installation Transparent Ready.	Schneider Electric vous recommande vivement d'utiliser un câble STP, de CAT5 minimum, pour toute installation Transparent Ready. Schneider Electric vous recommande également d'utiliser des connecteurs blindés sur les câbles, les équipements et les commutateurs.
2	Installez une barre omnibus de terre ou un plan de terre à raccorder au châssis sur lequel vous allez fixer le blindage de câble. Vous pouvez également fixer le blindage aux points d'entrée des armoires.	Assurez-vous qu'aucun revêtement isolant ou peinture ne recouvre la surface du plan sur lequel vous souhaitez fixer le câble. N'utilisez pas des cosse de câble soudées ou des fils de départ étamés pour connecter le blindage du câble. Si possible, essayez de connecter le blindage à une barre omnibus de terre ou au point d'entrée d'une armoire.  Dans tous les cas, assurez-vous d'avoir laissé une zone de contact intermétallique puissante tout autour du câble.
3	Vérifiez le câble afin de vous assurer que vous disposez d'un blindage continu d'une extrémité à l'autre.	Si le câble est endommagé ou le blindage entaillé, remplacez l'intégralité du câble.

Etape	Action	Commentaires
4	Otez la gaine plastique externe pour exposer la gaine interne du câble.	Un excellent contact intermétallique doit exister entre le blindage du câble maillé et la barre omnibus métallique ou le plan de terre. Pour réaliser une bonne connexion de terre, exposez le blindage de façon à ce qu'il ait une surface de contact de 360 degrés. 
5	Fixez le blindage de câble. Si possible, connectez le blindage de câble à une barre omnibus de terre ou au point d'entrée d'une armoire. Lorsque cela est possible, mettez les deux extrémités du câble à la terre en les fixant fermement à un plan de terre.	Veillez à ce que la connexion à l'extrémité du blindage fournisse une zone de contact intermétallique qui entoure entièrement la gaine. Vous pouvez utiliser des colliers de câbles métalliques pour fixer le blindage maillé et obtenir une zone de contact sur 360 degrés.  Vérifiez l'absence de couche de peinture ou de revêtement isolant entre les surfaces de contact.

Remarques relatives aux connexions

- Evitez d'utiliser des mauvaises connexions entre la gaine du câble et une barre omnibus métallique de terre ou un plan de terre.
- Retirez toute bande plastique isolante entre la couche de blindage du câble et la gaine.
- Evitez d'utiliser des blindages de câble trop longs. Le blindage perd de son efficacité si le câble est trop long. Pour optimiser l'efficacité du blindage, ajoutez plusieurs connexions intermédiaires vers la trame de mise à la terre.

Le schéma suivant illustre un câble avec de multiples connexions vers la trame de mise à la terre.



Options de connexion des blindages de câble

Méthodes de mise à la terre d'un blindage de câble

Il existe deux façons de mettre un blindage de câble à la terre :

- en créant des connexions de terre aux deux extrémités du câble ;
 - en créant des connexions de terre à une seule extrémité du câble.
- L'utilisation d'un câble blindé sans connexion de terre est déconseillée. En effet, sans mise à la terre, le blindage est peu efficace contre les champs magnétiques et les perturbations haute fréquence et basse fréquence. Tout contact avec le blindage du câble créerait alors une situation de danger, en raison de la différence de potentiel entre le blindage et la terre.

ATTENTION

Exposition à une basse tension.

La mise à la terre d'un blindage de câble à une seule extrémité crée une différence de potentiel entre le blindage et la prise de terre de l'extrémité non reliée.

- Evitez tout contact avec le blindage.

Le non-respect de ces instructions peut provoquer des blessures ou des dommages matériels.

Avantages et inconvénients

Le tableau ci-dessous décrit les avantages et les risques associés à chacune des deux méthodes de mise à la terre. Aidez-vous de ces informations pour choisir la méthode de mise à la terre la mieux adaptée à votre installation.

Méthode de mise à la terre	Avantages	Limites
Mise à la terre aux deux extrémités du câble	Extrêmement efficace contre les perturbations externes en haute et basse fréquence	Un courant de défaut à la terre peut être induit dans les signaux haute fréquence avec une forte interférence et intensité de champ, pour les câbles longs (>50 m).
	Très bonne protection contre la fréquence de résonance du câble	
	Aucune différence de potentiel entre le câble et la terre	
	Permet un placement courant des câbles alimentant des signaux de classe différente.	
	Très bonne suppression des perturbations haute fréquence	
Mise à la terre à une seule extrémité du câble	Efficacité moyenne du blindage	Inefficace contre les perturbations externes provoquées par des champs électriques de haute fréquence
	Protège les lignes isolées contre les champs électriques de basse fréquence	Le blindage peut créer une résonance à cause de l'effet d'antenne. Cela signifie que les perturbations sont plus importantes avec le blindage.
	Evite l'apparition de bourdonnement (perturbations basse fréquence)	

Boucles de terre des câbles blindés

L'un des risques de mise à la terre des blindages de câble aux deux extrémités est la création de boucles de terre. Celles-ci se créent lorsqu'un courant circule dans le blindage en raison de la différence de potentiel entre les deux extrémités du blindage. Pour les supprimer, vous devez obtenir le même potentiel aux deux extrémités. Si vous travaillez sur une installation existante, placez un conducteur de liaison parallèlement au câble du réseau. Pour les très longues distances, utilisez un câble à fibre optique.

Procédures de test des réseaux Ethernet en cuivre

Introduction

Les paragraphes qui suivent décrivent le processus de vérification des installations, comme le câblage et les longueurs appropriées, ainsi que les spécifications de référence pour les tests de performance définis au chapitre 7 de la norme ISO/CEI 11801.

Test des installations en cuivre

Testez chaque câblage en cuivre en vérifiant particulièrement :

- la terminaison correcte des broches à chaque extrémité ;
- la continuité à l'extrémité distante ;
- les courts-circuits entre deux ou plusieurs conducteurs ;
- les paires croisées ;
- les paires divisées ;
- les paires inversées ;
- les paires court-circuitées ;
- toute autre erreur de câblage.

Test des performances des installations en cuivre

Les spécifications de test des voies et des liaisons permanentes établies par la norme ISO/CEI 11801 sont les suivantes :

- Les performances d'une voie sont spécifiées aux interfaces et entre les interfaces avec la voie.
- Les performances d'une liaison permanente sont spécifiées aux interfaces et entre les interfaces avec la liaison.

La norme ISO/CEI 11801 spécifie également :

Les performances des liaisons sont satisfaites lorsque les composants spécifiés aux clauses 8 et 9 (de la norme ISO/CEI 11801) sont installés de manière professionnelle et conformément aux instructions du concepteur et du fournisseur, sur des distances ne dépassant pas celles spécifiées à la clause 6 (de la norme ISO/CEI 11801).

Paramètres de performance

Introduction

Les fournisseurs de composants et de câbles sont tenus, conformément à la norme ISO/CEI 11801, de publier les paramètres de performance de tous leurs produits. La norme stipule que chaque fournisseur de câbles et de composants doit présenter les paramètres des différents composants d'une liaison ou d'une voie permanente (dont les spécifications sont définies aux chapitres 8 et 9 de la norme ISO/CEI 11801). Les paramètres de performance spécifiés par la norme ISO/CEI 11801 s'appliquent aux liaisons et aux voies permanentes dotées d'éléments de câblage blindés ou non blindés (c'est-à-dire, avec ou sans blindage complet, sauf indication contraire). Les termes STP et UTP renvoient également au câblage symétrique. Les paramètres de performance sont définis pour 5 classes d'application. Par exemple, les applications de classes D concernent les liaisons et voies permanentes de classe D, spécifiées jusqu'à 100 MHz.

Paramètres de spécification et normes associées

Le tableau suivant répertorie tous les paramètres proposés et/ou requis pour les tests avec leurs normes associées. Les normes principales pour les réseaux Ethernet industriel sont spécifiées dans les deux dernières colonnes.

Norme	ISO/CEI 11801-2000	TIA/EIA 568B	ISO/CEI 11801-2000+	Amendement à TIA/EIA 568-B
Etat	Approuvé	Approuvé	Projet	Projet
Plage de fréquence par classe ou catégorie	Cl. C : 16 MHz Cl. D : 100 MHz	CAT 3 : 16 MHz CAT 5e : 100 MHz	Cl. C : 16 MHz Cl. D : 100 MHz Cl. E : 250 MHz Cl. F : 600 MHz	CAT 3 : 16 MHz CAT 5e : 100 MHz CAT 6 : 250 MHz
Affectation des fils	x	x	x	x
Longueur		x		x
Temps de propagation	x	x	x	x
Différence des temps de propagation	x	x	x	x
Pertes d'insertion (affaiblissement)	x	x	x	x
Perte PP NEXT	x	x	x	x
Perte PS NEXT	x	x	x	x
PP ACR	x			
PS ACR	x			
PP ELFEXT	x	x	x	x
PS ELFEXT	x	x	x	x
Perte par retour	x	x	x	x
Résistance cc	x		x	

Liste des paramètres

Les paramètres suivants sont requis pour les tests et la mesure des performances des liaisons et des voies permanentes de câblage symétrique :

- Impédance nominale (*voir page 560*)
- Perte par retour (*voir page 560*)
- Affaiblissement (*voir page 560*)
- Perte paradiaphonique paire à paire (*voir page 561*)
- Paradiaphonie cumulée (*voir page 562*)
- Rapport affaiblissement sur diaphonie paire à paire (*voir page 562*)
- Rapport affaiblissement sur diaphonie cumulée (*voir page 562*)
- Ecart télédiaphonique paire à paire (*voir page 563*)
- Ecart télédiaphonique cumulé (*voir page 563*)
- Résistance cc de la boucle (*voir page 563*)
- Temps de propagation (*voir page 563*)
- Différence des temps de propagation (*voir page 563*)
- Perte de conversion longitudinale à différentielle (*voir page 563*)
- Impédance de transfert du blindage

Définition des paramètres de performance

Introduction

Ce sous-chapitre décrit chacun des paramètres de spécification définis dans la norme ISO/CEI 11801.

Impédance nominale

L'impédance est la mesure du degré de résistance d'un composant face au flux d'énergie provenant d'une source donnée. L'impédance d'un câble est un facteur important, car il détermine la charge placée sur la source ainsi que le rendement de la transmission du signal. Un moyen simple de définir l'impédance nominale consiste à mesurer un composant qui ne réfléchit pas l'énergie vers la source de transmission. Lorsqu'un système de transmission détecte l'impédance nominale comme étant sa charge, toute l'énergie qu'il transmet est absorbée par l'extrémité réceptrice. Si, au contraire, il ne détecte pas l'impédance nominale, une partie de l'énergie est renvoyée. Dans un système idéal, toute l'énergie transmise est absorbée par l'extrémité réceptrice. L'impédance est mesurée en Ohms (Ω).

Perte par retour

La perte par retour est une mesure de l'énergie réfléchie due au défaut d'adaptation de l'impédance dans le système de câblage. Si le système qui transmet l'énergie ne détecte pas d'impédance égale à l'impédance nominale, une partie de l'énergie est alors réfléchie (autrement dit, l'extrémité réceptrice renvoie une partie de l'énergie). Dans ce cas, il existe un écho du signal transmis. La perte par retour est mesurée en décibels ou en pourcentage d'intensité du signal.

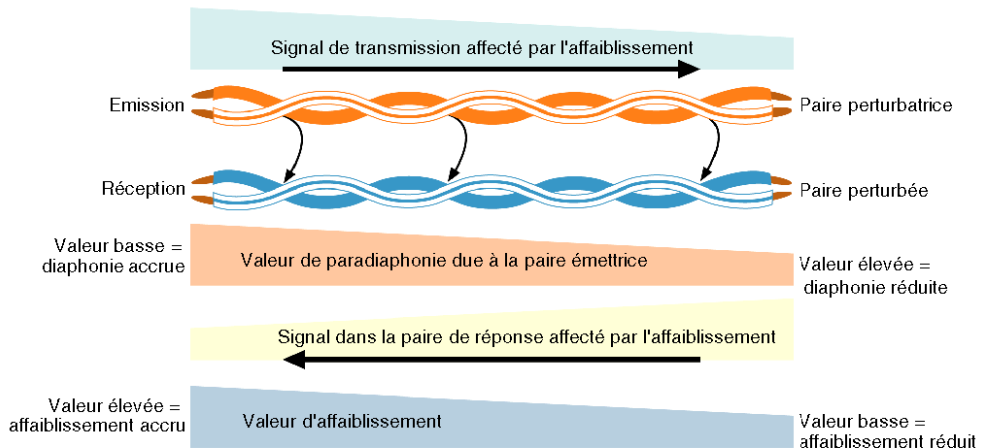
Affaiblissement (perte d'insertion)

L'affaiblissement est la perte d'intensité du signal au fur et à mesure de sa traversée le long du câble. Il est mesuré en décibels (dB). Une valeur d'affaiblissement basse est satisfaisante : plus l'affaiblissement est faible, plus le signal est fort. L'affaiblissement dépend de la longueur du câble et de la fréquence. Il augmente lorsque la longueur du câble ou la fréquence augmente. Il est également affecté par le calibre du câblage. Des câbles épais affichent un affaiblissement plus faible que des câbles fins. Les problèmes d'affaiblissement qui apparaissent sont généralement dus à l'utilisation de câbles fins, de mauvaises terminaisons ou de câbles trop longs. L'affaiblissement augmente également avec la température.

Perte paradiaphonique paire à paire (PP NEXT)

La paradiaphonie est le couplage d'un signal émis par une paire (la paire perturbatrice) vers une autre paire (la paire perturbée), mesuré à l'extrémité où le signal est injecté (l'extrémité proche). Elle équivaut à la proportion du signal transmis dans la paire perturbatrice qui est électromagnétiquement couplée dans la paire perturbée. Elle est mesurée dans la paire perturbée au niveau de l'extrémité émettrice. La paradiaphonie est mesurée en décibels (dB). Une valeur de paradiaphonie élevée est satisfaisante, car elle révèle un fort affaiblissement d'une paire à l'autre. La paradiaphonie varie avec la fréquence et doit donc être mesurée dans une plage de fréquences donnée.

La figure ci-dessous représente un exemple de valeurs de paradiaphonie et d'affaiblissement



La figure illustre deux paires Ethernet, l'une émettrice et l'autre réceptrice. Lorsque la paire émettrice est alimentée, elle génère une diaphonie vers la paire réceptrice. A l'extrémité proche, le signal dans la paire réceptrice est au niveau le plus bas et donc davantage sensible à l'effet de la paradiaphonie. Dès que la valeur de paradiaphonie augmente, la valeur de l'affaiblissement augmente également.

Des câbles à paire torsadée ont été développés afin d'empêcher l'apparition de diaphonie et de permettre aux champs opposés de s'annuler. Un nombre de torsades élevé fournit une meilleure annulation et permet au câble de supporter une fréquence plus élevée. Il arrive souvent que la paradiaphonie d'une liaison ou d'une voie permanente décroisse (indiquant que la diaphonie augmente), en raison d'une mauvaise terminaison d'installation des câbles. Pour connecter un câble à un équipement, vous devez détordre le câble pour accéder aux fils. Les fils non tordus favorisent la diaphonie. Pour minimiser la diaphonie, conservez autant que possible la torsion des paires de câble lors de la terminaison des câbles et de leur connexion au matériel.

Paradiaphonie cumulée (PS NEXT)

La paradiaphonie cumulée est la somme de toutes les combinaisons de paires pour la diaphonie mesurée à l'extrémité proche vers l'émetteur et simule le fonctionnement des quatre paires simultanément. Elle équivaut à la cumulation des effets paradiaphoniques des trois paires perturbatrices dans la quatrième paire, vu de l'extrémité proche. Ce paramètre est destiné aux systèmes utilisant plus de deux paires. La paradiaphonie cumulée varie en fonction de la fréquence et doit donc être mesurée dans une plage de fréquences donnée.

Rapport affaiblissement sur diaphonie paire à paire (PP ACR)

Le rapport atténuation sur diaphonie correspond à la différence entre la paradiaphonie et l'affaiblissement dans la paire testée. La formule est la suivante :

$$ACR = \text{Paradiaphonie} - \text{Affaiblissement}$$

C'est à l'extrémité proche que la paradiaphonie (avec une valeur minimale) et l'affaiblissement (avec un niveau d'affaiblissement maximal et un niveau de signal minimal) sont les plus forts. La définition du rapport affaiblissement sur diaphonie est analogue à celle du rapport signal sur bruit. (Le rapport affaiblissement sur diaphonie ne tient pas compte de l'effet du bruit externe susceptible d'affecter la transmission du signal.)

Rapport affaiblissement sur diaphonie cumulée (PS ACR)

Le rapport affaiblissement sur diaphonie cumulée est un calcul mathématique qui simule le fonctionnement des quatre paires simultanément. La formule est la suivante :

$$PSACR = \text{Paradiaphonie cumulée} - \text{Affaiblissement}$$

Etant donné que le rapport affaiblissement sur diaphonie cumulée équivaut à un rapport signal sur bruit mesuré, une valeur élevée (davantage de signal et moins de bruit) est préférable à une valeur basse (davantage de bruit et moins de signal).

Télédiaphonie (FEXT)

La télédiaphonie s'apparente à la paradiaphonie. La paire perturbatrice envoie le signal depuis l'extrémité proche, comme pour la paradiaphonie, mais celui-ci est ensuite mesuré dans la paire perturbée au niveau de l'extrémité éloignée. Le signal dans la paire perturbatrice est plus faible à l'extrémité éloignée, en raison de l'affaiblissement. Etant donné que la valeur de télédiaphonie est liée à l'affaiblissement du câble, elle est généralement mesurée pour obtenir l'écart télédiaphonique, mais non reportée.

Ecart télédiaphonique paire à paire (PP ELFEXT)

L'écart télédiaphonique est un calcul mathématique obtenu en soustrayant l'affaiblissement de la paire perturbatrice de la mesure de télédiaphonie. Cette paire induit une paire adjacente. La formule est la suivante :

$$ELFEXT = \text{Télédiaphonie} - \text{Affaiblissement}$$

Ecart télédiaphonique cumulé (PS ELFEXT)

L'écart télédiaphonique cumulé est la somme des valeurs des effets d'écart télédiaphonique générés sur chaque paire par les trois autres paires. Elle équivaut au calcul utilisé pour obtenir la paradiaphonie cumulée. Le calcul utilisé pour mesurer l'écart télédiaphonique ne tient pas compte de l'affaiblissement sur la télédiaphonie.

Résistance cc de la boucle

La résistance cc de la boucle équivaut à la résistance totale passant par deux conducteurs bouclés à une extrémité de la liaison. Elle est généralement fonction du diamètre des conducteurs et varie uniquement avec la distance. Cette mesure est parfois effectuée pour éviter tout ajout conséquent de résistance à la liaison dû aux erreurs de connexions globales.

Temps de propagation

Le temps de propagation est la mesure du temps mis par un signal pour se propager d'une extrémité à l'autre du circuit. Il est mesuré en nanosecondes (ns). La présence de ce temps de propagation a entraîné l'institution d'une limitation de longueur sur les câblages de réseaux LAN. Dans la plupart des applications réseau, telles que celles basées sur CSMA/CD, il existe un délai maximal pouvant être pris en charge sans risque de perte de communication.

Différence de temps de propagation

La différence de temps de propagation est la différence entre le temps de propagation d'un signal sur la paire la plus rapide et celui sur la paire la plus lente, dans un câble ou un système de câblage UTP.

Perte de conversion longitudinale à différentielle (équilibrage)

La transmission des signaux dans des câbles à paire torsadée suppose que les signaux sur chaque fil par rapport à la prise de terre soient équilibrés. Cela signifie que, sur toute la longueur du câble, le signal sur l'un des fils d'une paire torsadée, mesuré par rapport à la prise de terre, est exactement identique en amplitude mais aussi exactement opposé en phase au signal sur l'autre fil de la même paire torsadée.

Dans de telles conditions idéales, aucun signal RF ne serait émis de la paire (aucune interférence de radiofréquence et électromagnétique), et le couplage à l'intérieur de la liaison serait réduit. La paradiaphonie normale est le résultat du couplage d'un signal différentiel appliqué à une paire et détecté comme signal en mode différentiel à l'entrée réceptrice. D'autres mécanismes de couplage, générés lorsque le signal n'est pas appliqué de façon purement différentielle, incluent le couplage mode différentiel à mode commun, le couplage mode commun à mode différentiel et le couplage mode commun à mode commun. Ces mécanismes de couplages peuvent être sources de paradiaphonie excessive. Par conséquent, ce paramètre permet de définir le degré d'équilibrage du signal appliqué par le testeur à l'entrée de la liaison.

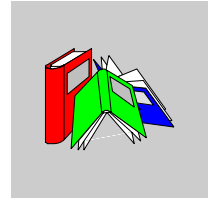
Valeurs de paramètres pour le câble CAT5 conformes à ISO/CEI 11801

Le tableau ci-dessous répertorie les paramètres de spécification et leurs valeurs de classe D pour les liaisons et les voies réseau.

Paramètre	Liaison permanente Classe D	Voie permanente Voie D
Fréquence (présentée à 100 Mhz à mesurer de préférence dans la plage 1 à 100 Mhz)	100 MHz	100 MHz
Affaiblissement maximal	20,6 dB	24 dB
NEXT minimum	29,3 dB	27,1 dB
PS NEXT minimum	26,3 dB	24,1 dB
ACR minimum	8,7 dB	3,1 dB
PS ACR minimum	5,7 dB	0,1 dB
ELFEXT minimum	19,6 dB	17,0 dB
PS ELFEXT minimum	17,0 dB	14,4 dB
Perte par retour minimale	17 dB	17 dB
Temps de propagation maximal	489,6 ns	547,6 ns
Différence de temps de propagation maximale	43 ns	50 ns
Perte de conversion longitudinale à différentielle minimale	La mesure de ces valeurs sur systèmes installés n'est pas encore parfaitement établie. Une vérification des valeurs à la conception est suffisante.	La mesure de ces valeurs sur systèmes installés n'est pas encore parfaitement établie. Une vérification des valeurs à la conception est suffisante.

Paramètre	Liaison permanente classe D
Résistance de boucle maximale (ohms)	40 Ω

Glossaire



0-9

100BaseT4

Ethernet 100 Mb/s fonctionnant sur quatre paires torsadées non blindées de catégorie 3, 4 ou 5.

10Base-F

Ethernet 10 Mb/s sur fibre optique. 10BASE-F est un support réseau point à point, par exemple entre un concentrateur/commutateur et une station.

10Base-T

Ethernet 10 Mb/s fonctionnant sur câbles à paire torsadée non blindée. 10BASE-T est un support réseau point à point, par exemple entre un concentrateur/commutateur et une station.

10Base2

Ethernet 10 Mb/s sur un câble réseau coaxial fin.

10Base5

Ethernet 10 Mb/s sur un câble réseau coaxial épais.

802

Spécifications IEEE pour les réseaux locaux (LAN, Local Area Network) et les réseaux métropolitains (MAN, Metropolitan Area Network).

802.1

Spécifications IEEE pour la gestion générale et les opérations entre réseaux, comme le pontage.

802.2

Spécifications IEEE qui définissent des normes au niveau de la sous-couche de contrôle des liaisons logiques de la couche de liaison de données.

802.3

Normes CSMA/CD (Ethernet) qui s'appliquent à la couche physique et la sous-couche MAC.

802.4

Spécifications IEEE pour les bus de transmission de jeton.

802.5

Spécifications IEEE pour l'anneau à jeton.

802.6

Spécifications IEEE pour les réseaux métropolitains (MAN). Les normes IEEE 802 sont devenues les normes ANSI et sont généralement reconnues comme normes internationales.

A

accès distant

Accès à des ressources réseau qui ne se trouvent pas sur le même Ethernet physique, ce dernier renvoyant à la topologie réseau d'un site global.

ack - numéro d'acquittement

Un expéditeur transmet un message dans le code **ack** d'acquittement pour signaler que la réception s'est déroulée sans erreurs.

adaptateur RIO

Remote Input/Output CRP (processeur de communication vers les équipements distants)

adressage sans classe

Voir CIDR.

adressage X-Way

Mécanisme d'adressage (au niveau de la couche réseau) pour le protocole Uni-TE. Il permet l'interconnexion de plusieurs réseaux ou segments Ethway, Ethernet TCP/IP et/ou Fipway. Sur un réseau TCP/IP Ethernet, l'adressage X-Way et IP sont utilisés ensemble.

adresse IP

Adresse 32 bits associée à une station de travail connectée à Internet avec le protocole TCP/IP.

adresse MAC

Adresse de *contrôle de l'accès au support* d'un équipement, qui est gravée dans une carte DNI et qui est ajoutée au début du paquet.

adresse matérielle

Voir adresse réseau.

adresse physique

Adresse identifiant un nœud unique.

adresse réseau

Chaque nœud d'un réseau possède au moins une adresse, avec au moins une adresse de matériel fixe attribuée par le fabricant de l'équipement. La plupart des nœuds ont une adresse spécifique au protocole affectée par un gestionnaire du réseau.

algorithme de l'arbre recouvrant

Algorithme utilisé par des ponts pour créer une topologie logique qui connecte tous les segments réseau et assurer qu'il n'existe qu'un seul chemin entre deux stations.

anneau

Topologie de réseau dans laquelle les nœuds sont connectés dans une boucle fermée. Les données passent d'un nœud à l'autre dans la boucle, toujours dans la même direction.

anneau à jeton

Réseau informatique dans lequel une configuration de bits, appelée jeton, est transmise sur un anneau (topologie circulaire) d'ordinateurs pour éviter la collision de données entre deux ordinateurs qui tentent d'envoyer un message en même temps.

ARP

(*Address Resolution Protocol, protocole de résolution d'adresses*) Cache composé d'une table mettant en correspondance des adresses IP et des adresses de matériels.

ATM

(*Asynchronous Transfer Mode, mode de transfert asynchrone*) Technologie de transfert rapide de la voix, des vidéos et des données sur un réseau.

AUI

(*Attachment Unit Interface, interface d'unité de rattachement*) Câble Ethernet à paire torsadée blindée 15 broches utilisé pour connecter des équipements réseau et une unité de raccordement à un support (telle qu'un émetteur-récepteur).

auto-négociation/auto-détection

Capacité d'un équipement (au niveau de la sous-couche MAC) d'identifier la vitesse (10 ou 100 Mb/s) et le mode full duplex ou semi-duplex d'une connexion et de la régler, conformément à la clause 28 de la norme IEEE 802.3u.

B

bande passante

Plage de fréquences qu'une transmission peut transporter. La capacité d'une voie numérique se mesure en bits par seconde (bits/s).

bits/s

Bits par seconde, unité de vitesse de transmission.

BNC

(*Bayonet Neill Concelman*) Connecteur standard utilisé pour relier un coaxial fin 10Base2 à un émetteur-récepteur.

BootP

(*Bootstrap Protocol*) Protocole réseau TCP/IP qui fournit aux nœuds du réseau des informations de configuration à partir d'un nœud serveur BOOTP.

BRI

(*Basic Rate Interface*) Des deux niveaux de services RNIS, il s'agit de celui destiné à un usage résidentiel et aux petites entreprises. Cette interface comporte deux voies B à 64 Kips et une voie D à 16 Kbps pour un service total de 128 Kbps.

bus

Topologie LAN dans laquelle tous les nœuds sont connectés à un câble unique. Les nœuds sont tous jugés égaux et tous reçoivent les transmissions sur le support.

C

câble à fibre optique

Support de transmission composé de deux fibres optiques en verre (ou en plastique) qui transmet des signaux numériques sous la forme d'impulsions lumineuses modulées à partir d'un laser ou d'un voyant. Il se présente comme un fin filament de verre, d'un diamètre global généralement compris entre 125 et 140 μm .

En raison de sa grande bande passante et d'une résistance élevée aux interférences, le câble à fibre optique est utilisé dans des liaisons à grande distance ou à fort bruit parasite.

câble à paire torsadée

Câble peu onéreux, composé de plusieurs conducteurs, comprenant une ou plusieurs paires de brins de cuivre de 18 à 24 AWG. Les brins sont tressés afin d'améliorer la protection contre les interférences radio et électromagnétiques. Ce câble, qui peut être blindé ou non, est utilisé pour les communications peu rapides, par exemple comme câble téléphonique. Il est utilisé uniquement dans des réseaux à bande de base, en raison de l'étroitesse de la bande passante.

câble coaxial

Câble électrique composé d'un fil conducteur solide en son centre, entouré de matériaux isolants et d'un écran conducteur métallique externe ayant le même axe de courbure que le conducteur interne.

câble d'émetteur-récepteur

Câble qui relie un équipement à un segment Ethernet standard ou à coaxial fin.

câble de dérivation

Câble qui permet la connexion et l'accès au câble principal dans un réseau, également appelé *câble AUI (Attachment Unit Interface)* ou *câble émetteur-récepteur*.

câble épais

câble coaxial d'un diamètre de 12 mm (un demi-pouce).

câble fin

Câble coaxial similaire à celui utilisé pour le raccordement de télévisions ou d'équipements vidéo.

CBN

(*Common Bonding Network*) Composants métalliques interconnectés qui comprennent un système de mise à la terre dans un bâtiment. On parle également de *circuit de mise à la terre intégré*.

CENELEC

Comité Européen de Normalisation en Electrotechnique situé à Bruxelles.

certification de câble UL

En collaboration avec plusieurs fabricants, la société Underwriters Laboratories (UL) a mis au point un programme d'évaluation des niveaux de performances applicables aux transmissions de données. Cette approbation apparaît sur les câbles comme indiqué ci-dessous :

Niveau I - performances adaptées aux communications de base et aux câbles à bas débit.

Niveau II - les exigences de performances sont similaires à celles d'un câble de type 3 (câble de communication multipaire) décrit dans le document IBM Cabling System Technical Interface Specification (GA27-3773-1). Ces exigences s'appliquent aux câbles blindés de 2 à 25 paires.

Niveau III - les câbles de données sont conformes aux exigences de transmission décrites dans le document EIA/TIA Wiring Standard pour les câbles UTP (Unshielded Twisted Pair, paire torsadée non blindée) horizontaux et aux exigences de catégorie 3 décrites dans la norme EIA/TIA 568A. Ces exigences s'appliquent à la fois aux câbles blindés et non blindés.

Niveau IV - les câbles de niveau IV sont conformes aux exigences décrites dans la norme National Electrical Manufacturer's Association (NEMA) pour les câbles de télécommunications à faibles pertes. Les exigences sont similaires à celles de la catégorie 4 de la norme EIA/TIA 568A. Ces exigences s'appliquent à la fois aux constructions de câbles blindés et non blindés.

Niveau V - les câbles de niveau V sont conformes aux exigences décrites dans la norme National Electrical Manufacturer's Association (NEMA) pour les câbles de télécommunications à faibles pertes et à large étendue de fréquence. Les exigences du Niveau V sont similaires à celles de la catégorie 5 de la norme EIA/TIA 568A. Ces exigences s'appliquent à la fois aux constructions de câbles blindés et non blindés.

checksum

Vérification de redondance qui consiste le plus souvent à additionner des octets afin de détecter des erreurs dans un message.

CIDR

(Classless Inter-Domain Routing, routage interdomaine sans classe). Egalement appelé adressage sans classe ou supernetting. Méthode souple pour allouer des adresses IP avec le moins de pertes possibles.

collision

Résultat de deux nœuds réseau transmettant sur la même ligne en même temps. Les données transmises ne sont pas utilisables et les stations doivent renouveler l'envoi. Un mécanisme de retard employé par les deux stations réduit les risques d'une autre collision.

commutateur

Équipement Ethernet multiport conçu pour accroître les performances du réseau en n'autorisant que le trafic important sur les segments Ethernet reliés. Les paquets sont filtrés ou transférés en fonction de leur adresse source et de destination.

commutation de circuits

Maintien en activité d'un commutateur uniquement pendant que l'expéditeur et le récepteur sont en communication.

commutation de groupe de travail

Configuration dans laquelle un certain nombre d'utilisateurs est connecté à un réseau Ethernet via un commutateur. La commutation permet à chaque utilisateur de bénéficier d'un meilleur débit qu'avec un concentrateur.

concentrateur

Équipement concentrant le câblage dans un réseau à topologie en étoile.

concentrateur (hub)

Centre d'un réseau à topologie en étoile ou d'un système de câblage. Topologie d'un réseau multinœud qui comprend un multiplexeur central avec de nombreux nœuds qui y accèdent ou qui en partent. Les autres nœuds ne sont généralement pas interconnectés directement. Les concentrateurs LAN sont de plus en plus nombreux en raison du développement des fibres optiques et des paires torsadées ainsi que des besoins de gestion LAN.

concentrateur de câblage intelligent

Concentrateur réseau qui permet la prise en charge de plusieurs supports et leur gestion depuis un point central. Lorsqu'ils prennent en charge des systèmes de câblage structurés, les concentrateurs intelligents assurent la gestion des ports.

concentrateurs de commutation

Systèmes de commutation Ethernet intelligents qui interconnectent plusieurs réseaux locaux (LAN) Ethernet et des LAN plus rapides tels que ceux du type FDDI.

connecteur en T

Dispositif en forme de T doté de deux connecteurs femelles et d'un connecteur BNC mâle.

connecteur RJ

(*Registered Jack*) Type de connecteur utilisé avec les paires torsadées UTP/STP, par exemple, RJ45.

connecteur TAP

Composant physique qui permet de connecter un équipement ou une nouvelle section de câble à un câble principal.

ConneXium

Famille d'équipements et de solutions Ethernet de Schneider.

contrôle distant

Forme d'accès distant où un équipement en accès entrant prend le contrôle d'un autre nœud du réseau. Toutes les séquences de touches sur le dispositif distant sont traduites en séquences de touches spécifiques du nœud réseau. Ce type de contrôle est essentiellement utilisé avec le protocole IPX.

couche

Dans le domaine des réseaux, les couches sont les niveaux d'un protocole logiciel qui constituent l'architecture du réseau, chaque couche exécutant des fonctions pour la ou les couches situées au-dessus.

couche de contrôle physique

Couche 1 du modèle d'architecture de réseau SNA.

couche de liaison de données

Couche 2 du modèle de référence OSI (qui en contient sept), réservée aux communications entre les ordinateurs d'un réseau. Cette couche définit des protocoles pour les paquets de données et la manière dont ils sont transmis entre chaque équipement du réseau. Il s'agit d'un mécanisme de communication de niveau liaison, indépendant du support, qui se superpose à la couche physique ; elle est divisée en deux sous-couches : la couche de contrôle d'accès au support (MAC, Medium-Access Control) et la couche de liaison logique (LLC, Logical-Link Control).

couche physique

La couche 1 (niveau inférieur) du modèle de référence OSI est mise en œuvre par la voie physique. Elle régit les connexions matérielles et le codage du flux d'octets à transmettre. Elle est la seule couche faisant intervenir un transfert physique d'informations entre les nœuds du réseau. La couche physique isole la couche 2 (liaison des données) des caractéristiques physiques dépendant du support telles que transmission sur bande de base, large bande ou fibre optique. La couche 1 définit les protocoles qui régissent le support de transmission et les signaux.

coupe-feu

Routeur ou station de travail qui comporte plusieurs interfaces réseau et qui contrôle et limite certains protocoles, des types de trafic au niveau de chaque protocole, des types de services, ainsi que le sens du flux des informations.

CRC

(*Cyclical Redundancy Check, contrôle de redondance cyclique*) Technique qui consiste à vérifier si un message contient des erreurs, en exécutant des calculs mathématiques sur le nombre de bits du message, les résultats étant envoyés avec les données au destinataire. Ce dernier refait les calculs sur les données reçues. En cas de différence entre les deux calculs, le destinataire demande à l'expéditeur de transmettre à nouveau les données.

CSMA/CD

(*Carrier Sense Multiple Access with Collision Detection*) Méthode d'accès aux supports Ethernet et IEEE 802.3. Tous les équipements réseau se partagent l'accès aux supports pour la transmission. Si un dispositif détecte le signal d'un autre équipement en train de transmettre, il abandonne la transmission et effectue une nouvelle tentative après un certain temps.

CSU/DSU

(*Channel Service Unit/Data Service Unit, unité de service de voie/unité de service numérique*). Evite les interférences électriques pendant la transmission/la réception de signaux depuis/vers le WAN.

cut-through

Technique d'examen des paquets entrants selon laquelle un commutateur Ethernet ne vérifie que les quelques premiers octets d'un paquet avant de le transmettre ou de le filtrer. Ce processus est plus rapide que l'examen complet du paquet mais il arrive aussi qu'il laisse passer des paquets défectueux.

D

datagramme

Moyen d'envoyer des données dans lesquelles certaines parties du message sont transmises dans un ordre aléatoire, que la machine destinataire remet dans le bon ordre.

DCF

Système de signaux horaires précis envoyés depuis un émetteur situé près de Francfort (Allemagne), utilisé pour les synchronisation du temps.

DCOM

Distributed Component Object Model, modèle objet distribué) Extension du mode COM (Component Object Model), le protocole DCOM est utilisé pour permettre à deux machines distantes de communiquer. Il remplace les protocoles de communication inter-processus par des protocoles réseau. Il s'agit d'une norme Microsoft Windows.

débit IP

(Internal Protection) Décrit le degré de protection des circuits internes des capteurs.

délai de segment

Temps nécessaire à un signal pour aller d'une extrémité du segment à l'autre.

détection de collisions

Signal indiquant que d'autres stations se disputent la transmission sur la station locale. Le signal est envoyé par la couche physique à la couche de liaison de données sur un nœud Ethernet/IEEE 802.3. Avec Ethernet, chaque équipement peut détecter les collisions et tente de renvoyer le signal. La technologie CSMA/CD est basée sur ce principe.

DHCP

Dynamic Host Configuration Protocol, protocole de configuration d'hôte dynamique) Protocole de communication qui attribue des adresses IP aux équipements d'un réseau, sur la base du protocole BootP.

diaphonie

Bruit véhiculé entre des câbles de communication ou les éléments d'un équipement. Le signal de paradiaphonie est mesuré à proximité du point où le bruit parasite est introduit. Le signal de télédiaphonie est introduit à une extrémité et mesuré à l'autre.

diffusion générale

Message envoyé à tous les équipements du réseau.

DO

(Device Outlet) Prise équipement

domaine de diffusion

Ensemble d'équipements qui reçoivent un message de diffusion générale envoyé sur un réseau Ethernet. Le domaine de diffusion se termine par un routeur installé dans le réseau. Si un équipement du domaine diffuse des informations, celles-ci sont reçues par tous les équipements du même domaine ; en revanche, elles ne sont pas reçues par les équipements connectés via un routeur.

dongle

Câble réseau court qui connecte un adaptateur PCMCIA à un câble réseau.

DSL

(*Digital Subscriber Line, ligne d'abonné numérique*) Connexion Internet à grande vitesse qui utilise les câbles téléphoniques normaux.

DVMRP

(*Distance Vector Multicast Routing Protocol*) Protocole de routage utilisé pour gérer la multidiffusion basée sur la distance, mesurée en sauts de routage, et qui permet de déterminer le chemin optimal de diffusion d'un paquet.

E

E/S

(*Entrées/Sorties*) Transfert de données depuis et vers un ordinateur.

EGP

(*Exterior Gateway Protocol, protocole de passerelle externe*) Permet l'échange d'informations de routage, notamment des tables de routage, entre deux hôtes d'un réseau.

émetteur-récepteur

Équipement réseau capable à la fois de transmettre et de recevoir des messages. Il sert d'interface entre un équipement utilisateur et un réseau et peut donc activement convertir des signaux entre le réseau et le nœud local.

EMI

(*Electromagnetic Interference, interférence électromagnétique*) Se produit en cas de dysfonctionnement ou de détérioration d'un équipement suite à l'émission d'un champ magnétique par un autre équipement voisin.

en-tête

Informations de contrôle ajoutées au début d'un message transmis. Il contient des informations essentielles telles que l'adresse du paquet ou du bloc, la source, la destination, le numéro de message, la longueur et les instructions de routage.

encapsulation

Le fait d'envelopper un ensemble de données dans un en-tête de protocole, par exemple des données Ethernet emballées dans un en-tête Ethernet spécifique avant de transiter sur le réseau.

Désigne aussi une méthode de pontage pour des réseaux différents, où une trame entière provenant d'un réseau est simplement incluse dans l'en-tête utilisé par le protocole de la couche liaison de l'autre réseau.

envoi en différé

Technique permettant d'examiner les paquets entrants sur un commutateur ou un pont Ethernet et de lire en entier chaque paquet avant de le transmettre ou de le filtrer. L'envoi en différé est légèrement plus lent que le processus cut-through, mais il offre la garantie que tous les paquets erronés ou mal alignés sont supprimés du réseau par l'équipement de commutation.

EOS

(*Ethernet over SONET/SDH*) Transfère des signaux Ethernet dans SONET/SDH.

ERP

(*Enterprise Resource Planning, progiciel de gestion intégré*) Système logiciel pour entreprise qui gère la planification, la fabrication et les ventes et peut également inclure des modèles de finance et de gestion des ressources humaines.

Ethernet

Réseau local à bande de base CSMA/CD, à 10 ou 100 Mb/s, qui peut utiliser des câbles coaxiaux fins, épais, à paire torsadée ou à fibre optique. La norme IEEE 802.3 définit les règles de configuration d'un réseau Ethernet.

Ethernet commuté

Concentrateur Ethernet avec une fonctionnalité intégrée de commutation ou de pontage de la couche MAC, qui offre à chaque port une bande passante de 10 Mb/s. Des transmissions séparées peuvent se dérouler sur chaque port du concentrateur de commutation. Le commutateur filtre le trafic en fonction de l'adresse MAC de destination.

Ethernet partagé

Configuration Ethernet dans laquelle un certain nombre de segments sont reliés dans un même domaine de collision. Les concentrateurs fournissent ce type de configuration, la transmission n'étant assurée que par un seul nœud à la fois.

F

FDDI

(*Fiber-Distributed Data Interface*) Norme ANSI pour l'utilisation de la fibre optique en vue de transmettre des données sur le réseau à des vitesses allant jusqu'à 100 Mb/s.

Initialement définie pour les lignes à fibre optique, la norme FDDI est également utilisable sur des câbles à paire torsadée de courte distance (on parle également de *CDDI*).

FDR

(*Faulty Device Replacement*) Remplacement d'équipements défectueux

fichier d'application STU

Extension de fichier de projet pour le logiciel Unity Pro

fichier de symboles XVM

Extension de fichier des variables exportées depuis Unity Pro, utilisée par OFS.

filtrage

Dans un environnement Ethernet, processus selon lequel un commutateur ou un pont lit le contenu d'un paquet et, s'il estime qu'il n'est pas nécessaire de transférer ce dernier, le supprime. La *vitesse de filtrage* est la vitesse à laquelle un équipement reçoit des paquets et les supprime sans perdre de paquets entrants et sans générer de retard de traitement.

FOIRL

(*Fiber Optic Inter-Repeater Link*) Technique de gestion des signaux basée sur la norme IEEE 802.3 régissant les fibres optiques.

fragment

Dans un environnement Ethernet, élément d'un paquet qui a été décomposé en petites unités.

fragmentation

Division d'un paquet en petites unités lors de son transfert sur un support du réseau qui ne prend pas en charge la taille d'origine du paquet.

FTP

(File Transfer Protocol, protocole de transfert de fichiers) Protocole TCP/IP pour le transfert de fichiers.

FTP

(Foil Twisted Pair, paire torsadée à blindage général) Câble constitué de deux brins conducteurs enroulés l'un autour de l'autre pour réduire la diaphonie et entouré d'une feuille protectrice d'aluminium.

full duplex

Mode dans lequel un équipement ou une ligne est capable de transmettre des données de manière indépendante et simultanée dans les deux sens.

G**gestion du réseau**

Services d'administration d'un réseau, qui englobent la configuration et la mise au point, la gestion des opérations réseau, la surveillance des performances et le diagnostic des problèmes du réseau.

GMRP

(GARP Multicast Registration Protocol, protocole d'enregistrement générique GARP) Système permettant la multidiffusion des données. Des stations terminales reçoivent les données envoyées au groupe de multidiffusion pour lequel elles sont enregistrées.

Gopher

Protocole réseau qui permet la recherche et l'extraction de documents et utilise une structure de menus pour aller chercher les informations sur Internet.

GPS

(Global Positioning System, système de positionnement global) Système de satellites et d'équipements de réception utilisés pour calculer une position sur la Terre.

H

homologation UL

Désigne un équipement ou un composant testé et approuvé par l'organisme Underwriters Laboratories, Inc.

hôte

Généralement, nœud d'un réseau utilisable de manière interactive, c'est-à-dire auquel on peut se connecter, comme à un ordinateur.

HSBY

(Hot Standby System, système de redondance d'UC) Ce système est basé sur deux automates programmables industriels configurés de manière identique, reliés l'un à l'autre et au même réseau d'E/S distantes ; si un contrôleur tombe en panne, l'autre prend le contrôle du système d'E/S.

HTML

(*Hypertext Markup Language, langage de balisage hypertexte*) Code utilisé pour écrire des pages Web.

HTTP

(*Hyper Text Transfer Protocol, protocole de transfert hypertexte*) Protocole employé pour transmettre des fichiers sur le Web.

hystérésis

Tant que le seuil maximum ou minimum pour la valeur d'une variable n'est pas dépassé, le signal servant à avertir les autres systèmes d'un changement d'état est supprimé.

I

ICMP

(*Internet Control Message Protocol, protocole de contrôle des messages sur Internet*) Cette extension du protocole IP permet de tester une connexion sur Internet à l'aide de la commande *ping*. ICMP prend en charge des paquets de données avec des messages d'erreur, de contrôle et d'information.

IEC

CEI - Commission électrotechnique internationale (Genève)

IEEE 802.3

Norme *Institute of Electrical and Electronic Engineers* qui définit la méthode d'accès au support CSMA/CD et les spécifications des couches physique et de liaison de données d'un réseau local. Elle inclut notamment les mises en œuvre Ethernet 10BASE2, 10Base5, 10Base-FL et 10Base-T.

IGMP

(Internet Group Management Protocol, protocole de gestion de groupes Internet)
Norme Internet de multidiffusion qui permet à un hôte de souscrire à un groupe de multidiffusion spécifique.

IHM

(Interface Homme-Machine) Ecran d'un équipement dont la conception rend son utilisation intuitive.

InterBus

Norme de communication ouverte qui permet la mise en place d'un réseau à grande vitesse pour connecter des modules d'E/S, des capteurs, des actionneurs et des équipements de contrôle à des automates programmables industriels ou à des gros ordinateurs.

interconnexion de réseaux

Terme général décrivant l'activité consistant à utiliser différents produits et technologies pour mettre des réseaux en relation.

Internet

Ensemble de réseaux locaux, régionaux, nationaux et internationaux interconnectés par le biais du protocole TCP/IP. Internet relie de nombreux sites gouvernementaux, universitaires et de recherche. Il offre des services de messages, de connexion à distance et de transfert de fichiers.

ISDN (RNIS)

(Integrated Services Digital Network, Réseau Numérique à Intégration de Services ou RNIS) Ensemble de normes pour la transmission numérique sur des câbles téléphoniques en cuivre.

ISP (FAI)

(Internet Service Provider, Fournisseur d'Accès à Internet ou FAI)

J

jabber

Erreur réseau qui survient lorsqu'une carte d'interface transmet des données corrompues sur le réseau.

Il s'agit également d'une condition d'erreur due à la transmission par un nœud Ethernet de paquets de données d'une longueur supérieure à la valeur autorisée.

JVM

(Java Virtual Machine, machine virtuelle Java) Exécute du code Java compilé. La machine virtuelle se situe au-dessus du système d'exploitation.

L

LAN

(Local Area Network, réseau local) Système de communication de données composé d'un groupe d'ordinateurs interconnectés partageant des applications, des données et des équipements. La zone géographique couvre généralement un bâtiment ou un groupe de bâtiments.

latence

Dans un environnement Ethernet, délai qui sépare, au niveau d'un équipement de commutation ou de pontage, la réception et l'envoi de la trame.

liaison

Connexion physique entre deux nœuds d'un réseau. Il peut s'agir d'un circuit de communication de données ou d'une connexion directe par voie (câble).

liaison de données

Connexion logique entre deux nœuds d'un même circuit.

liaison logique

Connexion temporaire entre des nœuds source et destinataire ou entre deux processus d'un même nœud.

liaison RIO

Communications réseau qui passent par les équipements RIO (Remote Input/Output).

LLC

(*Logical Link Control, contrôle de liaison logique* ou *Link Layer Control, contrôle de la couche de liaison*) Protocole de liaison de données basé sur HDLC, développé pour des réseaux locaux par le Comité IEEE 802 et commun à toutes les normes LAN pour la transmission de liaison de données (partie supérieure de la couche 2 du modèle ISO).

LNI

(*Local Network Interconnect*) Concentrateur ou multiplicateur de ports qui prend en charge plusieurs équipements ou contrôleurs de communication actifs, soit de manière autonome, soit rattaché à un câble Ethernet standard.

LS

(*Low Smoke*) Désigne un câble à faible émission de fumée toxique en cas d'incendie.

M**MAC**

(*Media Access Control, contrôle de l'accès au support*) Expression générique désignant la manière dont les stations de travail accèdent au support de transmission. Plus généralement utilisée en référence aux réseaux locaux.

MAN

(*Metropolitan Area Network, réseau métropolitain*) Réseau qui couvre une zone géographique plus grande que celle d'un réseau local mais moins important que celle d'un réseau étendu. IEEE 802.6 spécifie les protocoles et le câblage pour un réseau MAN. Cependant, il est possible de les remplacer par un mode de fonctionnement asynchrone (ATM).

mappage de diffusion générale d'interface

Propriété mappant le taux de trafic à diffusion générale passant par chaque port des commutateurs gérés.

MAU

(*Medium Attachment Unit, unité de rattachement à un support*) Equipement utilisé pour convertir des signaux passant d'un support Ethernet à un autre. Un émetteur-récepteur est une unité MAU.

MES

(*Manufacturing Execution System, système intégré d'exécution de fabrication*) Système informatisé facilitant la gestion des données et des communications au niveau du flux de production.

MIB

(*Management Information Base, base d'informations de gestion*) Base de données des paramètres réseau utilisée par les protocoles SNMP (Simple Network Management Protocol) et CMIP (Common Management Information Protocol) pour surveiller et modifier les paramètres des équipements du réseau. Elle fournit la liste des noms logiques de toutes les ressources et informations du réseau concernant la gestion de ce dernier.

MICE

(Mechanical, Ingress, Climatic, Environmental) Travail de standardisation internationale réalisé par un groupe d'experts de IEC TC65, TIA TR-42.9 et CENELEC TC215 WG1 afin de définir des normes environnementales pour l'Ethernet industriel.

micrologiciel

Système d'exploitation (OS) d'un équipement

MII

(*Media-Independent Interface, interface indépendante du support*) Norme IEEE 802.3u pour Fast Ethernet. MII est l'équivalent Fast Ethernet de AUI dans l'Ethernet 10 Mb/s. Il permet la connexion de différents types de supports Fast Ethernet à un équipement Fast Ethernet via une interface commune.

mise à jour de routage

Message envoyé depuis un routeur pour indiquer l'accessibilité du réseau et les informations de coût associées. Les mises à jour de routage sont généralement envoyées à intervalles réguliers et après une modification de la topologie du réseau.

MMF

(*Multi-Mode Fiber, fibre multimode*) Câble qui transporte la lumière au lieu d'impulsions électriques. Ce type de câble est utilisé pour des connexions point à point uniquement, sur une longueur maximale de 2 km. Il représente le meilleur type de câble à utiliser entre deux bâtiments.

modèle de référence OSI

Modèle d'architecture à sept couches pour les protocoles de communication de données, mis au point par les organismes ISO et CCITT. Chaque couche décrit des fonctions réseau spécifique comme l'adressage, le contrôle du flux, le contrôle des erreurs, l'encapsulation et le transfert fiable de messages.

modèle en couches ISO

L'*ISO (International Standards Organization)* est l'organisation internationale de normalisation qui définit les normes pour les ordinateurs et les communications. Son modèle d'interconnexion de systèmes ouverts (OSI, Open Systems Interconnection) spécifie la manière dont des équipements informatiques différents tels que des cartes NIC, des ponts et des routeurs échangent des données sur un réseau. Le modèle comprend sept couches. Celles-ci sont, du bas vers le haut : physique, liaison de données, réseau, transport, session, présentation et application. Chaque couche effectue des services destinés à la couche supérieure.

MPLS

Multiprotocol Label Switching, commutation multiprotocole par étiquette Intègre des informations de la couche 2 dans la couche 3, de façon à permettre le routage du trafic même en cas de problèmes sur les systèmes.

MSTR

Bloc fonction utilisé pour la programmation.

MT-RJ

Nouveau connecteur standard pour des câbles optiques.

MTU

(*Maximum Transmission Unit, unité de transmission maximale*) La plus grande taille de paquet d'un réseau peut transmettre (mesurée en octets). La taille est définie par l'administrateur du réseau et peut différer d'un réseau à l'autre. Les paquets les plus grands sont divisés avant d'être envoyés, mais cette opération réduit la vitesse de transmission.

multidiffusion

Envoi d'un message par un hôte à plusieurs équipements du réseau.

Forme spéciale de diffusion dans laquelle des copies du paquet ne sont transmises qu'à un sous-ensemble de toutes les destinations possibles.

multiplicateur de ports

Concentrateur qui connecte plusieurs équipements à un réseau.

N

Nano

Plate-forme d'automates entrée de gamme de Schneider.

NFS

(Network File System, système de fichiers réseau) Protocole pour le partage de fichiers entre des hôtes UNIX.

NIC

(Network Interface Card, carte d'interface réseau) Carte adaptateur insérée dans un ordinateur qui contient le logiciel et les éléments électroniques nécessaires pour permettre à la station de communiquer sur le réseau.

NMS

(Network Management System, système de gestion de réseau) Gestionnaire, inclus dans le protocole SNMP, qui peut interroger les agents, en obtenir des réponses et définir des variables dans ces derniers.

NTP

(Network Time Protocol, protocole de synchronisation horaire) Protocole TCP utilisé pour synchroniser l'heure sur les équipements d'un réseau. Il utilise des signaux émis par des horloges radios et atomiques.

nœud

Tout équipement intelligent connecté au réseau, y compris des serveurs terminaux, des ordinateurs hôtes et des équipements tels que des imprimantes et des terminaux qui sont directement rattachés au réseau. Un nœud est en quelque sorte un équipement ayant une adresse matérielle.

nœud distant

Forme d'accès distant où l'équipement en accès entrant se comporte comme un équipement homologue sur le réseau cible. Ce type de contrôle est essentiellement utilisé avec les protocoles IP et IPX.

O**OEM**

(Original Equipment Manufacturer, fabricant de matériel informatique d'origine)
L'OEM, ou équipementier, construit des ordinateurs en gros, les personnalise avec certaines applications et les revend sous son propre nom.

OLE

(Object Linking and Embedding, liaison et incorporation d'objets) Système logiciel Microsoft qui permet à des applications Windows de déplacer et de partager des informations.

OPC

Spécification pour le contrôle des processus et l'automatisation de la fabrication ; définit des normes pour des objets, des méthodes et des interfaces.

OSI

(Open Systems Interconnect/Interconnection, interconnexion de systèmes ouverts)
Structure permettant d'interconnecter des ordinateurs hétérogènes pour le traitement d'applications distribuées conformément aux normes internationales.

OSPF

(Open Shortest Path First) Protocole de routage de type Link-State (état de liaison), dans lequel chaque nœud de commutation (routeur) transmet une carte complète des connexions réseau servant à calculer le saut optimal suivant d'un routeur vers le suivant.

P

paquet

Série de bits contenant des données et des informations de contrôle, mises en forme pour être transmises d'un nœud à un autre. Il inclut un en-tête avec une trame de départ, les adresses source et destination, des données de contrôle, le message lui-même et un code de fin avec des données de contrôle d'erreur (appelé *séquence de vérification de trame*).

passerelle

Combinaison d'éléments matériels et logiciels interconnectant des réseaux ou des équipements réseau qui, à défaut, seraient incompatibles. Les passerelles incluent des assembleurs/désassembleurs de paquets (PAD, Packet Assembler/Disassembler) et des convertisseurs de protocole. Elles opèrent au niveau des couches 5, 6 et 7 (session, présentation et application) du modèle OSI.

PCMCIA

(*Personal Computer Memory Card International Associates*) Développeurs d'une norme pour une carte d'équipement informatique permettant d'ajouter de la mémoire, d'utiliser un modem/fax ou d'utiliser un disque dur portable.

perte

On parle également de perte de signal. Atténuation ou dégradation d'un signal durant une transmission.

perte de signal

Voir *perte*

ping

(*Packet Internet Groper*) Pour tester le réseau, tapez *ping.exe* au niveau de la ligne de commande pour essayer d'atteindre une destination avec une demande d'écho ICMP et attendre une réponse.

point à point

Circuit connectant deux nœuds uniquement, ou configuration nécessitant une connexion physique distincte entre chaque paire de nœuds.

pont

Équipement qui connecte deux réseaux locaux (LAN) et qui transmet ou filtre des paquets de données entre les deux en fonction de leurs adresses de destination. Les ponts interviennent au niveau de la liaison de données (ou couche MAC) du modèle de référence OSI, et ils sont transparents pour les protocoles et pour les équipements de niveau supérieur tels que les routeurs.

Les ponts connectent des réseaux qui utilisent des protocoles différents et qui opèrent au niveau de la liaison de données ou de la couche 2 du modèle OSI. Ils sont souvent présentés comme des ponts du niveau Contrôle de l'accès au support (couche MAC, Media-Access Control). Ils n'interprètent pas les informations qu'ils transportent. Lorsque deux réseaux locaux (LAN) sont correctement reliés par un pont, ils forment un réseau local unique. Différentes techniques d'équilibrage de la charge ont été mises au point pour remédier aux problèmes de limitation de la bande passante et de panne d'éléments sur le réseau. Les ponts sont de plus en plus utilisés pour contrôler le trafic réseau afin que le reste du réseau ne soit pas affecté. Ils améliorent les performances du réseau et s'avèrent utiles pour la sécurité.

pont de routage

Pont de la couche MAC qui utilise la couche réseau pour déterminer la topologie d'un réseau.

pont-routeur

Équipement qui achemine des protocoles spécifiques, tels que TCP/IP et IPX, et connecte d'autres protocoles, combinant les fonctions à la fois des routeurs et des ponts.

pont/routeur

Équipement qui assure les fonctions d'un pont ou d'un routeur, ou les deux simultanément. Un pont/routeur peut acheminer un ou plusieurs protocoles, tels que TCP/IP et/ou XNS et servir de pont pour tous les autres types de trafic.

port

Connecteur physique sur un équipement permettant d'établir la connexion.

PPP

(Point-to-Point Protocol, protocole point à point) Protocole qui fournit des connexions de routeur à routeur ou d'hôte à réseau, aussi bien sur des circuits synchrones qu'asynchrones. Succède au protocole SLIP.

PRI

(*Primary Rate Interface*) Des deux niveaux de services RNIS, il s'agit de celui destiné aux grandes entreprises. Cette interface comporte 23 voies B et une voie D à 16 Kbps (aux Etats-Unis) ou 30 voies B et une voie D (en Europe).

protocole

Toute méthode standard de communication sur un réseau.

protocole de routage

Protocole qui met en œuvre un algorithme de routage spécifique.

protocole UMAS

Unified Messaging Application Protocol, protocole unifié d'applications de messagerie Permet de rassembler tous les supports de messagerie dans une seule interface.

Q

QoS

(*Quality of Service, Qualité de Service*) Spécification de performance utilisée pour mesurer et améliorer la qualité des transmissions et la disponibilité des services dans un système de communication.

R

Rapid Spanning Tree (Arbre recouvrant rapide)

(*RSTP*) Enrichissement du protocole Spanning Tree qui diminue le temps de convergence ; il réduit le temps de reconfiguration et accélère ainsi la reprise des services. Voir *Spanning Tree*.

RARP

(*Reverse Address Resolution Protocol, protocole de résolution inverse d'adresse*) Protocole utilisé pour convertir une adresse d'interface matérielle en adresse de protocole.

RAS

(*Remote Access Server/Service, serveur/service d'accès à distance*) Serveur qui permet un accès distant à un réseau local (LAN), le plus souvent par le biais d'une ligne téléphonique.

redondance

Duplication de composants critiques afin d'accroître la fiabilité.

relais de trame

Protocole utilisant la commutation de paquets pour connecter des équipements sur un réseau WAN.

répéteur

Équipement réseau qui connecte un segment Ethernet à un autre au sein du même réseau local. Le répéteur transmet des signaux dans les deux sens entre les segments. Il amplifie les signaux électriques, régénère l'en-tête de chaque paquet, développe les fragments de paquet et exécute une auto-segmentation ainsi qu'une reconnexion automatique sur les ports présentant des collisions continues.

répéteur multiport

Répéteur, autonome ou relié à un câble Ethernet standard, qui relie un maximum de huit segments Ethernet sur câble fin.

réseau

Système d'ordinateurs interconnectés qui peuvent communiquer entre eux et partager des fichiers, des données et des ressources.

réseau à commutation de circuits

Réseau qui établit provisoirement un circuit physique, jusqu'à réception d'un signal de déconnexion.

réseau à commutation de paquets

Réseau dans lequel les données sont transmises dans des paquets. Les paquets peuvent être acheminés individuellement sur la meilleure connexion réseau disponible et réassemblés au point de destination de façon à constituer le message complet.

réseau fédérateur

Câble principal du réseau.

réseau LAN virtuel commuté

Réseau logique comportant plusieurs domaines d'émulation de réseaux LAN différents et contrôlé par une application de gestion de réseau intelligente.

réseau local à bande de base

Réseau local qui utilise une fréquence porteuse unique sur un seul canal. Ethernet utilise une transmission sur bande de base.

RIP

(Routing Information Protocol, protocole d'informations de routage) Protocole de routage qui s'appuie sur le vecteur distance pour calculer en nombre de sauts le chemin optimal de diffusion d'un paquet.

RMON

(*Remote Monitoring, surveillance à distance*) Sous-ensemble du protocole SNMP. MIB II offre des fonctionnalités complètes et flexibles de surveillance et de gestion grâce à la prise en charge de 10 groupes d'informations.

RMON MIB

(*Remote Monitor Management Information Base, base d'informations de gestion de surveillance à distance*) Base d'informations contenant neuf niveaux (Ethernet) de présentation de statistiques pour la gestion d'un réseau.

routage

Processus de transmission d'un message sur un ou plusieurs réseaux par le chemin le plus approprié. Bien que simple dans son principe, le routage s'appuie sur une technique complexe et spécialisée dans laquelle interviennent de nombreux facteurs. Plus les réseaux sont reliés entre eux, plus la complexité du routage risque d'augmenter.

routeur

Équipement assurant le filtrage et le transfert de paquets sur la base des informations de la couche de liaison de données. Alors que le pont ou le commutateur peut uniquement lire les adresses de la couche MAC pour les filtrer, le routeur peut lire des données telles que des adresses IP et les acheminer en conséquence.

Contrairement aux ponts, les routeurs opèrent au niveau 3 (couche réseau) du modèle OSI. Par ailleurs, ils sont spécifiques à un protocole et agissent sur des informations de routage transportées par le protocole de communication dans la couche réseau. Les ponts transmettent les paquets de la couche 2 (liaison de données) directement au segment suivant d'un réseau local, tandis que les routeurs peuvent utiliser des informations sur la topologie du réseau et choisir ainsi la meilleure route pour l'envoi d'un paquet de la couche 3. Les routeurs intervenant au niveau 3, ils sont indépendants de la couche physique et sont utilisables pour relier différents types de réseau. Ils doivent pouvoir échanger des informations entre eux afin de connaître les conditions du réseau et de déterminer les liaisons actives et les nœuds disponibles.

RTPS

(Real-Time Publish-Subscribe, publication-souscription en temps réel) Norme permettant de transférer des données et des états sur des protocoles peu fiables comme UDP/IP.

S**SASL**

(Simple Authentication and Security Layer, couche de sécurité et d'authentification simple) Utilisé pour identifier et authentifier un utilisateur auprès d'un serveur, ce protocole peut aussi protéger les transmissions en fournissant une couche de sécurité.

saut de routeur

Chemin parcouru entre un routeur et le suivant. Tous les paquets de données spécifient après combien de sauts le paquet sera supprimé et un message d'erreur envoyé à la source de données.

SCADA

(Supervisory Control and Data Acquisition) Logiciel qui, relié à un automate programmable industriel, permet l'acquisition et l'analyse d'informations utilisées pour surveiller et contrôler un équipement commercial.

ScTP

(*Screen Twisted Pair, paire torsadée écrantée*) Câble constitué de deux conducteurs enroulés l'un autour de l'autre pour réduire la diaphonie, d'un blindage tressé tel qu'un câble STP et d'une tresse externe supplémentaire pour accroître la protection.

SDH

(Synchronous Digital Highway) Norme de signaux utilisée dans la transmission numérique.

segment

Dans un environnement Ethernet, partie de bus présentant une continuité électrique. Il est possible de relier des segments à l'aide de répéteurs ou de ponts.

segmentation

Dans un environnement Ethernet, division d'un anneau surchargé en deux ou trois anneaux distincts, reliés par un pont/un routeur ou par un concentrateur universel.

segmentation LAN

Division de la bande passante du *réseau local* en plusieurs LAN indépendants de façon à améliorer les performances.

semi-duplex

Mode de transmission des données qui peut s'effectuer dans les deux directions sur une même ligne, mais dans un seul sens à la fois.

serveur

Ordinateur qui contient des ressources à partager sur le réseau, telles que des fichiers (serveur de fichiers) ou des terminaux (serveur de terminaux).

serveur d'impression

Ordinateur dédié qui gère des imprimantes et des demandes d'impression provenant d'autres nœuds du réseau.

serveur de communication

Système autonome dédié qui gère les communications pour d'autres ordinateurs.

serveur de fichiers

Ordinateur qui stocke des données pour les utilisateurs du réseau et permet un accès réseau à ces données.

serveur de noms

Logiciel qui s'exécute sur les hôtes réseau chargés de convertir des noms de type texte en adresses IP numériques.

serveur de terminaux

Concentrateur qui facilite les communications entre des hôtes et des terminaux.

serveur/service DNS

(*Domain Name Server/Service, serveur/service de noms de domaines*) Service qui convertit un nom de domaine en adresse IP, cette dernière constituant l'identifiant unique d'un équipement du réseau.

services synchrones

L'application cliente qui appelle un service en lecture ou en écriture ne peut pas effectuer d'autres demandes tant qu'elle n'a pas obtenu de réponse à la première.

services Transparent Ready

Solutions Schneider visant à optimiser la distribution électrique, le contrôle industriel et les performances des automatismes.

session

Connexion à un service réseau.

SLIP

(*Serial-Line Internet Protocol, protocole Internet sur ligne série*) Protocole pour l'exécution TCP/IP sur des lignes série.

SMF

(*Single-Mode Fiber, fibre monomode*) Fibre avec un cœur de petit diamètre (environ 3 μm) et une gaine dont l'indice de réfraction est très proche de celui du cœur. Elle transmet les rayons lumineux qui pénètrent selon un angle de dispersion très étroit sur une très large bande passante. La fibre SMF a un diamètre relativement étroit qui ne permet la propagation que d'un seul mode. Elle offre une bande passante plus importante que la fibre MMF, mais nécessite une source de lumière de faible largeur spectrale.

SMS

(Short Message Service, service de messages courts) Messages de texte composés de 160 caractères maximum, qu'il est possible d'envoyer sur un équipement sans fil.

SMTP

(Simple Mail Transfer Protocol) Norme Internet utilisée pour envoyer et recevoir des messages électroniques.

SNA

(Systems Network Architecture, architecture de réseau systèmes) Protocoles en couche d'IBM pour les communications sur des gros systèmes.

SNMP

(Simple Network Management Protocol) Protocole en trois parties comprenant : une structure d'informations de gestion (SMI), une base d'informations de gestion (MIB) et le protocole lui-même. La SMI et la MIB définissent et stockent l'ensemble des entités gérées : le protocole SNMP proprement dit véhicule les informations vers et depuis ces entités. La norme du domaine public est basée sur l'expérience opérationnelle des travaux Internet TCP/IP au sein des réseaux DARPA/NSFnet.

Hôte TCP/IP exécutant une application SNMP pour interroger d'autres nœuds et obtenir des données relatives au réseau et connaître les conditions d'erreur. Les autres hôtes, qui fournissent des agents SNMP, répondent à ces requêtes et permettent à un seul hôte de collecter des statistiques depuis les nombreux autres nœuds du réseau.

SNP

(Sub-Network Protocol) Protocole TCP/IP résidant dans la couche de sous-réseau, sous IP. Il assure le transfert des données dans le sous-réseau local. Dans certains systèmes, un module adaptateur doit être inséré entre IP et le protocole SNP pour rendre les interfaces compatibles.

SNTP

(Simple Network Time Protocol) Version simplifiée du protocole NTP, utilisée pour synchroniser les horloges des systèmes informatiques.

SOAP

(Simple Object Access Code) Protocole simplifié d'accès aux objets.

socket

Identificateur unique composé d'une adresse IP et d'un numéro de port correspondant au point terminal d'une communication dans un système ou une application.

SONET

(*Synchronous Optical Network, réseau optique synchrone*) Norme de signaux utilisée dans la transmission numérique.

sous-réseau

Partie interconnectée mais séparée d'un réseau, qui partage une adresse réseau avec d'autres parties de celui-ci. Le sous-réseau est utilisé à des fins de sécurité et de performances.

spanning tree (arbre recouvrant)

(STP) Technique qui détecte les boucles dans un réseau et bloque de façon logique les chemins redondants, afin qu'il n'existe qu'une route entre deux réseaux LAN. Elle est utilisée dans les réseaux à pont régis par la norme IEEE 802.1d. Voir *Rapid Spanning Tree*.

SQL

(*Structured Query Language, langage de requête structuré*) Langage utilisé pour interroger une base de données relationnelles.

SSID

(*Service Set Identifier*) Séquence de 32 lettres ou chiffres placée dans l'en-tête du paquet et qui identifie de manière unique un réseau local sans fil.

STP

(*Shielded Twisted-Pair, paire torsadée blindée*) Support de transmission courant qui comprend un fil pour la réception (RX) et un fil pour la transmission (TX) enroulés l'un autour de l'autre de façon à diminuer la diaphonie. Le blindage est assuré par une gaine externe tressée.

supernetting

Voir *CIDR*.

support physique

Tout moyen physique permettant de transférer des signaux entre des systèmes OSI. Considéré comme étant externe au modèle OSI et parfois appelé Couche 0, ou base du modèle de référence OSI.

surveillance IGMP

Permet à un commutateur de surveiller ou d'écouter les messages transmis entre un routeur et des hôtes.

SYN

(*synchronize*) Type de paquet utilisé par TCP pour synchroniser les numéros de séquence sur deux ordinateurs qui entament une nouvelle connexion.

SYN ACK

Message qui accuse réception du signal de synchronisation envoyé par le client et ouvre le socket du serveur pour un renvoi au client.

T

table de routage

Table stockée sur un routeur ou un autre équipement d'interconnexion de réseau qui garde un suivi des routes (et, dans certains cas, des mesures associées à ces routes) vers des destinations particulières du réseau.

table des hôtes

liste des hôtes TCP/IP qui sont sur le réseau, ainsi que leur adresse IP.

TCP/IP

(*Transmission Control Protocol/Internet Protocol*) Ensemble de protocoles mis au point par l'ARPA (Advanced Research Projects Agency) du Département de la Défense des Etats-Unis au début des années 1970. Son but était de développer des techniques permettant de connecter différents types de réseaux et d'ordinateurs. TCP/IP ne possède pas les fonctionnalités fournies par l'OSI.

TCP/IP est un protocole de transport et de travail sur Internet, c'est-à-dire une norme de facto de gestion de réseaux. Il est couramment employé avec un câblage X.25 et Ethernet et considéré comme l'un des quelques protocoles capables d'assurer une véritable migration vers OSI. TCP/IP fonctionne dans la plupart des environnements. TCP/IP opère au niveau des couches 3 et 4 du modèle OSI (respectivement Réseau et Transport).

TCP et IP sont les protocoles réseau standard dans des environnements UNIX. Ils sont presque toujours mis en œuvre et utilisés ensemble.

Telnet

Programme d'émulation de terminal utilisé pour contrôler des serveurs à distance.

temporisation (time-out)

Signal d'interruption envoyé par un équipement qui, au bout d'un certain temps, n'a toujours pas reçu les données entrantes qu'il attend.

terminaison

Connecteur spécial utilisé aux deux extrémités d'un segment Ethernet standard ou à câble fin. Il offre au câble une résistance de terminaison de 50 Ω .

tête de ligne

Dans des réseaux à large bande, point central ou concentrateur qui reçoit des signaux sur une bande de fréquences définie et qui les retransmet sur une autre. Chaque transmission d'une station de travail vers une autre sur un réseau à large bande doit passer par la tête de ligne. Celle-ci permet au réseau de recevoir et d'envoyer sur le même câble.

TFTP

(*Trivial File Transfer Protocol*) Sur des ordinateurs qui exécutent un logiciel de gestion de réseaux TCP/IP, le protocole TFTP permet d'envoyer rapidement des fichiers sur le réseau avec des fonctions de sécurité moins nombreuses que sur FTP.

tolérance aux pannes

Capacité d'un réseau à éviter qu'une panne survenant sur une partie du réseau n'entraîne l'interruption d'autres services réseau. La tolérance aux pannes augmente l'intégrité du réseau et sa disponibilité.

Les alimentations redondantes sur des émetteurs-récepteurs, des concentrateurs et des commutateurs, ou encore les topologies en anneau simple ou double sur fil de cuivre ou fibre optique, sont des exemples de systèmes tolérants aux pannes.

topologie

Disposition des nœuds et du matériel de connexion qui composent le réseau. Les topologies sont en anneau, de type bus, en étoile ou en arbre.

topologie en étoile

Réseau dans lequel chaque station de travail est connectée à un concentrateur central par une connexion dédiée point à point.

TP

(*Twisted-Pair, paire torsadée*) Câble comprenant deux conducteurs en cuivre massif ou toronné de 18 à 24 AWG, chacun revêtu d'un matériau isolant, et tressés ensemble. Le tressage offre une protection contre les interférences radio et électromagnétiques.

trace route

TraceRT est un outil de suivi des routes utilisé pour mesurer le nombre de sauts du routeur, ou de routes, entre les systèmes afin de faciliter la détection des problèmes ; il suffit de taper *tracert.exe* à l'invite de commande.

traitement distribué

Système dans lequel chaque station ou nœud d'un réseau assure son propre traitement et gère certaines données, le réseau facilitant les communications entre les stations.

trame

Groupe de bits envoyé sur une liaison, qui contient ses propres informations de contrôle, telles que l'adresse et les données de détection d'erreur. La taille et la composition de la trame varient selon le protocole. Les termes *trame* et *paquet* sont souvent utilisés l'un pour l'autre, bien que selon le modèle OSI, une trame soit constituée au niveau de la couche 2 et un paquet au niveau de la couche 3 ou au-dessus.

transmission

Processus dans le cadre duquel un commutateur ou un pont Ethernet lit le contenu d'un paquet et l'achemine sur le segment connecté approprié. La *vitesse de transmission* est le temps qu'il faut pour que l'équipement exécute toutes les étapes requises.

U**UDP**

(*Universal Datagram Protocol, protocole universel de transmission par datagramme*) Protocole de la couche transport pour des datagrammes, utilisé essentiellement pour la diffusion. Il gère également les adresses des ports.

Uni-TE

Protocole de communication de la couche application. Ce service permet un accès en lecture et en écriture à des variables, des transferts de programmes, la gestion des modes opératoires des équipements, le diagnostic au niveau de l'équipement et des liaisons, ainsi que la transmission de données non sollicitées.

usurpation d'adresse (spoofing)

Attaque contre un système sécurisé dans laquelle une personne mal intentionnée envoie un message en utilisant l'adresse IP volée/piratée d'un hôte identifié du réseau afin d'obtenir un accès non autorisé.

usurpation d'identité

Possibilité de faire apparaître un utilisateur sur le système sous l'identité d'un autre utilisateur. Ce processus peut être utilisé à des fins malveillantes. Lorsqu'il y a usurpation d'identité IP, seule la connexion au niveau du coupe-feu ou du routeur est visible sur Internet, ce qui permet de dissimuler un espace d'adresse IP protégé.

UTP

(*Unshielded Twisted Pair, paire torsadée non blindée*) Une ou plusieurs paires de câbles avec une enveloppe isolante. Les paires UTP sont généralement utilisées pour les câbles téléphoniques.

V

verrouillage de trame

Division des données à transmettre en groupes de bits et ajout d'un en-tête et d'une séquence de vérification dans chaque groupe.

VijeoLook

Le logiciel d'interface homme-machine (IHM) pour PC, de Schneider S.D.

vitesse de la ligne

Vitesse maximale, exprimée en bits par seconde, à laquelle les données peuvent être transmises de manière fiable sur une ligne, avec un matériel spécifique.

voie

Chemin de données de bout en bout entre deux nœuds. Ensemble du câblage d'un équipement actif à un autre.

VPN

(*Virtual Private Network, réseau privé virtuel*) Réseau qui connecte des réseaux avec des sites distants en utilisant un fournisseur de services tiers.

VSD

(*Variable Speed Drive*) Variateur de vitesse.

W

WAN

(*Wide Area Network, réseau étendu*) Réseau qui utilise les services de télécommunications pour transmettre des données dans une zone géographique étendue.

WEP

(*Wired Equivalent Privacy*) Protocole de sécurité pour les réseaux locaux (LAN) sans fil qui crypte les données transmises par ondes radioélectriques.

Index



A

Abonné
 dans une opération Global Data, 219
Accès à distance
 à un système Ethernet, 155
accès au réseau
 à partir d'une station distante, 157
accès commuté
 contrôle à distance d'un PC, 157
accès distant
 via un accès commuté, 157
Accès distant à un VPN, 161
ACR
 rapport affaiblissement sur
 diaphonie, 562
Activer I/O Scanning, 191
Adaptateur de terminal RNIS
 dans un WAN Ethernet, 74
Administration
 câblage, 121
Adresse MAC, 150
Affaiblissement
 paramètre de performance
 ISO/CEI 11801, 560
Appartenance à un groupe
 dans un système de multidiffusion
 IP, 150
Applications industrielles
 pour Ethernet, 19
Armoires
 création d'une liaison
 équipotentielle, 108

B

Base de données des balises IHM
 dans le fonctionnement d'un serveur
 Web FactoryCast HMI, 263
Bit de fonctionnement
 pour I/O Scanning, 191
Blindage de câble
 connexion à une surface métallique, 552
 méthode de mise à la terre, 555
Bloc MBP_MSTR
 pour surveiller les communications
 Ethernet dans un système Quantum, 329
Bloc MSTR
 pour surveiller les communications
 Ethernet dans un système Quantum, 329
Blocage
 dans une communication SCADA, 307
BootP
 dépannage, 396
Boucles de terre, 556
BRI
 options RNIS, 70
Brochage
 connecteur RJ45 pour réseaux Ethernet
 à paire torsadée, 90
brochage
 connecteurs circulaires M12, 98
brochages
 pour un connecteur cuivre RJ45, 97
Bus en anneau de mise à la terre, 106

C**Câblage**

- administration, 121
- description technique des câbles à fibre optique, 91

câblage

- documentation, 123
- données d'essai, 124
- essais des composants, 123
- étiquettes, 124

Câblage

- fibre optique, 91
- fibre optique par rapport à cuivre, 94

câblage

- installations commerciales, 123

Câblage

- normes de fibre optique, 91

câblage

- spécifications de fibre optique
- 100Base-FX, 95
- spécifications de fibre optique
- 10Base-FL, 95

Câblage

- types de fibres optiques, 92, 94

Câblage horizontal, 38**Câble à paire torsadée blindée**

- caractéristiques, 88

Câble à paire torsadée non blindée

- caractéristiques, 88

Câble cuivre

- pour réseaux Ethernet, 87

Câble cuivre inverseur

- brochage, 116
- code couleur, 117

Câble cuivre simple

- brochage, 115
- code couleur, 116

Câbles cuivre

- outils de fabrication, 118

Câbles, composants

- étiquetage, 122

Capture de paquet

- outils, 406, 406, 407

Caractéristiques du scrutateur d'E/S, 185**Carte d'interface réseau**

- système d'exploitation, 384

CAT 1

- câble cuivre à paire torsadée 1 Mbit/s
- non blindée, 87

CAT 2

- câble cuivre à paire torsadée 4 Mbit/s
- non blindée, 87

CAT 3

- câble cuivre à paire torsadée
- 16 Mbit/s, 87

CAT 4

- câble cuivre à paire torsadée
- 20 Mbit/s, 88

CAT 5

- câble cuivre à paire torsadée
- 100 Mbit/s, 88

CAT 5E

- câble cuivre à paire torsadée 350 MHz
- CAT 5 améliorée, 88

CAT 6

- câble cuivre à paire torsadée
- 400 MHz, 88

CAT 7

- câble cuivre à paire torsadée
- 500-700 MHz, 88

Chien de garde

- pour surveiller les communications distantes dans un système Quantum, 330
- sauvegarde pour un système SCADA, 322

Chien de garde de sauvegarde

- dans un système SCADA, 322

Circuits virtuels

- dans un système Ethernet, 72

Circuits virtuels commutés

- dans un système Ethernet, 72

Classification des signaux, 109**Client**

- dans une opération de remplacement d'équipements défectueux, 227

Client FDR, 227

- Client Modbus, 200, 201
 - délais d'attente, 216
 - fonctionnement dans un système Momentum, 208
 - fonctionnement dans un système Premium, 207
 - fonctionnement dans un système Quantum, 205
 - limites dans un système Momentum, 208
 - limites dans un système Premium, 206
 - limites dans un système Quantum, 204
 - nombre de tentatives, 216
- Code IP
 - degré de protection contre la pénétration de corps étrangers, 83
- Codes fonction
 - Modbus, 201
- Combinaison de transferts de données, 182
- Communication au niveau de l'entreprise, 171
- communication au niveau de l'entreprise
 - services Transparent Ready, 172
- Communication au niveau du terrain, 171
- Communication au niveau inter automates, 171
- communication client
 - entre un serveur d'E/S et un affichage SCADA, 312
- Communication de transfert de données
 - services Transparent Ready, 173
- Communication distante transparente, 171
- communication SCADA
 - sur des sockets multiples prenant en charge une requête à la fois, 311
 - sur un socket unique prenant en charge des requêtes multiples, 310
 - sur un socket unique prenant en charge une requête à la fois, 309
- communication SCADA à SCADA, 312
- Communications au niveau du terrain
 - services Transparent Ready, 174
- Communications sans fil
 - dans un système Ethernet, 65
- commutateur
 - dans un système Ethernet, 67
- Commutateur
 - dans un WAN Ethernet, 74
- Commutation de circuits
 - dans un système Ethernet, 70
- Commutation de paquets
 - dans un système Ethernet, 71
- Compatibilité
 - des services, 182
- Compatibilité du service, 182
- Composants du système de mise à la terre, 105
- concentrateur
 - dans un système Ethernet, 66
- Conception d'un réseau, 182
- Conception réseau, 182
- Conducteur de terre principal, 105
- Conducteurs de terre, 105
- Configuration distante
 - en utilisant un serveur Web, 246
- Congestion du réseau
 - dans un système Ethernet, 63
- Connecteur RJ45
 - brochages, 90
 - code couleur des fils, 90
- connecteurs
 - brochage M12, 98
 - brochages RJ45 , 97
- Connecteurs
 - fibre optique, 99
 - LC pour fibre optique, 99
- connecteurs
 - M12, 98
- Connecteurs
 - MT/RJ pour fibre optique, 99
- connecteurs
 - RJ45, 96
 - RJ45 blindés, 97
- Connecteurs
 - SC pour fibre optique, 99
 - ST pour fibre optique, 99
- connecteurs circulaires M12, 98
- connecteurs cuivre RJ45, 96
- connecteurs cuivre RJ45 blindés, 97
- connexion d'un automate à Internet, 157
- Connexion d'un automate à Internet, 162

- connexion d'un automate à Internet
 - pour accéder à un système distant, 157
- Connexion de la base de données relationnelle
 - à un serveur Web FactoryCast HMI, 264
- Connexion de mise à la terre
 - pour un blindage de câble, 552
 - procédure, 550
- Connexion de terre
 - pour un blindage de câble, 552
 - procédure, 550
- Connexion Internet à un automate
 - pour l'accès au système à distance, 162
- Connexions de masse
 - recommandations, 548
- Connexions de terre
 - recommandations, 548
- Connexions logiques
 - dépannage d'un système Ethernet, 382
- Connexions physiques
 - dépannage d'un système Ethernet, 381
- Couche application
 - dans le modèle TCP/IP, 137
- Couche de transport
 - du modèle Transparent Ready, 141
- Couche interface réseau
 - dans le modèle TCP/IP, 138
- Couche interréseau
 - dans le modèle TCP/IP, 138
 - du modèle Transparent Ready, 139
- Couche transport
 - dans le modèle TCP/IP, 137
- Coupe
 - pour la fabrication de câbles cuivre Ethernet, 119
- Coupe-câble
 - pour la fabrication de câbles cuivre Ethernet, 118, 119

D

- Degré de protection
 - exigences de protection contre la pénétration de corps étrangers, 83
- Délai de passerelle, 372

- Dénudage
 - pour la fabrication de câbles cuivre Ethernet, 119
 - pour la fabrication de câbles cuivre Ethernet, 118
- Dépannage
 - BootP, 396
 - connexions logiques sur un système Ethernet, 382
 - connexions physiques sur un système Ethernet, 381
 - d'un système Ethernet, 377, 378
 - encombrement sur un système Ethernet, 382
 - équipement défectueux, 396
 - FTP, 395
 - NTP, 399
 - perte de paquets, 404
 - services, 389
 - SMTP, 398
 - synchronisation horaire, 399
 - Telnet, 395
- Désactiver I/O Scanning, 191
- Diagnostics intégrés
 - sélection du service, 177
- Différence de temps
 - paramètre de performance ISO/CEI 11801, 563
- Différence de temps de propagation
 - paramètre de performance ISO/CEI 11801, 563
- documentation
 - câblage, 123
- Domaines de collision
 - dans un système Ethernet, 62
- Domaines de diffusion
 - dans un système Ethernet, 63
- Données
 - capture de paquet, 406
 - dépannage, 404
 - perte de paquets, 404
- données d'essai
 - câblage, 124

E

- Ecart télédiaphonique
 - paramètre de performance
ISO/CEI 11801, 563
- Ecart télédiaphonique cumulé
 - paramètre de performance
ISO/CEI 11801, 563
- Ecart télédiaphonique paire à paire
 - paramètre de performance
ISO/CEI 11801, 563
- Editeur
 - dans une opération Global Data, 219
- Editeur de données graphiques
 - dans un serveur Web FactoryCast, 256
- Éléments d'un système Transparent Ready, 27
- ELFEXT
 - écart télédiaphonique, 563
- émetteur-récepteur
 - dans un système Ethernet, 67
- Encombrement
 - sur un système Ethernet, 382
- environnement industriel léger
 - connecteurs cuivre RJ45, 96
- Environnement industriel léger
 - exigences liées à l'écrasement, 79
 - exigences liées à la flexion, 79
 - exigences liées à la résistance à la traction, 79
 - exigences liées au choc, 78
 - exigences liées aux vibrations, 78
 - niveaux de pollution recommandés, 83
- environnement industriel lourd
 - connecteurs circulaires M12, 98
- Environnement industriel lourd
 - exigences liées à l'écrasement, 79
 - exigences liées à la flexion, 79
 - exigences liées à la résistance à la traction, 79
 - exigences liées au choc, 78
 - exigences liées aux vibrations, 78
 - niveaux de pollution recommandés, 83
- Équilibrage
 - paramètre de performance
ISO/CEI 11801, 563
- Équipement distant
 - exigences du service I/O Scanning, 185
- Équipements WAN
 - adaptateurs de terminaux RNIS, 74
 - commutateurs, 74
 - matériel CSU/DSU, 74
 - modems, 74
 - routeurs, 73
 - serveurs d'accès, 74
- essais des composants
 - câblage, 123
- Ethernet
 - considérations architecturales, 353
 - dans les applications industrielles, 19
 - industriel, 18
- Ethernet : outil de capture de paquet, 406, 406, 407
- Ethernet II
 - dans le modèle Transparent Ready, 139
- Ethernet industriel
 - définition, 18
 - différence avec l'Ethernet commercial, 20
- Étiquetage
 - câbles, composants, 122
- Étiquetage des câbles
 - normes, 121
- étiquettes
 - câblage, 124
- Évaluation d'un système, 182
- Évaluation du système, 182
- Exigences de protection contre la pénétration de corps étrangers
 - degré de protection, 83
 - niveaux de pollution, 82
- Exigences liées à l'écrasement, 79
- Exigences liées à la flexion, 79
- Exigences liées à la mécanique
 - choc, 78
 - écrasement, 79
 - flexion, 79
 - résistance à la traction, 79
 - vibrations, 78
- Exigences liées à la résistance à la traction, 79

Exigences liées au choc, 78
Exigences liées aux vibrations, 78

F

FactoryCast
 sélection du service, 177
Fast Ethernet, 61
FDR
 remplacement d'équipements
 défectueux, 176
 sélection du service, 176
FDR (Faulty Device Replacement, Remplacement d'équipements défectueux)
 quand utiliser le service, 228
FEXT
 télédiaphonie, 562
Fibre optique, 91
 description technique, 91
 types de câbles, 92
File d'attente
 pour la messagerie via une
 passerelle, 340
Fonction de réveil
 dans un fonctionnement OPC Factory
 Server, 286
Fonctions de calcul
 dans le fonctionnement d'un serveur
 Web FactoryCast HMI, 264
FTP
 dépannage, 395
 file transfer protocol, 178

G

GARP Multicast Registration Protocol, 149
Gestion de groupes
 sur un système Ethernet, 149, 149, 149
Gestion de l'adresse IP
 dans un système de redondance d'UC
 Quantum, 331
Gestion des collisions, 62
Gestion des erreurs
 dans une opération Global Data, 219
 pour I/O Scanning, 190

Gestion du réseau
 pour un système Ethernet, 151
Gigabit Ethernet, 61
Global Data
 limites, 220
 normes, 218
 prise en charge d'équipements, 221
 quand utiliser le service, 221
 sélection du service, 175
 synchronisation d'application, 223
 temps de réponse, 223
 utilisation de la technologie de multidiffusion, 222
GMRP, 149
Groupe d'éléments
 dans le fonctionnement d'un OPC
 Factory Server, 284
Groupe de distribution
 dans une opération Global Data, 219

H

Horloges internes
 pour les périodes de répétition d'I/O
 Scanning, 192

I

I/O Scanning
 activer, 191
 bit de fonctionnement, 191
 désactiver, 191
 exigences au niveau de l'équipement
 distant, 185
 fonctionnement, 188
 gestion des erreurs, 190
 mot de diagnostic, 191
 opérations d'écriture, 189
 opérations de lecture, 190
 périodes de répétition, 192
 quand l'utiliser, 186
 sélection du service, 175
 temps de réponse, 195
 utilisation du socket TCP, 191

Identification des problèmes
 sur un système Ethernet, 381
 IEEE 802.3
 dans le modèle Transparent Ready, 139
 Norme Ethernet, 34
 IGMP, 149
 IHM
 modèle autonome, 301
 modèle client/serveur, 302
 Impédance
 paramètre de performance
 ISO/CEI 11801, 560
 Impédance nominale
 paramètre de performance
 ISO/CEI 11801, 560, 560
 Indices mécaniques
 pour les paramètres et les exigences
 d'environnement, 32
 Instabilité
 pour déterminer si un chemin de
 communication SCADA est correct, 332
 installations commerciales
 câblage, 123
 interfaces indépendantes
 sur un réseau Ethernet, 317
 interfaces liées
 sur un réseau Ethernet, 316
 Internet Group Management Protocol, 149
 Internet Group Management Protocol,
 surveillance, 149
 ISO/CEI 8802-3
 norme Ethernet, 34

L

Les chemins de câbles, 112
 Liaison équipotentielle
 création d'un système de mise à la terre
 pour un bâtiment, 107
 définie, 105
 équipements locaux, 108
 norme, 106
 pour lutter contre les EMI dans les
 réseaux Ethernet, 104
 Liaison permanente, 127

liaison point à point
 dans un système Ethernet, 70
 Ligne louée
 dans un système Ethernet, 70
 Limites de charge
 pour les messages Ethernet, 365
 Logiciel de configuration
 d'un serveur Web FactoryCast, 255

M

Machines
 création d'une liaison
 équipotentielle, 108
 Matériel CSU/DSU
 dans un WAN Ethernet, 74
 Messagerie Modbus, 199
 délais d'attente du client, 216
 fonctionnement du client dans un
 système Momentum, 208
 fonctionnement du client dans un
 système Premium, 207
 fonctionnement du client dans un
 système Quantum, 205
 fonctionnement du serveur avec
 Concept, 210
 fonctionnement du serveur avec
 Proworx, 210
 fonctionnement du serveur dans un
 système Momentum, 214
 fonctionnement du serveur dans un
 système Premium, 213
 fonctionnement du serveur dans un
 système Quantum, 209
 limites du client dans un système
 Momentum, 208
 limites du client dans un système
 Premium, 206
 limites du client dans un système
 Quantum, 204

- mise en œuvre d'un équipement Modbus TCP, 199
- nombre de tentatives du client, 216
- nombre de tentatives du serveur, 216
- performances du serveur Unity, 211
- sélection du service, 175
- services client, 200, 201
- services serveur, 201, 202
- temps de réponse, 353
- temps de réponse client dans un système Momentum, 362
- temps de réponse client dans un système Premium, 361
- temps de réponse client dans un système Quantum, 360
- temps de réponse du serveur dans un système Premium, 213
- Mesures d'installation
 - pour lutter contre les EMI dans les réseaux Ethernet, 103
- MIB
 - pour la gestion du réseau, 151
- MIB privée
 - pour la gestion du réseau, 151
- MICE, 32, 32
- Mise à la terre
 - pour lutter contre les EMI dans les réseaux Ethernet, 104
- Modbus
 - codes fonction, 201
 - temps de réponse du serveur dans un système Momentum, 356
 - temps de réponse du serveur dans un système Premium, 355
 - temps de réponse du serveur dans un système Quantum, 356
- Modèle OSI, 135
- Modèle TCP/IP
 - basé sur OSI, 137
- Modèle Transparent Ready
 - basé sur OSI, 139
- Modem
 - dans un WAN Ethernet, 74

- Monitor Pro
 - mise en œuvre du modèle client/serveur SCADA, 313
- Mot de diagnostic
 - pour I/O Scanning, 191
- Mot de passe, 164

N

- Niveaux de gestion des informations
 - dans le fonctionnement d'un serveur Web FactoryCast HMI, 263
- Niveaux de pollution
 - exigences de protection contre la pénétration de corps étrangers, 82
- Niveaux de redondance
 - dans un système SCADA, 319
- Norme CEI 1000-4
 - interférences électriques et électromagnétiques, 85
- Norme de communication Modbus, 198
- Norme ISO/CEI 11801
 - définitions du test des câbles en cuivre, 557
 - pour la planification et l'installation de câbles cuivre, 542
- Normes
 - câblage structuré, 34
 - câbles à fibre optique, 91
 - étiquetage des câbles, 121
 - internationales, 31
 - pour l'installation d'un réseau Ethernet, 34
 - pour la performance du réseau Ethernet, 34
 - pour la planification du câblage, 34
 - pour la sélection des équipements Ethernet, 34
- Normes d'émission électromagnétique, 85
- Normes d'immunité, 85
- Normes d'immunité au bruit, 85
- Normes d'installation, 34
- Normes de câblage structuré, 34
- Normes de performance, 34
- Normes de planification du câblage, 34

Normes de sélection, 34
Normes Ethernet
 IEEE 802.3, 34
 ISO/CEI 8802-3, 34
Normes internationales
 pour les réseaux Ethernet industriel, 31
Normes ouvertes
 dans Ethernet pour l'automatisation, 134
notification par message électronique, 240
Notification par message électronique
 fonctionnement, 242
 protection facultative par mot de
 passe, 243
 sélection du service, 176
NTP
 dépannage, 399
Numéro des sockets TCP
 dans un système de redondance d'UC
 Quantum, 334

O

OPC Factory Server
 architecture d'exécution, 292
 avec multiples connexions SCADA, 298
 compactage d'éléments de même
 type, 289
 concaténation des requêtes, 289
 optimisation des requêtes, 289
 option build-time/runtime, 294
 service de notification, 286
 services, 282
 services synchrones, 285, 286
 taille des requêtes, 288
Opérations d'écriture
 pour I/O Scanning, 189
Opérations de lecture
 pour I/O Scanning, 190
outil de certification DSP-4000
 pour les installations de câblage en
 cuivre et les performances, 131
outil de certification OMNiscanner 2
 pour les installations de câblage en
 cuivre et les performances, 131

Outils
 pour la fabrication de câbles cuivre
 Ethernet, 118

P

Pages dynamiques
 dans un fonctionnement de serveur
 Web, 249
Pages statiques
 dans un fonctionnement de serveur
 Web, 248
Paire torsadée
 câble cuivre Ethernet, 87
Paramètres
 pour les tests de câble en cuivre, 558
Paramètres de performance
 pour câble Ethernet en cuivre, 558
Paramètres de performance ISO/CEI 11801
 différence de temps de propagation, 563
 écart télédiaphonique, 563
 écart télédiaphonique cumulé, 563
 impédance nominale, 560
 perte d'insertion, 560
 perte de conversion longitudinale à
 différentielle, 563
 perte par retour, 560
 perte paradiaphonique, 561
 perte paradiaphonique cumulée, 562
 rapport affaiblissement sur
 diaphonie, 562
 rapport affaiblissement sur diaphonie
 cumulée, 562
 résistance cc de la boucle, 563
 télédiaphonie, 562
 temps de propagation, 563
Pare-feu, 165
 avancé, 165
 avec filtrage Modbus, 165
 configuration, 165
Passerelle
 avec conversion de protocole
 d'application, 338
passerelle
 dans un système Ethernet, 68

Passerelle

- file d'attente de messages, 340
- sans conversion de protocole d'application, 337
- temps de réponse, 372
- utilisant une mémoire partagée, 339

Périodes de répétition effectives

- pour I/O Scanning, 192

Permutation

- dans un système de redondance d'UC Quantum, 331
- message UDP dans un système de redondance d'UC Quantum, 333

Perte de conversion longitudinale à différentielle

- paramètre de performance ISO/CEI 11801, 563

Perte par retour

- paramètre de performance ISO/CEI 11801, 560

Perte paradiaphonique

- paramètre de performance ISO/CEI 11801, 561

Perte paradiaphonique cumulée

- paramètre de performance ISO/CEI 11801, 562

Perte paradiaphonique paire à paire

- paramètre de performance ISO/CEI 11801, 561

Pince à dénuder

- pour la fabrication de câbles cuivre Ethernet, 118, 119

Pince à sertir

- pour la fabrication de câbles cuivre Ethernet, 118, 119

Plan de terre, 106**pont**

- dans un système Ethernet, 67

Prévention des EMI

- liaison équipotentielle, 104
- mesures d'installation, 103
- méthodes, 103
- méthodes de mise à la terre, 104

PRI

- options RNIS, 70

Prise en charge d'équipements

- pour Global Data, 221
- protocole simplifié de gestion de réseau fonctionnellement, 270

PS ACR

- rapport affaiblissement sur diaphonie cumulée, 562

PS ELFEXT

- écart télédiaphonique cumulé, 563

R

Rapport affaiblissement sur diaphonie

- paramètre de performance ISO/CEI 11801, 562

Rapport affaiblissement sur diaphonie cumulée

- paramètre de performance ISO/CEI 11801, 562

Rapport affaiblissement sur diaphonie paire à paire

- paramètre de performance ISO/CEI 11801, 562

rapport d'exception

- dans une communication SCADA, 303

Recommandations de câblage, 110**Recommandations de conformité pour l'installation de câbles en cuivre Ethernet, 126****Recommandations pour les chemins de câbles, 112****Redémarrage**

- lors du dépannage d'un système Ethernet, 377

redondance

- et services de communications réseau, 315

Redondance d'UC

- dans un système centré sur la communication, 324
- misés en œuvre SCADA, 323

Redondance d'UC Quantum

- dans un système centré sur la communication, 324
- misés en œuvre SCADA, 323

- Remplacement d'équipement défectueux, 396
- Répartiteur armoire, 46
- Répartiteur de site industriel, 45
- Répartiteur machine, 46
- Répartiteur terrain, 46
- Répartiteur usine, 45
- répéteur
 - dans un système Ethernet, 66
- Réseau de liaison commun, 106
- Réseau fédérateur bâtiment, 38
- Réseau fédérateur campus, 38
- Réseau fédérateur de site industriel, 45
- Réseau privé virtuel
 - pour accéder à un système distant, 161
- Réseaux commutés
 - et gestion des collisions, 62
- Résistance cc de la boucle
 - paramètre de performance ISO/CEI 11801, 563
- Résistance de la boucle
 - paramètre de performance ISO/CEI 11801, 563
- RNIS
 - dans un système Ethernet, 70
- Routage
 - avec adressage IP, 153
- Routage des câbles
 - entre les armoires, 114
 - entre les bâtiments, 114
- Routage des câbles entre les armoires, 114
- Routage des câbles entre les bâtiments, 114
- routeur
 - dans un système Ethernet, 68
- Routeur
 - dans un WAN Ethernet, 73
- S**
- SCADA
 - chien de garde de sauvegarde, 322
 - communication vers un équipement redondant, 321
 - étapes de communications, 302
 - mise en œuvre chien de garde vers automate Quantum, 330
 - modèle autonome, 301
 - modèle client/serveur, 302
 - pour un système de redondance d'UC Quantum, 323
 - rapport d'exception, 303
 - technique de blocage pour une communication efficace, 307
- Scruteur d'E/S
 - formules des temps de réponse, 363
- Section
 - pour la fabrication de câbles cuivre Ethernet, 118
- Sécurité
 - accès physique, 164
 - configuration de pare-feu, 165
 - contrôle d'accès à l'automate, 166
 - d'un système Ethernet, 164
 - liste de contrôle d'accès, 166
 - mot de passe, 164
 - pare-feu, 165
 - points d'accès, 167
 - politique, 164
 - port, 166
 - sans fil, 166
 - VPN, 167
 - WEP, 167
- Sensibilité
 - dans la performance CME, 109
- Sensibilité CME
 - classification des signaux, 109
- Sertissage
 - pour la fabrication de câbles cuivre Ethernet, 118, 119
- Serveur
 - dans une opération de remplacement d'équipements défectueux, 227
- Serveur à accès distant
 - structure, 159
- Serveur d'accès
 - dans un WAN Ethernet, 74
- Serveur FDR, 227

Serveur Modbus, 201, 202

- fonctionnement avec , 210
- fonctionnement avec Proworx, 210
- fonctionnement dans un système Momentum, 214
- fonctionnement dans un système Premium, 213
- fonctionnement dans un système Quantum, 209
- nombre de tentatives, 216
- performances dans Unity, 211
- temps de réponse dans un système Premium, 213

Serveur Web FactoryCast

- hébergement, 254
- logiciel de configuration, 255

Service de notification

- dans un fonctionnement OPC Factory Server, 286

service de protocole de transfert de fichiers, 268**Service de serveur**

- fonctionnement, 248

Service de serveur Web

- pages dynamiques, 249
- pages statiques, 248

Service du serveur Web

- prise en charge de la configuration distante, 246

Service Global Data

- gestion des erreurs, 219

Service serveur Web FactoryCast

- éditeur de données graphiques, 256
- visualisateur d'alarme, 256

Service serveur Web FactoryCast HMI

- architecture, 261
- architectures hybrides, 262
- base de données des balises IHM, 263
- connecté à une base de données relationnelle, 264
- fonctionnement, 261
- fonctions de calcul, 264
- niveaux de gestion des informations, 263

Service Telnet, 272**Services**

- dépannage, 389
- diagnostics intégrés, 177
- disponibles dans un système de redondance d'UC Quantum, 333
- FDR, 176
- FDR (Faulty Device Replacement, Remplacement d'équipements défectueux), 226
- Global data, 175
- Global Data, 218
- I/O Scanning, 175, 184
- messaging Modbus, 175, 198

services

- notification par message électronique, 240

Services

- notification par message électronique, 176
- OPC Factory Server, 281
- pour la synchronisation des applications, 173
- pour les communications au niveau du terrain, 174
- pour les communications au niveau inter-automates, 173
- pris en charge par les équipements Advantys STB, 348
- pris en charge par les équipements Momentum M1E, 347
- pris en charge par les équipements Premium, 345
- pris en charge par les équipements Quantum, 344
- pris en charge par les équipements Twido, 348
- pris en charge par les modules de communication Ethernet Momentum, 347
- pris en charge par les modules de communication Ethernet Premium, 345
- pris en charge par les modules de communication Ethernet TSX Micro, 346
- pris en charge par les passerelles Power Logic, 350

- pris en charge par les systèmes de câblage ConneXium, 351
- pris en charge par les variateurs de vitesse Altivar ATV 38/58, 349
- protocole de transfert de fichiers, 267
- services
 - protocole simplifié de gestion de réseau, 269
- Services
 - serveur Web, 246
 - serveur Web FactoryCast, 254
 - serveur Web FactoryCast HMI, 260
 - synchronisation horaire, 176
 - Telnet, 272
 - Trivial File Transfer Protocol, 271
- services
 - utilisés pour la communication au niveau de l'entreprise, 172
 - utilisés pour les applications, 172
 - utilisés pour les équipements terrain, 172
 - utilisés pour les systèmes de supervision et les automates, 172
- Services
 - Web/FactoryCast, 177
- Services d'accès commuté
 - dans un système Ethernet, 72
- Services pris en charge par les équipements
 - services pour Advantys STB, 348
 - services pour les modules de communication Ethernet Momentum, 347
 - services pour les modules de communication Ethernet TSX Micro, 346
 - services pour les modules Ethernet Premium, 345
 - services pour les passerelles Power Logic, 350
 - services pour les processeurs Momentum M1E, 347
 - services pour les systèmes de câblage ConneXium, 351
 - services pour les variateurs de vitesse Altivar ATV 38/58, 349
 - services pour Quantum, 344
 - services pour Twido, 348
 - services pour UC Premium, 345
- Services synchrones
 - dans un fonctionnement OPC Factory Server, 285, 286
- SMTP
 - dépannage, 398
 - pour la notification par message électronique, 242
- SNMP
 - pour la gestion du réseau, 151
 - pour les stations de gestion du réseau, 172
 - simple network management protocol, 178
- Socket de passerelle, 341
- Sous-systèmes de câblage, 38
- Standard 100Base-TX
 - pour réseaux Ethernet à paire torsadée, 89
- Stations terminales VLAN
 - dans un système Ethernet, 64
- Stratégie
 - pour Transparent Ready, 21
- Suite de protocoles Internet, 140
- Surveillance de l'automate redondant
 - utilisation de SCADA dans un système de redondance d'UC Quantum, 330
- Surveillance IGMP, 149
- Synchronisation d'application
 - pour Global Data, 223
- Synchronisation des applications
 - services Transparent Ready, 173
- Synchronisation horaire
 - dépannage, 399
 - sélection du service, 176
- Système
 - Transparent Ready et ses éléments, 27
- Système d'exploitation
 - carte d'interface réseau, 384
 - vérification logique, 384
- Système de câblage
 - éléments, 38
- Système redondant
 - entièrement mis en œuvre pour Quantum, 328

- limitations dans un système
 - Quantum, 327
 - pour Quantum, 326
- Systèmes de serveur à accès distant, 159
- Systèmes Ethernet
 - domaines de collision, 62
 - domaines de diffusion, 63
 - IP sans fil, 65
 - technologies LAN, 61
 - VLAN, 64

T

- TCP
 - dans le modèle Transparent Ready, 141
- TCP/IP
 - dans le modèle Transparent Ready, 140
- Technologie de multidiffusion
 - pour Global Data, 222
- Technologies LAN
 - pour les systèmes Ethernet, 61
- Télédiaphonie
 - paramètre de performance
 - ISO/CEI 11801, 562
- Telnet, 178
 - dépannage, 395
- Temps de propagation
 - paramètre de performance
 - ISO/CEI 11801, 563
- Temps de réponse
 - d'une passerelle, 372
 - performances I/O Scanning
 - Premium, 196
 - performances I/O Scanning
 - Quantum, 195
 - pour Global Data, 223
- Terre réelle, 105
- Test
 - d'une installation en cuivre, 557
- Test des performances
 - d'une installation en cuivre, 557
- TFTP
 - trivial file transfer protocol, 178
- Timeout de passerelle, 342

- Topologie
 - anneau auto-régénérant, 59
- Topologie à double anneau, 51
- Topologie d'anneau auto-régénérant, 59
- Topologie de bus, 47
- Topologie de chaînage, 50
- Topologie de maillage, 52
- Topologie en anneau, 50
- Topologie en anneau Ethernet, 56
- Topologie en bus Ethernet, 54
- Topologie en chaînage Ethernet, 56
- Topologie en étoile, 49
- Topologie en étoile Ethernet, 55
- Topologie maillée, 57
- Topologies
 - anneau Ethernet, 56
 - bus, 47
 - bus Ethernet, 54
 - chaînage, 50
 - chaînage Ethernet, 56
 - double anneau, 51
 - en anneau, 50
 - en étoile, 49
 - étoile Ethernet, 55
 - maillage, 52
 - maillée, 57
- Trames
 - dans un système Ethernet, 61
- Trames Ethernet, 61
- Transferts de données
 - combinaison, 182
- Transparent Ready
 - définition, 18
 - éléments du système, 27
 - stratégie, 21
- Trivial File Transfer Protocol, 271

U

- UDP
 - dans le modèle Transparent Ready, 141
- Utilisation du socket TCP
 - pour I/O Scanning, 191

V

- Vérification logique
 - système d'exploitation, *384*
- VijeoLook
 - mise en œuvre du serveur OPC, *313*
- Visualisateur d'alarme
 - dans un serveur Web FactoryCast, *256*
- Visualisateur du rack
 - dans un fonctionnement de serveur Web, *250*
- Voie, *129*
- VPN
 - sécurité, *167*
- VPN à accès distant, *161*
- VPN point à point, *161*

W

- Web/FactoryCast
 - sélection du service, *177*
- WEP
 - sécurité, *167*

