

Systèmes de contrôleurs Modicon

Cybersécurité

Guide utilisateur

Traduction de la notice originale

11/2024

EIO0000002001.10

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité	5
Avant de commencer	6
Démarrage et test	7
Fonctionnement et réglages	8
A propos de ce manuel	9
Présentation	17
Recommandations de Schneider Electric	17
Comment sécuriser l'architecture	19
Vue Système	19
Définition des mots de passe dans Control Expert	21
Sécurisation renforcée du PC	23
Désactiver les services de communication intégrés inutilisés	32
Limiter le flux de données du réseau de contrôle (contrôle d'accès)	33
Configuration de la communication chiffrée	36
Cible de sécurité CSPN	43
Configuration d'un audit de Cybersécurité (consignation des événements)	52
Description des messages du journal des événements pour Control Expert	62
Description des messages du journal des événements pour les contrôleurs M580 (à partir de la version de micrologiciel V4.10) et pour BMENOR2200H (à partir de la version de micrologiciel 3.01)	68
Description des messages du journal des événements des contrôleurs M580 (micrologiciel antérieur à la version 4.10), BMENUA0100 et BMENOR2200H (micrologiciel antérieur à la version 3.01)	82
Identification et authentification	100
Autorisations de contrôle	105
Gestion des vérifications d'intégrité des données	109
Configurer une liaison d'ingénierie sécurisée entre Control Expert et un contrôleur Ethernet M580	113
Caractéristiques d'une connexion sécurisée	114
Procédure de configuration d'une connexion sécurisée	117
Considérations relatives au mode de fonctionnement	118

Compatibilité et limites de la programmation sécurisée imposée	119
Compatibilité des adaptateurs de communication	121
Ports et services Ethernet du système M580	126
Services de Cybersécurité par système	128
Services de Cybersécurité	128
Services de sécurité Modicon M340.....	136
Services de sécurité Modicon M580.....	136
Services de sécurité Modicon Quantum	136
Services de sécurité Modicon X80.....	138
Services de sécurité Modicon Premium/Atrium	141
Services de sécurité Modicon Momentum MDI	142
Services de sécurité Modicon MC80	142
Comment protéger les architectures M580, M340, Momentum MDI et MC80 avec EAGLE40 en utilisant un VPN	143
Pare-feu EAGLE40	143
Prérequis.....	144
Architecture standard	146
Configuration du pare-feu	146
Glossaire	155
Index.....	180

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer 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.



La présence de ce symbole sur une étiquette "Danger" ou "Avertissement" signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.



Ce symbole est le symbole d'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 signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

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 ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

▲ AVERTISSEMENT
EQUIPEMENT NON PROTEGE
• N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement. • N'accédez pas aux machines pendant leur fonctionnement.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automate et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠ Avertissement

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 :

(En cas de divergence ou de contradiction entre une traduction et l'original anglais, le texte original en anglais prévaudra.)

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit dérégulé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- L'opérateur ne doit avoir accès qu'aux réglages fonctionnels dont il a besoin. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Objectif du document

Ce manuel définit les aspects de la cybersécurité qui permettent de configurer un système moins vulnérable aux cyberattaques.

NOTE: Dans ce document, les termes "sécurité", "sécurisé", "sécuriser" et "sécurisation" sont utilisés en relation avec les questions de cybersécurité.

Champ d'application

Ce document a été actualisé pour EcoStruxure™ Control Expert V16.0.

Pour plus d'informations sur la conformité des produits avec les normes environnementales (RoHS, REACH, PEP, EOL, etc.), consultez le site www.se.com/ww/en/work/support/green-premium/.

Langues disponibles du document

Ce document est disponible dans les langues suivantes :

- Chinois (EIO0000002004)
- Anglais (EIO0000001999)
- Français (EIO0000002001)
- Allemand (EIO0000002000)
- Italien (EIO0000002002)
- Espagnol (EIO0000002003)

Informations concernant la Cybersécurité

Vous trouverez des informations sur la cybersécurité sur le site Web de Schneider Electric : <https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp>

Documents disponibles en téléchargement dans la section de support à la cybersécurité :

Titre de documentation	Adresse de page Web
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations	www.se.com/ww/en/download/document/STN v2

Documents à consulter

Titre de documentation	Référence commerciale
<i>Modicon M580 - Guide de planification du système</i>	HRB65322 (CHS) HRB62666 (ENG) HRB65318 (FRE) HRB65319 (GER) RB65320 (ITA) HRB65321 (SPA)
<i>Modicon M580 - Guide de référence du matériel</i>	EIO0000001583 (CHS) EIO0000001578 (ENG) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001582 (ITA) EIO0000001581 (SPA)
Modicon M580 BMENOC0301 / BMENOC0311 - Module de communication Ethernet - Guide d'installation et de configuration	HRB65316 (CHS) HRB62665 (ENG) HRB65311 (FRE) HRB65313 (GER) HRB65314 (ITA) HRB65315 (SPA)
<i>Modicon M340 pour Ethernet - Processeurs et modules de communication - Manuel utilisateur</i>	31007493 (CHS) 31007131 (ENG) 31007132 (FRE) 31007133 (GER) 31007494 (ITA) 31007134 (SPA)
Quantum avec EcoStruxure™ Control Expert - Configuration TCP/IP - Manuel utilisateur	31007110 (CHS) 33002467 (ENG) 33002468 (FRE) 33002469 (GER) 31008078 (ITA) 33002470 (SPA)
Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur	31007102 (CHS) 35006192 (ENG) 35006193 (FRE) 35006194 (GER) 31007214 (ITA) 35006195 (SPA)
EcoStruxure™ Control Expert - Modes de fonctionnement	33003697 (CHS) 33003101 (ENG)

Titre de documentation	Référence commerciale
	33003102 (FRE) 33003103 (GER) 33003696 (ITA) 33003104 (SPA)
Quantum avec EcoStruxure™ Control Expert - Manuel de référence du matériel	35012184 (CHS) 35010529 (ENG) 35010530 (FRE) 35010531 (GER) 35013975 (ITA) 35010532 (SPA)
Quantum avec EcoStruxure™ Control Expert - 140NOC77101 - Module de communication Ethernet - Manuel utilisateur	S1A33993 (CHS) S1A33985 (ENG) S1A33986 (FRE) S1A33987 (GER) S1A33989 (ITA) S1A33988 (SPA)
Premium avec EcoStruxure™ Control Expert - TSXETC101 - Module de communication Ethernet - Manuel utilisateur	S1A34008 (CHS) S1A34003 (ENG) S1A34004 (FRE) S1A34005 (GER) S1A34007 (ITA) S1A34006 (SPA)
Modicon M340 - Module de communication Ethernet BMXNOC0401 - Manuel utilisateur	S1A34014 (CHS) S1A34009 (ENG) S1A34010 (FRE) S1A34011 (GER) S1A34013 (ITA) S1A34012 (SPA)
<i>Quantum EIO, Réseau de contrôle, Guide d'installation et de configuration</i>	S1A48999 (CHS) S1A48993 (ENG) S1A48994 (FRE) S1A48995 (GER) S1A48997 (ITA) S1A48998 (SPA)
<i>EcoStruxure™ Control Expert, Communication, Librairie de blocs</i>	33003683 (CHS) 33002527 (ENG) 33002528 (FRE) 33002529 (GER) 33003682 (ITA) 33002530 (SPA)
Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur	31007112 (CHS) 33002479 (ENG) 33002480 (FRE) 33002481 (GER) 31007213 (ITA) 33002482 (SPA)
<i>Modicon M580 - Modules CANopen BMECXM - Manuel utilisateur</i>	EIO0000002134 (CHS) EIO0000002129 (ENG) EIO0000002130 (FRE) EIO0000002131 (GER)

Titre de documentation	Référence commerciale
	EIO0000002132 (ITA) EIO0000002133 (SPA)
<i>EcoStruxure Automation Device Maintenance - Outil de mise à niveau du firmware</i>	EIO0000004050 (CHS) EIO0000004033 (ENG) EIO0000004046 (GER) EIO0000004048 (FRE) EIO0000004049 (ITA) EIO0000004047 (SPA)
<i>Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide</i>	HRB44124 (ENG)
<i>Modicon MC80 Program Logic Controller (PLC) User Manual</i>	EIO0000002071 (ENG)

Informations produit

 **DANGER**

RISQUE DE CHOC ÉLECTRIQUE, D'EXPLOSION OU D'ARC ÉLECTRIQUE

- Coupez l'alimentation de tous les équipements, y compris les appareils connectés, avant de retirer des caches ou des portes d'accès ou avant d'installer ou de retirer des accessoires, matériels, câbles ou fils, sauf dans les cas de figure spécifiquement indiqués dans le guide de référence du matériel correspondant à cet équipement.
- Utilisez toujours un appareil de mesure de tension réglé correctement pour vous assurer que l'alimentation est coupée lorsque cette précaution est mentionnée.
- Remettez en place et fixez tous les caches, accessoires, matériels, câbles et fils, puis vérifiez que l'équipement est correctement relié à la terre avant de le mettre sous tension.
- Utilisez uniquement la tension indiquée pour faire fonctionner l'équipement et les produits associés.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

⚠ Avertissement

PERTE DE CONTROLE

- Réalisez une analyse des modes de défaillance et de leurs effets (FMEA) ou une analyse de risques équivalente sur l'application et appliquez les contrôles de prévention et de détection appropriés avant la mise en œuvre.
- Prévoyez un état de repli pour les événements ou séquences de commande indésirables.
- Le cas échéant, prévoyez des chemins de commande séparés et redondants.
- Définissez les paramètres appropriés, notamment pour les limites.
- Examinez les conséquences des retards de transmission et prenez les mesures correctives nécessaires.
- Examinez les conséquences des interruptions de la liaison de communication et prenez des mesures correctives nécessaires.
- Prévoyez des chemins indépendants pour les fonctions de commande critiques (arrêt d'urgence, dépassement de limites, conditions d'erreur, etc.) en fonction de votre évaluation des risques ainsi que des réglementations et consignes applicables.
- Appliquez les réglementations et les consignes locales de sécurité et de prévention des accidents.¹
- Testez chaque mise en œuvre d'un système pour vérifier son bon fonctionnement avant de le mettre en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

¹ Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), *Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems* (Normes de sécurité relatives à la construction et manuel de sélection, installation et opération de variateurs de vitesse) ou leur équivalent en vigueur dans votre pays.

⚠ Avertissement

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠️ Avertissement

COMPOURTEMENT INATTENDU DE L'EQUIPEMENT, PERTE DE CONTROLE, PERTE DE DONNEES

Les instructions fournies dans le présent document doivent être lues, comprises et suivies par toute personne qui possède, conçoit, utilise et/ou entretient un équipement utilisant Ecostruxure Control Expert.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Marques commerciales

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant sur les produits eux-mêmes proviennent généralement des normes internationales.

Dans le domaine des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, il s'agit par exemple de termes tels que *sécurité, fonction de sécurité, état sécurisé, défaut, réinitialisation de défaut, dysfonctionnement, panne, erreur, message d'erreur, dangereux*, etc.

Ces normes incluent entre autres les éléments suivants :

Norme	Description
IEC 61131-2:2007	Automates programmables, partie 2 : Spécifications et essais des équipements.
ISO 13849-1:2023	Sécurité des machines : Composants liés à la sécurité dans les systèmes de commande. Principes généraux de conception
EN 61496-1:2020	Sécurité des machines : Equipement de protection électrosensible. Partie 1 : Exigences générales et tests.
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Equipement électrique des machines - Partie 1 : exigences générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix

Norme	Description
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2021	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmables relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences concernant la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Configuration logicielle requise.
IEC 61784-3:2021	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain liés à la sécurité fonctionnelle - Règles générales et définitions de profil.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes utilisés dans le présent document peuvent provenir d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* peut être utilisé dans le contexte de la description de dangers spécifiques et a la même signification que *zone à risque* ou *zone dangereuse* dans la directive *Machines (2006/42/EC)* et *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Informations concernant la terminologie inclusive/sensible

Schneider Electric s'efforce de mettre constamment à jour ses communications et ses produits pour respecter ses engagements en matière de terminologie inclusive/sensible. Il se peut malgré tout que nos contenus présentent encore des termes jugés inappropriés par certains clients.

Présentation

Introduction

L'objectif de ce document est de présenter les solutions de cybersécurité mises en œuvre dans les contrôleurs Modicon et les applications logicielles associées. Outre les solutions présentées dans ce document, appliquez les directives fournies dans les notes techniques de cybersécurité de Schneider Electric disponibles sur [Schneider Electric website](#).

Recommandations de Schneider Electric

Introduction

Votre système PC peut exécuter différentes applications destinées à améliorer la sécurité de votre environnement de contrôle. Le système présente à sa sortie d'usine des réglages par défaut qui doivent être reconfigurés afin de répondre aux directives de renforcement de la protection des équipements liées à l'approche de défense en profondeur de Schneider Electric.

Une rubrique dédiée à la cybersécurité est disponible dans la zone d'assistance du site Web de Schneider Electric.

Approche de défense en profondeur

Outre les solutions présentées dans le présent document, respectez l'approche Schneider Electric de défense en profondeur décrite dans les documents suivants :

- **Titre du document** : How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations
- **Description du lien de site Web (document)** : How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures?

Gestion des vulnérabilités

Les vulnérabilités signalées par les équipements Schneider Electric sont documentées dans la page Web <http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page>.

Vous pouvez accéder à la liste des notifications de sécurité en cliquant sur le lien **Security Notifications** qui ouvre la page <https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp>.

Si vous observez un incident de cybersécurité ou une vulnérabilité qui ne figure pas dans la liste fournie par Schneider Electric, vous pouvez le signaler en cliquant sur **Signaler une vulnérabilité** dans la page Web **Support de cybersécurité** pour ouvrir la page suivante : <https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp>

Comment sécuriser l'architecture

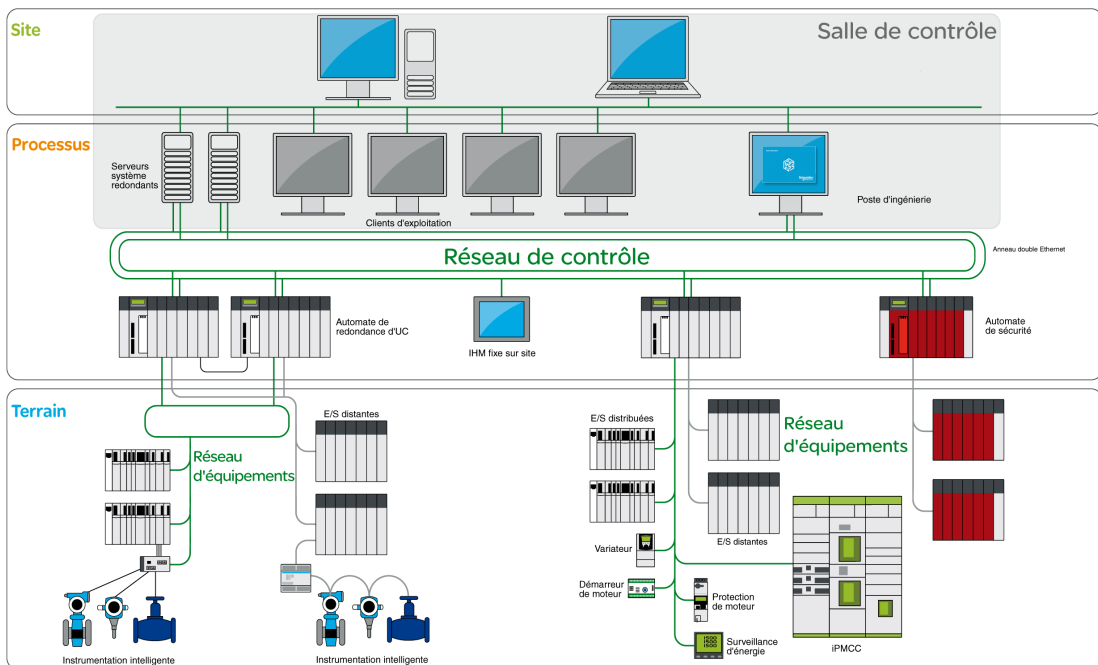
Introduction

Ce chapitre explique comment sécuriser au maximum les contrôleurs Modicon.

Vue Système

Architecture du système

L'architecture ci-après souligne la nécessité d'avoir plusieurs couches (avec un réseau de contrôle et un réseau d'équipements) permettant une meilleure sécurisation. Une architecture plate (avec tous les équipements connectés au même réseau) n'est pas sécurisable.



Communication plus sécurisée

Les équipements situés dans la salle de commande sont plus vulnérables aux attaques que ceux qui sont connectés au réseau d'équipements. Par conséquent, vous devez mieux sécuriser la communication entre la salle de contrôle d'une part, le contrôleur et les équipements d'autre part. Isolez le réseau d'équipements des autres niveaux de réseau (comme les réseaux de contrôle et les réseaux distants).

Dans l'architecture système ci-dessus, la zone de la salle de contrôle est grisée pour la distinguer du contrôleur et des autres équipements.

Accès plus sécurisé aux ports USB

L'accès physique aux ports USB doit être contrôlé.

NOTE: La sécurisation des ports USB ne peut être réalisée que par des moyens physiques (par exemple, armoire ou clé physique).

Accès plus sécurisé à la liaison de redondance d'UC et au réseau d'équipements

Contrôlez l'accès physique à la liaison de redondance d'UC et au réseau d'équipements.

Test

Control Expert fournit un simulateur permettant de tester l'application avant de la mettre en service dans le cadre de votre système d'automatisme industriel. Ce simulateur est conforme aux exigences de cybersécurité suivantes :

- Le simulateur ne peut être utilisé qu'avec une application ouverte dans Control Expert.
- L'application ouverte dans le simulateur ne peut pas être chargée du simulateur vers le contrôleur.

Pour plus d'informations sur l'utilisation du simulateur, consultez l'aide du *Simulateur de contrôleur Ecostruxure™ Control Expert* (<https://youtu.be/RrkorSe0G8s>).

Définition des mots de passe dans Control Expert

Utilisez le logiciel Control Expert pour définir des mots de passe qui permettent de sécuriser votre projet. Les mots de passe suivants peuvent être définis :

- Mot de passe de l'application, avec ou sans chiffrement de fichier
- Mot de passe de zone liée à la sécurité
- Mot de passe de mise à niveau du micrologiciel
- Mot de passe de l'unité de programme, de la section et du sous-programme
- Mot de passe de stockage de données/Web

Mot de passe de l'application

Control Expert comporte une fonction de protection par mot de passe qui empêche tout accès non autorisé à l'application. Control Expert demande le mot de passe lorsque :

- Vous ouvrez l'application dans Control Expert
- Vous vous connectez au contrôleur dans Control Expert.

La protection de l'application par un mot de passe permet d'empêcher la modification, le téléchargement et l'ouverture indésirables des fichiers d'application. Le mot de passe est stocké de manière chiffrée dans l'application.

En plus de cette protection par mot de passe, vous pouvez chiffrer les fichiers .STU, .STA et .ZEF. La fonction de chiffrement de fichiers de Control Expert permet d'empêcher toute modification par du personnel non qualifié et renforce la protection contre le vol de propriété intellectuelle et d'autres actes de malveillance. L'option de chiffrement de fichier est protégée par un mécanisme de mot de passe.

NOTE: Lorsqu'un contrôleur est géré dans le cadre d'un projet système, le mot de passe de l'application et le chiffrement de fichier sont désactivés dans l'éditeur Control Expert et doivent être gérés à l'aide de Topology Manager.

Pour plus d'informations sur la définition et l'utilisation des mots de passe d'application, consultez la rubrique *Protection des applications* du manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Mot de passe de zone liée à la sécurité

Les contrôleurs de sécurité incluent une fonction de protection par mot de passe de la zone liée à la sécurité, accessible depuis l'écran **Propriétés** projet. Cette fonction permet de protéger les éléments du projet situés dans la zone liée à la sécurité du projet de sécurité fonctionnelle.

Lorsque la fonction de protection par mot de passe de la zone liée à la sécurité est active, les parties de l'application qui sont liées à la sécurité ne peuvent pas être modifiées.

Pour plus d'informations sur la définition et l'utilisation des mots de passe de zone liée à la sécurité, consultez la rubrique *Protection par mot de passe de la zone sécurisée* dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Mot de passe de mise à jour du micrologiciel

La protection du micrologiciel par un mot de passe permet d'empêcher tout accès indésirable au micrologiciel du module.

Pour les contrôleurs M580, la gestion des mises à jour du micrologiciel dépend de la version de micrologiciel utilisée pour créer l'application.

- Pour les versions de micrologiciel de contrôleur antérieures à 4.01 :
 - La mise à jour du micrologiciel est gérée à l'aide de FTP.
 - L'accès à la mise à jour du micrologiciel *peut* être protégé par un mot de passe.
- Pour les versions de micrologiciel de contrôleur 4.01 et ultérieures :
 - L'accès à la mise à jour du micrologiciel est géré à l'aide de HTTPS (plus sécurisé que FTP).
 - L'accès à la mise à jour du micrologiciel *doit* être protégé par un mot de passe.
 - L'accès au stockage des données et aux pages Web est protégé par le même mot de passe.

Pour plus d'informations sur la définition et l'utilisation des mots de passe de micrologiciel, consultez la rubrique *Protection du micrologiciel* dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Mot de passe d'unité de programme, de section et de sous-programme

La fonction de protection de l'unité de programme, des sections et des sous-programmes (si elle est activée) utilise un mot de passe pour protéger ces éléments de programme. Cette fonction est paramétrable et accessible dans l'écran Propriétés du projet en mode déconnecté (hors ligne).

Pour plus d'informations sur la définition et l'utilisation des mots de passe d'unité de programme, de section et de sous-programme, consultez la rubrique *Protection d'unité de programme, de section et de sous-programme* dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Mot de passe de stockage de données/Web

La protection par mot de passe permet d'empêcher tout accès indésirable à la zone de stockage des données de la carte mémoire SD (lorsqu'une carte valide est insérée dans le contrôleur).

Pour les contrôleurs M580 d'un projet créé par Control Expert, en fonction de la version :

- Version antérieure à 15.1 : vous pouvez fournir une protection par mot de passe pour l'accès au stockage des données.
- A partir de la version 15.1, vous pouvez fournir une protection par mot de passe pour l'accès aux diagnostics Web et au stockage des données.

Pour les contrôleurs M580, la gestion du stockage des données et des interfaces Web dépend de la version de micrologiciel contrôleur utilisée pour créer l'application :

- Pour les versions de micrologiciel de contrôleur antérieures à 4.01 :
 - Le stockage des données est géré à l'aide de FTP.
 - L'accès au stockage des données *peut* être protégé par un mot de passe.
 - L'accès aux pages Web ne peut pas être protégé par un mot de passe.
- Pour les versions de micrologiciel de contrôleur 4.01 et ultérieures :
 - Le stockage des données est géré à l'aide de HTTPS (plus sécurisé que FTP).
 - L'accès au stockage des données et aux pages Web *doit* être protégé par un mot de passe.
 - L'accès au stockage des données et aux pages Web est protégé par le même mot de passe.

Pour plus d'informations sur la définition et l'utilisation de mots de passe d'accès au stockage des données/Web, consultez la rubrique *Protection du stockage de données/Web* dans le manuel *EcoStruxure™ Control Expert - Modes de fonctionnement*.

Sécurisation renforcée du PC

Les PC situés dans la salle de contrôle sont très exposés aux attaques. Ceux qui prennent en charge EcoStruxure™ Control Expert ou EcoStruxure™ Server Expert nécessitent une sécurisation renforcée.

Ces applications étant toutes exécutées sous le système d'exploitation Windows, ce chapitre fournit des instructions sur la manière de renforcer un PC en se concentrant sur la sécurité pour Windows 10.

Renforcement de la station de travail d'ingénierie

Les fonctions principales suivantes permettent de sécuriser le poste de travail. Cliquez sur un élément pour en savoir plus sur cette fonction :

- Réduction de la surface d'attaque, page 24
- Configuration et vérification de la stratégie de sécurité, page 25
- Gestion des comptes d'utilisateur, page 25
- Gestion du contrôle d'accès, page 26
- Sécurisation des services réseau, page 27, notamment :
 - Désactivation du protocole RDP (Remote Desktop Protocol), page 28
 - Désactivation de LANMAN et NTLM, page 28
 - Désactivation des cartes d'interface réseau inutilisées, page 28
 - Configuration de la connexion au réseau local, page 29
- Activation ou installation d'une protection antivirus, page 29
- Gestion systématique des correctifs, page 30
- Gestion des sauvegardes, page 30
- Gestion de la confidentialité, page 31
- Gestion des audits, page 31

Cette rubrique comprend également des références à plusieurs guides de configuration de la cybersécurité sous Windows 10, page 31.

Réduction de la surface d'attaque

La surface d'attaque de votre système en réseau est l'ensemble des zones où un intrus peut tenter d'ajouter ou d'extraire des données.

Pour réduire la surface d'attaque potentielle, procédez comme suit :

- Désactivez toutes les applications logicielles, tous les services et tous les ports de communication qui ne sont pas utilisés.
- Désactivez ou limitez l'accès aux périphériques de stockage amovibles (USB, par exemple).
- Utilisez le poste de travail pour une seule fonction (par exemple, installez OPC UA Server Expert et Control Expert sur différents PC).

Configuration et vérification de la stratégie de sécurité

La stratégie de sécurité Windows peut être définie via des objets de stratégie de groupe.

Un objet de stratégie de groupe (GPO) est un ensemble de modifications de configuration qui peuvent être appliquées à un poste de travail PC. Pour plus d'informations sur l'Editeur de stratégie de groupe local, consultez les guides de configuration de la sécurité du Centre pour la sécurité Internet (CIS) référencés ci-dessous., page 31

Les objets GPO de domaine peuvent également être définis dans Windows Active Directory.

Les configurations de sécurité doivent être vérifiées régulièrement et automatiquement.

Gestion des comptes d'utilisateur

- **Modifier les mots de passe par défaut :**

Avant de déployer un nouvel actif, remplacez tous les mots de passe par défaut par des valeurs cohérentes avec les comptes de niveau administratif.

Désactivez la connexion automatique à Windows.

Pour obtenir une description des paramètres de mot de passe du compte Windows, consultez les guides de configuration de la sécurité du Centre pour la sécurité Internet (CIS) référencés ci-dessous., page 31

- **Configuration des comptes d'utilisateur :**

Les comptes d'utilisateur peuvent être définis localement (groupe de travail) sur un ordinateur autonome ou via un contrôleur de domaine Windows Active Directory qui permet de centraliser la gestion de tous les utilisateurs d'un système.

Suivez les recommandations suivantes lors de la configuration des comptes d'utilisateur :

- Utilisez un compte d'utilisateur individuel standard (sans privilège d'administrateur) pour utiliser les applications logicielles configurées pour s'exécuter en tant qu'applications autonomes (par exemple, Control Expert).
- Utilisez un compte système local pour les applications logicielles configurées pour s'exécuter en tant que service (par exemple, OFS UA).
- Utilisez un compte d'administrateur dédié pour installer les applications logicielles et configurer IPSec.
- Configurez un gestionnaire de mots de passe pour gérer vos mots de passe (par exemple, KeyPass).
- Désactivez tous les comptes qui ne sont pas associés à une entreprise (par exemple, les comptes de débogage). Voir Commande CIS 16.8, page 31.
- Désactivez automatiquement les comptes inactifs après une période d'inactivité définie. Voir Commande CIS 16.9, page 31.
- Verrouillez automatiquement les sessions des stations de travail après une période d'inactivité standard. Voir Commande CIS 16.11, page 31.

Gestion du contrôle d'accès

Il est nécessaire de contrôler l'accès à toutes les informations stockées sur les systèmes avec système de fichiers, partage réseau, revendications, application ou base de données. Ces contrôles appliquent le **principe du moindre privilège**, selon lequel seuls les individus autorisés peuvent accéder aux informations et les informations auxquelles ils ont accès sont celles dont ils ont le moins besoin compte tenu de leurs responsabilités.

Les **autorisations** sont liées aux objets. Selon les objets, l'autorisation peut être mise en œuvre en fonction :

- des objets Windows Active Directory ;
- de l'accès aux fichiers NTFS via une liste de contrôle d'accès discrétionnaire (DACL) ;
- des autorisations de dossier partagé ;
- le service Registre à distance (activation/désactivation).

Les **privilèges** sont des droits d'utilisateur qui ne sont pas liés à un objet, mais qui sont propres à la machine. Ils peuvent être gérés via les paramètres de la stratégie de groupe, par exemple, les paramètres "Accès au stockage amovible" dans l'éditeur de stratégie de

groupe local peuvent restreindre l'accès au stockage de périphériques USB (en lecture ou en écriture).

Sécurisation des services réseau

Désinstallez ou désactivez les services réseau inutiles ou inutilisés.

Il existe plusieurs façons de désactiver un service (outil Services, modèle de sécurité, objet de stratégie de groupe, PowerShell, SC.exe).

Utilisez le pare-feu Windows avec une règle de refus par défaut qui supprime tout le trafic à l'exception des services et des ports explicitement autorisés.

- **Utilisation du pare-feu :**

Le pare-feu Windows est nécessaire pour la configuration IPSEC sous Windows 10. Dans les versions récentes des systèmes d'exploitation Windows, y compris Windows 10, le pare-feu est activé par défaut. Pour plus d'informations sur les paramètres du pare-feu Windows, consultez les guides de configuration de la sécurité du Centre pour la sécurité Internet (CIS) référencé ci-dessous.

- **Outil Server Manager :**

Serveur Manager vous permet d'afficher toutes les dépendances d'une fonction afin de déterminer s'il convient de la supprimer d'un serveur Windows.

Les rôles de serveur peuvent être sélectionnés (par exemple, Serveur Web (IIS), Serveur DNS, etc.).

Les fonctions du serveur peuvent être sélectionnées (par exemple, BitLocker, .NET Framework, etc.).

- **Internet Information Server (IIS) - Sécurité du serveur Web :**

Utilisez une installation minimale de la dernière version.

Configurez le contrôle d'accès IIS (TLS et authentification utilisateur).

Activez la consignation et recherchez les signatures de piratage dans les journaux.

Vous trouverez plus de détails sur les paramètres d'IIS dans le document de référence CIS (cliquez sur le lien ci-dessous), page 31.

- **Désactivation de SMBv1 :**

Server Message Block version 1 (SMBv1) est un protocole utilisé pour partager des services (tels que l'impression, les fichiers et la communication) entre des PC d'un réseau. Il est prouvé que SMBv1 présente la vulnérabilité d'autoriser l'exécution de code à distance sur le PC hôte.

Vous pouvez désactiver SMBv1 pour réduire les vulnérabilités.

Désactivation du protocole RDP (Bureau à distance)

Les recommandations de Schneider Electric en matière de défense en profondeur incluent la désactivation du protocole RDP (Remote Desktop Protocol) lorsque l'application n'a pas absolument besoin de RDP. La procédure ci-dessous décrit comment désactiver ce protocole :

Etape	Action
1	Dans Windows 10, désactivez RDP dans Ordinateur > Propriétés du système > Paramètres avancés du système .
2	Dans l'onglet Utilisation à distance , désélectionnez la case à cocher Autoriser les connexions d'assistance à distance vers cet ordinateur .
3	Cochez la case Ne pas autoriser les connexions à cet ordinateur .

Désactivation de LANMAN et de NTLM

Désactivez les deux protocoles Microsoft LAN Manager (LANMAN) et son successeur NT LAN Manager (NTLM)) pour réduire les vulnérabilités.

La procédure suivante explique comment désactiver LANMAN et NTLM dans un système Windows 10 :

Etape	Action
1	Dans une fenêtre de commande, exécutez <code>secpol.msc</code> pour ouvrir la fenêtre Stratégie de sécurité locale .
2	Ouvrez Paramètres de sécurité > Stratégies locales > Options de sécurité .
3	Sélectionnez Envoyer réponse NTLMv2 uniquement Refuser LM et NTLM dans le champ Sécurité réseau : Niveau d'authentification du gestionnaire de réseau local .
4	Cochez l'option Sécurité réseau : Ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe .
5	Dans une fenêtre de commande, entrez <code>gpupdate</code> pour valider la stratégie de sécurité modifiée.

Désactivation des cartes d'interface réseau inutilisées

Désactivez les cartes d'interface de réseau non requises par l'application. Par exemple, si votre système compte deux cartes et que l'application n'en utilise qu'une, vérifiez que l'autre (Connexion au réseau local 2) est désactivée.

Pour désactiver une carte réseau sous Windows 10, procédez comme suit :

Etape	Action
1	Ouvrez Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de carte.
2	Cliquez avec le bouton droit de la souris sur la connexion non utilisée. Sélectionnez Désactiver .

Configuration de la connexion au réseau local

Divers paramètres réseau de Windows permettent de renforcer la sécurité pour l'aligner sur l'approche de défense en profondeur.

Sur les systèmes Windows 10, vous accédez à ces paramètres en sélectionnant **Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte > Connexion au réseau local (x).**

Cette liste montre des exemples de modification de la configuration que vous pouvez effectuer sur votre système via l'écran **Propriétés de la connexion au réseau local** :

- Désactivez toutes les piles IPv6 sur leurs cartes réseau respectives.
- Désélectionnez tous les éléments dans **Propriétés de la connexion au réseau local** sauf **Planificateur de paquets QoS** et **Internet Protocol Version 4**.
- Dans l'onglet **Wins** de **Paramètres TCP/IP avancés**, désélectionnez les cases à cocher **Activer la recherche LMHOSTS** et **Désactiver NetBIOS sur TCP/IP**.
- Activez **Partage de fichiers et d'imprimantes pour le réseau Microsoft**.

L'approche de défense en profondeur de Schneider Electric inclut également les recommandations suivantes :

- Ne définissez que des adresses, masques de sous-réseau et passerelles IPv4 statiques.
- N'utilisez pas DHCP ou DNS dans la salle de contrôle.

Activation ou installation de protections antivirus

Vous pouvez améliorer la réponse du système contre les virus et le code malveillant à l'aide des outils intégrés dans Windows 10. Vous pouvez également installer un logiciel antivirus supplémentaire, si nécessaire.

Les éditions professionnelles de Windows 10 incluent *Windows Defender Advanced Threat Protection*, une plate-forme de sécurité qui surveille les points de terminaison tels que les PC Windows 10 utilisant des capteurs comportementaux. La technologie *SmartScreen* de Microsoft est une autre fonctionnalité intégrée qui analyse, télécharge et bloque l'accès aux sites Web et téléchargements réputés malveillants.

Pour plus d'informations sur les paramètres de *Windows Defender*, consultez le document du Centre pour la sécurité Internet (CIS) référencé ci-dessous, notamment :

- Assurez-vous que le logiciel anti-programme malveillant de l'entreprise met régulièrement à jour son moteur d'analyse et sa base de données de signatures (Commande CIS 8.2).
- Configurez la recherche anti-programme malveillant sur les supports amovibles : USB (consultez la section Commande CIS 8.4)., page 31
- Configurez les périphériques pour qu'ils n'exécutent pas automatiquement le contenu situé sur un support amovible : USB (Consultez la section Commande CIS 8.5)., page 31

Gestion systématique des correctifs

Installez toujours la dernière version stable de toutes les mises à jour liées à la sécurité du système d'exploitation, des applications (y compris les navigateurs Web et le client de messagerie), des pilotes.

Activez la mise à jour automatique sous Windows 10.

Pour plus d'informations, consultez le document du Centre pour la sécurité Internet (CIS) référencé ci-dessous., page 31

Gestion de la sauvegarde

Assurez-vous que :

- Toutes les données du système sont sauvegardées automatiquement et régulièrement (voir la section Commande CIS 10.1), page 31.
- Les systèmes clés de l'entreprise sont sauvegardés sous forme de système complet, par le biais de processus tels que l'imagerie, pour permettre la récupération rapide de l'ensemble du système. (Voir Commande CIS 10.2)., page 31
- Les sauvegardes sont protégées de manière appropriée, par la sécurité physique ou par chiffrement, lorsqu'elles sont stockées mais aussi lorsqu'elles sont déplacées sur le réseau. Cela inclut les sauvegardes à distance et les services cloud. (Voir Commande CIS 10.4)., page 31
- Toutes les sauvegardes ont au moins une destination de sauvegarde hors ligne (non accessible via une connexion réseau) (voir Commande CIS 10.5), page 31.

Vous pouvez :

- Utiliser l'outil *Historique des fichiers* et d'autres outils gratuits de Windows 10 pour créer des sauvegardes de fichiers.

- Créer un lecteur de récupération pour restaurer votre système à partir d'une sauvegarde d'image.
- Utiliser un service de synchronisation et de partage du stockage pour placer vos sauvegardes dans le cloud, par exemple *OneDrive*, *Dropbox* ou *Google Drive*.

Pour plus d'informations sur l'outil Historique des fichiers de Windows et les paramètres de sauvegarde/restauration disponibles, consultez la documentation CIS référencée ci-après.

Gestion de la confidentialité

Supprimez du réseau les données sensibles ou les systèmes non régulièrement consultés par l'entreprise. Ces systèmes peuvent être utilisés en tant que systèmes autonomes (déconnectés du réseau) de la division qui doit parfois les utiliser, ou virtualisés et mis hors tension jusqu'à ce que cela soit nécessaire. Consultez le document CIS référencé ci-dessous. (Voir Commande CIS 13.2)., page 31

Activez le chiffrement de disque avec *Bitlocker*. Pour plus d'informations sur les paramètres de *Bitlocker*, consultez la documentation CIS référencée ci-après.

Gestion des audits

Assurez-vous que la journalisation de la sécurité locale a été configurée sur les hôtes Windows. Pour plus d'informations sur la configuration de la stratégie d'audit, consultez la documentation CIS référencée ci-après, page 31.

Guides de configuration de la Cybersécurité sous Windows 10

Assurez-vous de disposer d'un ensemble complet de paramètres de Cybersécurité Windows 10 pour utiliser les guides de configuration Windows, notamment :

- Guides de configuration de la sécurité du Centre pour la sécurité Internet (CIS)
<https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/>
 - Niveau IG1 :
<https://www.cisecurity.org/cis-benchmarks/>
https://www.cisecurity.org/benchmark/microsoft_windows_desktop/
https://www.cisecurity.org/benchmark/microsoft_iis/

- Consignes pour la configuration de la sécurité, élaborées par le ministère américain de la Défense (DISA STIG)

https://www.stigviewer.com/stig/windows_10/2020-06-15/

Les documents "CIS benchmark" et "STIG Windows 10 Security technical implementation guide" proposent des profils facultatifs. Le choix d'un profil dépend de la criticité de vos applications exécutées sous Windows.

Désactiver les services de communication intégrés inutilisés

Services de communication intégrés

Les services de communication intégrés sont des services de communication IP utilisés en mode serveur sur un produit intégré (par exemple, HTTP ou FTP).

Désactiver les services inutilisés

Pour réduire les risques d'attaque, désactivez tout service intégré qui n'est pas utilisé, par exemple HTTP et FTP, afin de fermer les portes de communication potentielles.

Désactiver les services Ethernet dans Control Expert

Vous pouvez activer/désactiver des services Ethernet à l'aide des onglets Ethernet de control Expert. Une description de ces onglets est fournie pour les plates-formes suivantes :

- Modicon M340, page 136
- Modicon M580, page 136
- Modicon Quantum, page 136
- Modicon X80 modules, page 138
- Modicon Premium/Atrium, page 141
- Modicon Momentum MDI, page 142
- Modicon MC80, page 142

Configurez les paramètres des onglets Ethernet avant de télécharger l'application sur le contrôleur.

Les paramètres par défaut (sécurité maximale) réduisent les capacités de communication. Si des services sont requis, vous devez les activer.

NOTE: Sur certains produits, le bloc fonction `ETH_PORT_CTRL` (see `EcoStruxure™ Control Expert, Communication, Block Library`) permet de désactiver un service après la configuration dans l'application Control Expert. Le service peut être réactivé à l'aide du même bloc fonction.

Limiter le flux de données du réseau de contrôle (contrôle d'accès)

Flux de données du réseau de contrôle

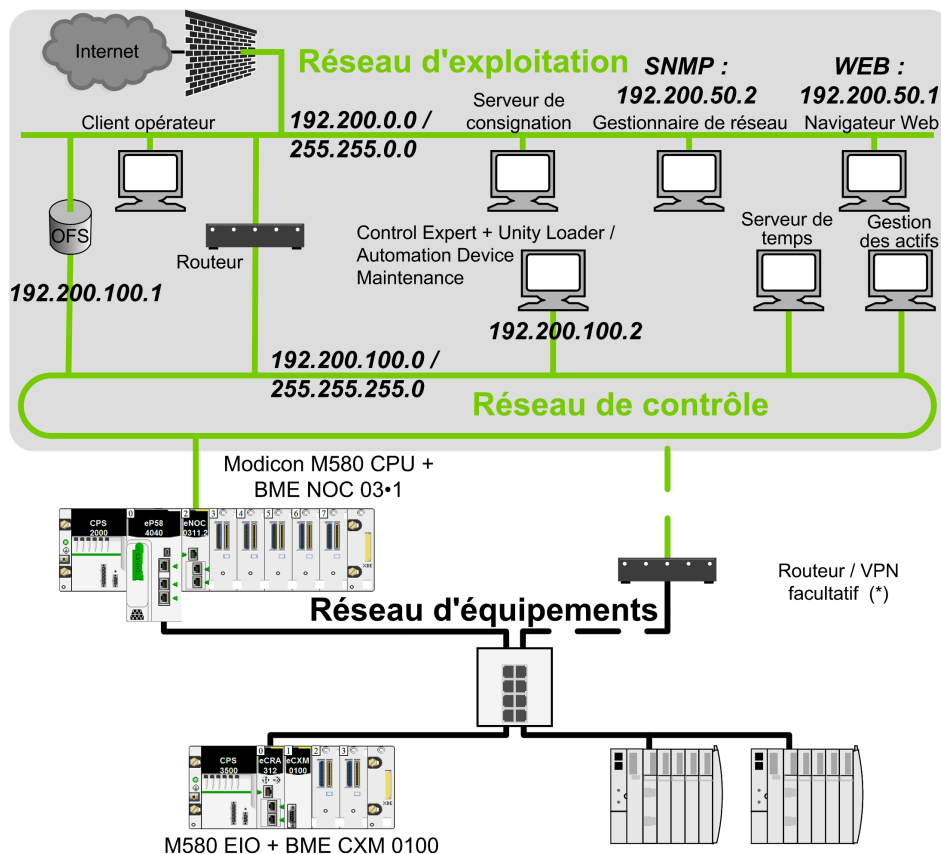
Le flux de données en provenance du réseau de contrôle est un flux IP.

Description

Afin de contrôler l'accès aux serveurs de communication dans un produit intégré, la gestion du contrôle d'accès restreint le flux de données IP en provenance du réseau de contrôle et destiné à une source ou une adresse IP de sous-réseau autorisée.

Exemple d'architecture

La figure suivante montre le rôle et l'impact des paramètres de contrôle d'accès. Le contrôle d'accès gère le flux de données Ethernet en provenance des équipements qui communiquent sur les réseaux d'exploitation et de contrôle (zone grisée).



(*) Certains services nécessitent un accès au réseau d'équipements (par exemple, mise à jour du micrologiciel à l'horodatage de la source). Dans ce cas, un routeur/VPN en option permet de sécuriser le contrôle d'accès.

Configuration des adresses autorisées dans l'exemple d'architecture

Objectifs du contrôle d'accès :

- Tout équipement raccordé au réseau d'exploitation (adresse IP = 192.200.x.x) peut accéder au serveur Web du contrôleur.
- Tout équipement raccordé au réseau de contrôle (adresse IP = 192.200.100.x) peut communiquer avec le contrôleur via Modbus TCP et accéder au serveur Web.

Pour limiter le flux de données dans l'exemple d'architecture précédent, les adresses et services autorisés sont définis comme indiqué dans le tableau de contrôle d'accès EcoStruxure Control Expert suivant :

Source	Adresse IP	Sous-réseau	Masque de sous-réseau	FTP	TFTP	HTTP / HTTPS	Port-502	EIP	SN-MP
Gestionnaire de réseau	192.200.50.2	Non	–	–	–	–	–	–	+
Réseau d'exploitation	192.200.0.0	Oui	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance	192.200.100-.2	Non	–	+ (1)	–	– (2)	+	–	–
Réseau de contrôle	192.200.100-.0	Oui	255.255.255-.0	–	–	–	+	–	–
+ Sélectionné – Non sélectionné ou aucun contenu (1) Pour les versions de micrologiciel M580 supérieures ou égales à v4.10, FTP n'est pas sélectionné. (2) Pour les versions de micrologiciel M580 supérieures ou égales à v4.10, HTTP/HTTPS est sélectionné.									

Description des réglages

Une adresse autorisée est définie pour les équipements autorisés à communiquer avec le contrôleur via Modbus TCP ou EtherNet/IP.

Explication des réglages des services pour chaque adresse IP dans l'exemple ci-dessus :

192.200.50.2 (SNMP)	Défini pour autoriser l'accès à partir du gestionnaire de réseau via SNMP.
192.200.0.0 (HTTP/HTTPS)	Le sous-réseau du réseau d'exploitation est configuré pour autoriser tous les navigateurs Web connectés au réseau d'exploitation à accéder au navigateur Web du contrôleur.
192.200.100.2 (FTP) ⁽¹⁾	Configuré pour autoriser l'accès depuis Automation Device Maintenance via FTP.
192.200.100.0 (Port502)	Le sous-réseau du réseau de contrôle est configuré pour autoriser tous les équipements connectés au réseau de contrôle (OFS, Control Expert, Automation Device Maintenance) à accéder au contrôleur via le Port502 Modbus.
⁽¹⁾ Pour les versions de micrologiciel M580 supérieures ou égales à v4.10, le protocole FTP n'est pas utilisé. Utilisez plutôt HTTP/HTTPS.	

NOTE: L'analyse passe en revue chaque entrée de la liste de contrôle d'accès. Si une correspondance (adresse IP + service autorisé) est trouvée, les autres entrées sont ignorées.

Dans l'écran de **sécurité** EcoStruxure Control Expert pour un sous-réseau dédié, entrez les règles spécifiques avant la règle de sous-réseau. Par exemple : Pour accorder un droit SNMP spécifique à l'équipement 192.200.50.2, saisissez la règle avant la règle globale de sous-réseau 192.200.0.0/255.255.0.0 qui autorise l'accès HTTP à tous les équipements du sous-réseau.

Configuration de la communication chiffrée

Introduction

L'objectif de la communication chiffrée est de protéger les canaux de communication qui permettent d'accéder à distance aux ressources critiques du système (application intégrée Modicon M580 PAC, micrologiciel). IPsec (Internet Protocol Security) est une norme ouverte définie par l'IETF pour fournir des communications protégées et privées sur des réseaux IP en combinant des mécanismes de sécurité de protocole et cryptographiques. Notre

implémentation de la protection IPsec inclut l'anti-reproduction, la vérification de l'intégrité des messages et l'authentification de leur origine.

Le protocole IPsec est pris en charge sur Microsoft Windows 7 et 10. Il est mis œuvre à partir du système d'exploitation du PC.

Description

La fonction IPsec permet de sécuriser :

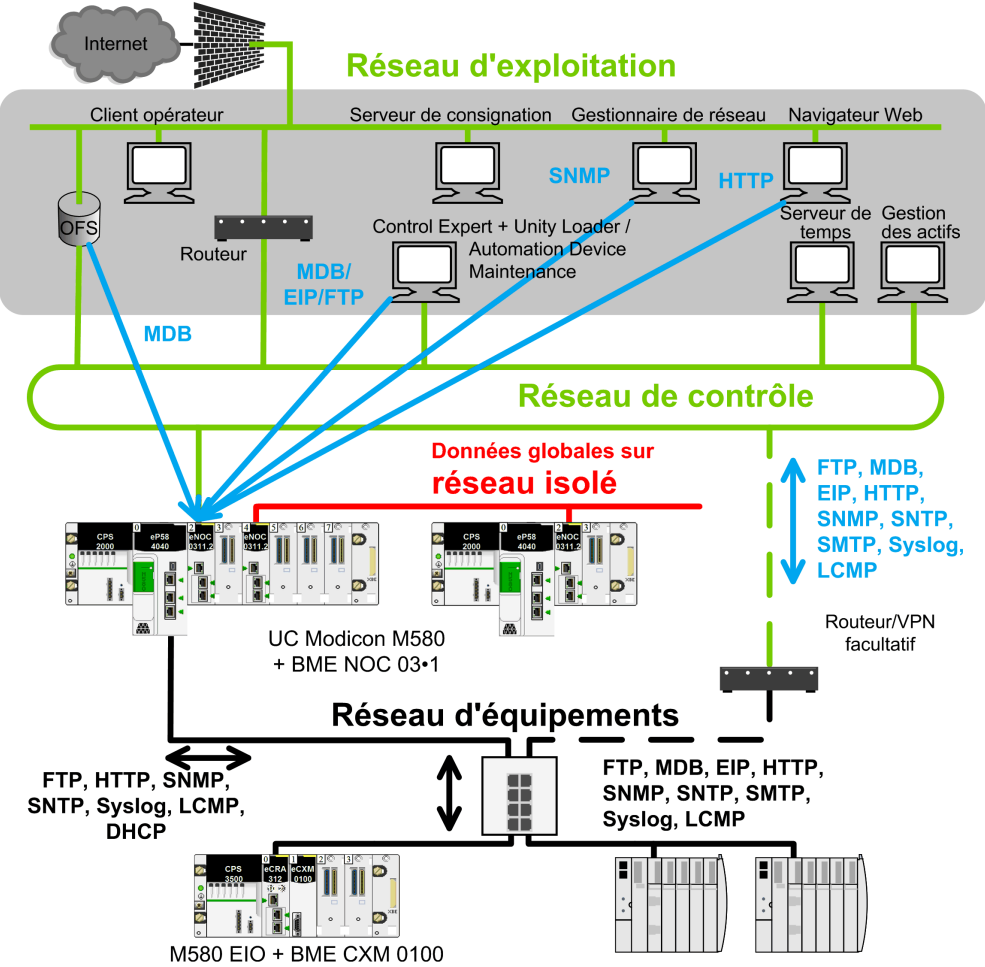
- L'accès Modbus de la salle de contrôle au contrôleur via les modules BMENOC0301 and BMENOC0311.
- L'accès de la salle de contrôle aux services de communication exécutés dans les modules BMENOC0301 and BMENOC0311 en mode serveur (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

NOTE: IPsec vise à sécuriser les services qui s'exécutent en mode serveur dans le contrôleur. Ce manuel n'aborde pas les services clients sécurisés lancés par le PAC Modicon M580.

Connexion sans fil : Lorsqu'un module sans fil PMXNOW0300 est utilisé pour configurer une connexion sans fil, configurez ce module avec les paramètres de sécurité maximum disponibles (WPA2-PSK).

Exemple d'architecture

La figure ci-dessous illustre, à travers un exemple, les différents protocoles ou services impliqués dans une communication chiffrée entre la salle de contrôle et un Modicon M580 controller.



Flux de données avec fonction de communication chiffrée

Utilisez ces services pour faciliter les communications lorsque IPsec est activé :

Service Ethernet	Sécurité des flux de données
Serveur EIP de classe 3	Ces services sont pris en charge par le biais de connexions chiffrées.
Serveur FTP, serveur TFTP	
HTTP	
ICMP	
Serveur Modbus (port 502)	
ARP	Ces services sont pris en charge par le biais de connexions chiffrées et non chiffrées. NOTE: Ce trafic contourne le traitement du protocole IPsec dans le BMENOC et n'utilise donc pas IPsec.
LLDP	
Protocole de vérification de boucle	
Scrutateur Modbus	
RSTP	
DHCP, client BootP	Ces services ne sont pas pris en charge lorsque IPsec est activé. NOTE: Avant l'initialisation de IKE/IPsec par l'homologue (PC), ce trafic n'est pas sécurisé par IPsec. Une fois IKE/IPsec établi, ce trafic est chiffré par IPsec. Le protocole peut être pris en charge, mais uniquement si le destinataire du paquet est un PC avec IPsec configuré et activé.
DHCP, serveur BootP	
EIP classe 1, TCP (requête Forward Open)	
EIP classe 1, UDP (échange de données)	
Client Modbus	
Client NTP	
Agent SNMP	
Interruptions SNMP	
Client Syslog (UDP)	

NOTE:

- IPsec est une protection de couche 3 OSI. Les protocoles de couche 2 OSI (ARP, RSTP, LLDP, protocole de vérification de boucle) ne sont pas protégés par IPsec.
- Les flux de communication de **données globales** (utilisation de modules BMXNGD0100) ne peuvent pas être sécurisés par IPsec. Utilisez cette configuration sur un réseau isolé.

Limites

Limites imposées par IPsec dans l'architecture : les modules BMENOC0301 and BMENOC0311 ne prennent pas en charge le transfert IP vers le réseau d'équipements.

Si la transparence est requise entre le réseau de contrôle et le réseau d'équipements, un routeur/VPN externe est nécessaire pour assurer le chiffrement de la communication entre les deux réseaux (comme indiqué dans l'exemple d'architecture précédent, page 38).

La transparence est requise pour exécuter les opérations suivantes à partir du réseau de contrôle :

- Mettre à jour le micrologiciel d'un contrôleur M580 à partir de Automation Device Maintenance via le service HTTPS.
- Effectuer un diagnostic réseau de contrôleur M580 à partir d'un outil de gestion réseau via le service SNMP.
- Etablir le diagnostic d'un contrôleur M580 à partir d'un DTM via le service EIP.
- Etablir le diagnostic d'un contrôleur M580 à partir d'un navigateur Web via le service HTTP.
- Consigner les événements de cybersécurité d'un contrôleur M580 sur un serveur syslog via le service syslog.
- Synchroniser l'heure d'un contrôleur M580 à partir d'un serveur de temps global via le service NTP.

Configuration de la communication IPsec dans l'architecture système

Procédez comme suit pour configurer la communication IPsec :

- Dans la salle de contrôle, identifiez les applications clientes autorisées qui ont besoin de communiquer avec le système Modicon M580 PAC à l'aide de Modbus (Control Expert, Automation Device Maintenance, OFS, applications du client telles que SGBackup, etc.).

Configurez IPsec sur chaque PC prenant en charge ces applications autorisées.

- Dans la salle de contrôle, identifiez les applications clientes autorisées qui ont besoin de communiquer avec les modules BMENOC0301 and BMENOC0311 configurés dans le rack local (Control Expert DTM, Automation Device Maintenance, gestionnaire SNMP, navigateur Web, concepteur Web pour modules FactoryCast BMENOC0301 and BMENOC0311).

Configurez IPsec sur chaque PC prenant en charge ces applications autorisées.

- Incorporez les modules BMENOC0301 and BMENOC0311 avec fonction IPsec sur l'embase de chaque système Modicon M580 PAC connecté au réseau de contrôle.

Pour configurer la fonction IPsec sur les modules BMENOC0301 and BMENOC0311, procédez en 2 temps :

- Activez la fonction IPsec.
- Configurez une clé pré-partagée. Une clé pré-partagée permet de créer un secret partagé autorisant deux équipements à s'authentifier l'un l'autre.

NOTE: Comme IPsec repose sur ce secret partagé, il s'agit d'un élément clé de la stratégie de sécurité gérée par l'administrateur de la sécurité. Afin de renforcer la sécurité de la clé pré-partagée, utilisez un outil externe tel que KeePass, page 41 pour générer une chaîne de caractères appropriée.

Les modules BMENOC0301 and BMENOC0311 sont configurés à l'aide de Control Expert. Pour sécuriser cette configuration, il est préférable d'effectuer le premier téléchargement via une connexion point à point telle que le port USB. Les téléchargements ultérieurs peuvent être réalisés via Ethernet avec une fonction IPsec, pourvu que IPsec soit activé.

Chaque PC prenant en charge IPsec doit respecter les exigences suivantes pour la configuration IPsec :

- Utiliser le système d'exploitation Microsoft Windows 10.
- Disposer des droits d'administrateur pour configurer IPsec.

Une fois la fonction IPsec configurée, définissez le compte Windows comme un compte utilisateur normal sans privilège d'administrateur.

- **Renforcez le PC comme expliqué dans la section *Sécurisation renforcée du PC*, page 23.**

Pour plus d'informations sur la configuration, consultez la rubrique *Configuration des communications IP sécurisées* (voir Modicon M580 BMENOC0301 / BMENOC0311 - Module de communication Ethernet - Guide d'installation et de configuration).

Générer des clés pré-partagées les plus sécurisées possible

La sécurité des communications IPsec repose sur la complexité de la clé pré-partagée. Utilisez des outils spécialisés pour générer des clés pré-partagées de sécurité optimale.

Un de ces outils est KeePass, que vous pouvez télécharger gratuitement à partir d'Internet. Téléchargez et installez KeePass sur votre PC et lancez-le.

Configurez et utilisez KeePass v2.34 pour générer des mots de passe utilisables en tant que clés pré-partagées :

Etape	Action
1	Créez un nouveau dossier de base de données de clés (File > New).
2	Dans la boîte de dialogue Create New Password Database , entrez un nom de dossier dans le champ File name et enregistrez vos modifications.
3	Dans la boîte de dialogue Create Composite Master Key , entrez un mot de passe dans le champ Master password . Saisissez à nouveau le mot de passe dans le champ Repeat .
4	Choisissez OK pour ouvrir l' étape 2 et appuyez de nouveau sur OK .
5	Dans la boîte de dialogue de la nouvelle base de données, développez New Database .
6	Sélectionnez Network et ajoutez une entrée (Edit > Add Entry).
7	Dans le champ Title , indiquez le nom de votre module (par exemple, eNOC).
8	Dans le champ User name , indiquez un nom d'utilisateur.
9	Cliquez sur l'icône Generate a password .
10	Sélectionnez Open password generator .
11	Appuyez sur OK pour remplir les champs Password et Repeat .
12	Ouvrez la boîte de dialogue Password Generation Options (Tools > Generate Password) .
13	Effectuez les sélections suivantes dans Generate using character set : • Majuscules (A, B, C, ...) • Minuscules (a, b, c, ...) • Chiffres (0, 1, 2, ...) • Signe moins (-) • Trait de soulignement (_) • Caractères spéciaux (!, \$, %, &, ...) • Parenthèses/crochets ([,], [, (,), <, >) NOTE: Les caractères suivants ne sont pas autorisés dans la clé pré-partagée : • { • } • ; • #
14	Appuyez sur OK .
15	Cliquez avec le bouton droit sur votre appareil dans la liste Database et faites défiler jusqu'à Copy Password .
16	Ouvrez l'écran de configuration de la sécurité dans Control Expert.
17	Collez la clé dans l'écran de configuration de la fonction IPsec.

Diagnostiquer la communication IPsec dans l'architecture du système

Pour plus d'informations sur le diagnostic de la fonction IPsec dans l'architecture du système, consultez la rubrique *Configuration des communications IP cryptées* (voir Modicon M580 BMENOC0301 / BMENOC0311 - Module de communication Ethernet - Guide d'installation et de configuration).

Cible de sécurité CSPN

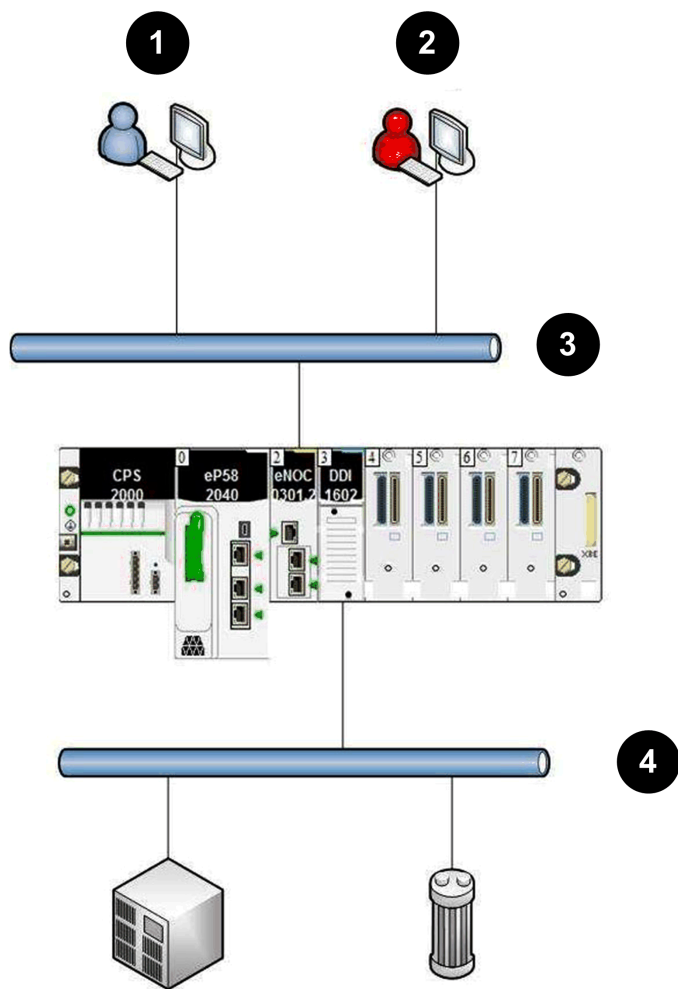
Présentation de la certification CSPN

CSPN (Certification de Sécurité de Premier Niveau) est une certification de cybersécurité actuellement utilisée en France. Un produit certifié CSPN est censé résister à une cyberattaque menée par deux hommes-mois de pirates expérimentés. Le système M580 est certifié CSPN. Cette rubrique décrit l'environnement, les configurations de contrôleur d'automatisme programmable et les paramètres qui répondent aux exigences CSPN pour assurer un niveau optimal de sécurité.

Présentation du système Modicon M580

Le système PAC Modicon M580 est conçu pour contrôler et commander un processus industriel en continu sans intervention humaine. A chaque étape, le contrôleur traite les données reçues de ses entrées, des capteurs, et envoie des commandes à ses sorties, des actionneurs. Les échanges avec la supervision (IHM, SCADA) sont effectués à l'aide de modules de communication Ethernet BMENOC0301 and BMENOC0311 situés avec le contrôleur sur le rack local.

L'illustration suivante décrit une architecture de système M580 classique qui peut être vulnérable à une attaque de sécurité :



Fonctionnalités M580

Le contrôleur M580 offre les fonctionnalités suivantes :

Fonctionnalité	Description
exécution du programme utilisateur	Un contrôleur M580 exécute un programme utilisateur qui traite les entrées et met à jour les sorties.
gestion des entrées/sorties	Un contrôleur M580 peut lire des entrées locales et écrire des sorties locales. Ces entrées/sorties peuvent être numériques ou analogiques et permettent au contrôleur M580 de contrôler et commander le processus industriel.
communication avec la supervision	Un contrôleur M580 peut communiquer avec un système SCADA pour recevoir des commandes et transmettre des données de processus via le protocole Modbus.
fonctions administratives	Un contrôleur M580 intègre des fonctions administratives, fournies dans EcoStruxure Control Expert, à des fins de configuration et de programmation.
consignation à distance	Un contrôleur M580 prend en charge la définition d'une stratégie de consignation à distance ; il peut consigner des événements de sécurité et d'administration.

Configuration M580

Une configuration M580 certifiée CSPN comprend les composants suivants :

Module	Micrologiciel	Description
BMEP58-0-0	à partir de la version 2.20	Le contrôleur suit les règles de sécurité décrites dans les documents de sécurité (voir les hypothèses).
BMENOC0301 and BMENOC0311	à partir de la version 2.11	Ce module Ethernet gère les communications chiffrées avec la couche supérieure (logiciel de supervision et d'ingénierie EcoStruxure Control Expert).

NOTE: Le logiciel de programmation EcoStruxure Control Expert, les PC, les autres modules de contrôleur et les composants d'embase ne sont pas couverts par la certification.

Profils d'utilisateur

Les utilisateurs qui interagissent avec le contrôleur pour une implémentation améliorée présentent les profils EcoStruxure Control Expert Security Editor prédéfinis suivants :

Profil utilisateur	Description
Lecture seule	Aucune modification d'application n'est autorisée.
Exploitation	Seules l'exécution de l'application et la modification de paramètres sont activées.
Programme	Toutes les fonctions sont activées.

Amélioration de la mise en œuvre

Ces éléments contribuent à un environnement sain pour une meilleure mise en œuvre :

Elément	Critères de sécurité
documentation sur la sécurité	Toutes les instructions contenues dans la documentation (guides utilisateur, livres blancs, etc.) sont appliquées avant l'évaluation.
administrateurs	Les administrateurs système sont compétents, formés et dignes de confiance.
locaux	L'accès à l'emplacement du contrôleur est limité aux personnes de confiance. En particulier, un utilisateur malveillant n'a pas accès aux ports physiques des contrôleurs. Comme des produits identiques sont en vente libre, l'utilisateur malveillant peut s'en procurer un et rechercher des vulnérabilités par tous les moyens possibles.
désactivation des services non évalués	Les services ne répondant pas aux impératifs de sécurité sont désactivés dans la configuration ou par un programme utilisateur (comme indiqué dans la documentation de sécurité).
vérification de l'application utilisateur	L'administrateur contrôle l'intégrité de l'application EcoStruxure Control Expert avant son chargement dans le contrôleur.
consignation active	La fonction de consignation est opérationnelle et les journaux ne sont pas endommagés.
Vérification des journaux	Les administrateurs système vérifient régulièrement les journaux locaux et distants.
configuration initiale	La configuration initiale est chargée dans le contrôleur via l'interface USB et le contrôleur est débranché du réseau.
mise à niveau de micrologiciel	La mise à niveau du micrologiciel s'effectue via l'interface USB et le contrôleur est débranché du réseau.
mots de passe renforcés	Les administrateurs système utilisent des mots de passe renforcés, qui combinent des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Modes de fonctionnement

Les modes de fonctionnement suivants sont compatibles avec les exigences CSPN :

- Pendant la phase de mise en service, la configuration initiale du contrôleur peut être effectuée avec une station d'ingénierie Control Expert connectée soit en point à point au port Ethernet, soit au port USB local du contrôleur.
- Dans les conditions de fonctionnement normal (mode d'exécution, SCADA connecté au réseau de contrôle Ethernet), vérifiez que Control Expert est déconnecté.
- Effectuez toute modification ultérieure de la configuration ou du programme d'application avec Control Expert connecté au port USB du contrôleur.

Paramètres de Cybersécurité

Le tableau suivant décrit les paramètres de cybersécurité :

Paramètre	Rubrique	Guide utilisateur
ACL activée.	Configuration des services de sécurité	Modicon M580 BMENOC0301 / BMENOC0311 - Module de communication Ethernet - Guide d'installation et de configuration
IPsec activée sur BMENOC0301/0311 avec le niveau de sécurité maximum.	Configuration des services de sécurité	
Sélection du paramètre Appliquer la sécurité (protocoles FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP désactivés).	Configuration des services de sécurité	
Journal activé.	Consignation d'événements de DTM et de module dans le serveur Syslog	
RUN/STOP par entrée uniquement activé.	Gestion de l'entrée Run/Stop	Guide de référence du matériel M580
Protection de la mémoire activée.	Protection mémoire	
Sécurisation d'un projet : • Application verrouillée avec identifiant et mot de passe. • Protection de section activée.	Sécurisation d'un projet dans Control Expert	
Aucune information de chargement stockée dans le contrôleur.	Données incorporées dans le contrôleur	EcoStruxure™ Control Expert - Modes de fonctionnement
Modification du mot de passe par défaut pour le service FTP.	Protection du micrologiciel	
Sections d'application non accessibles en lecture/écriture.	Protection de sections et de sous-routines	

Equipements critiques

Environnement : Ce tableau indique les actifs critiques pour l'environnement :

Actif	Description pour une utilisation appropriée
contrôle-commande du processus industriel	Le contrôleur contrôle et commande un processus industriel en lisant les entrées et en envoyant des commandes à des actionneurs. La disponibilité de ces actions fait l'objet d'une protection.
flux du poste d'ingénierie	Les flux entre le contrôleur et le poste de travail d'ingénierie sont protégés en termes d'intégrité, de confidentialité et d'authenticité.

Exigences de sécurité concernant les actifs critiques par rapport à l'environnement :

Actif	Disponibilité	Confidentialité	Intégrité	Authenticité
contrôle-commande du processus industriel	X			
flux du poste de travail d'ingénierie		X	X	X

contrôleur : Le tableau suivant présente les actifs critiques pour les contrôleurs :

Actif	Description pour une utilisation appropriée
micrologiciel	L'intégrité et l'authenticité du micrologiciel sont protégées.
mémoire du contrôleur	La mémoire du contrôleur contient la configuration de ce dernier ainsi qu'un programme chargé par l'utilisateur. Son intégrité et son authenticité sont protégées pendant l'exécution.
mode d'exécution	L'intégrité et l'authenticité du mode d'exécution du contrôleur sont protégées.
secrets d'utilisateur	Les utilisateurs concernés ne divulguent pas les mots de passe qu'ils utilisent pour s'authentifier.

Exigences de sécurité concernant les actifs critiques pour le contrôleur :

Actif	Disponibilité	Confidentialité	Intégrité	Authenticité
micrologiciel			X	X
mémoire du contrôleur			X	X
mode d'exécution			X	X
secrets d'utilisateur		X	X	

Menaces pour la sécurité

Menaces par les attaquants contrôlant un équipement connecté au réseau de supervision :

Type de menace	Contrôle-commande du processus industriel	Flux du poste de travail d'ingénierie	Micrologiciel	Mémoire du contrôleur	Mode d'exécution	Secrets d'utilisateur
Refus de service	Di					
Altération du micrologiciel		I, Au				
altération du mode d'exécution					Au, I	
Altération du programme en mémoire				I, Au		
Altération des flux	Di	Au, C, I				C, I
Di : disponibilité I : intégrité C : confidentialité Au : authenticité						

Type de menace	Description
refus de service	L'attaquant parvient à générer un refus de service sur le contrôleur en effectuant une action inattendue ou en explorant une vulnérabilité (envoi d'une requête mal formée, utilisation d'un fichier de configuration corrompu, etc.). Ce refus de service affecte l'ensemble du contrôleur ou certaines de ses fonctions.
altération du micrologiciel	L'attaquant parvient à injecter et exécuter un micrologiciel corrompu sur le contrôleur. L'injection de code peut être temporaire ou permanente et elle ne comprend aucune exécution de code inattendu ou non autorisé. Un utilisateur peut tenter d'installer cette mise à jour sur le contrôleur par des moyens légitimes. Enfin, l'attaquant parvient à modifier la version du micrologiciel installé sur le contrôleur sans en avoir le droit.
altération du mode d'exécution	L'attaquant parvient à modifier le mode d'exécution du contrôleur sans y être autorisé (commande d'arrêt, par exemple).
altération de la mémoire	L'attaquant parvient à modifier (de manière temporaire ou permanente) le programme utilisateur ou la configuration qui s'exécute dans la mémoire du contrôleur.
altération des flux	L'attaquant parvient à altérer les échanges entre le contrôleur et un composant externe sans être détecté. L'attaquant peut notamment effectuer des vols d'informations d'identification, des violations du contrôle d'accès ou des interventions de contrôle-commande sur la modulation du processus industriel.

Type de menace	Refus de service permanent	Altération du micrologiciel	Altération du mode d'exécution	Altération de la mémoire	Altération des flux
gestion des entrées mal formées	X				
stockage des secrets				X	
authentification sur l'interface d'administration					X
stratégie de contrôle d'accès					X
signature de micrologiciel		X			
intégrité et authenticité de la mémoire du contrôleur				X	
intégrité du mode d'exécution du contrôleur			X		
communication plus sécurisée					X

Type de menace	Description
gestion des entrées mal formées	Le contrôleur a été développé pour gérer correctement les entrées mal formées, en particulier sur le trafic réseau.
force des secrets	Le contrôleur a été développé pour gérer correctement les entrées mal formées, en particulier sur le trafic réseau. • PSK utilisé pour monter le tunnel IPsec • Mot de passe d'application utilisé pour lire le fichier Control Expert .STU et connecter ce fichier au contrôleur • Mots de passe d'autres services (comme FTP)
authentification sur l'interface d'administration	Les jetons de session sont protégés contre le piratage et la reproduction ; ils ont une durée de vie brève. L'identité et les autorisations du compte utilisateur sont systématiquement vérifiées avant toute action privilégiée. Un mot de passe d'application est défini dans chaque configuration afin d'empêcher toute modification du contrôleur par un utilisateur non authentique.
stratégie de contrôle d'accès	La stratégie de contrôle d'accès permet de contrôler l'authenticité des opérations privilégiées, lesquelles sont susceptibles de modifier des actifs identifiés comme étant critiques. La liste de contrôle d'accès (ACL) est activée dans chaque configuration et seules les adresses IP identifiées peuvent se connecter au contrôleur.
signature du micrologiciel	Lors de chaque mise à jour de micrologiciel, l'intégrité et l'authenticité du nouveau micrologiciel sont vérifiées avant le lancement de la mise à jour.

Type de menace	Description
intégrité et authenticité de la mémoire du contrôleur	La fonction de protection de la mémoire est activée dans chaque configuration afin d'empêcher la modification du programme en cours d'exécution en l'absence d'action dans des entrées ou des sorties spécifiques. Si aucun module d'entrée/sortie n'est installé, l'interface de programmation est bloquée. Le contrôleur garantit l'intégrité et l'authenticité du programme utilisateur, de sorte que seuls les utilisateurs autorisés puissent le modifier. La protection de la mémoire permet également de garantir la protection de la configuration, ce qui implique plusieurs paramètres de sécurité : • Stratégie de contrôle d'accès. • RUN/STOP par entrée uniquement activé. • Protection de la mémoire activée. • Services activés/désactivés (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP). • Paramètres IPsec. • Paramètres Syslog.
intégrité du mode d'exécution du contrôleur	Le contrôleur garantit que le mode d'exécution peut être modifié uniquement par des utilisateurs autorisés qui ont été authentifiés. La fonction RUN/STOP par entrée uniquement est activée, ce qui empêche toute modification d'état RUN/STOP via l'interface Ethernet.
communication chiffrée	Le contrôleur prend en charge la communication chiffrée, protégée en termes d'intégrité, de confidentialité et d'authenticité (IPsec chiffré avec ESP). Le protocole FTP est désactivé et IPsec sécurise la communication Modbus via les modules BMENOC0301 and BMENOC0311.

Configuration d'un audit de Cybersécurité (consignation des événements)

La consignation des événements et l'analyse des journaux sont essentielles. L'analyse permet de tracer les actions de l'utilisateur en cas de maintenance ou d'événements anormaux susceptibles de révéler une attaque potentielle.

Le système doit être équipé d'un robuste système de consignation englobant tous les équipements. Les événements liés à la cybersécurité sont consignés localement et envoyés à un serveur distant à l'aide du protocole Syslog.

Dans l'architecture du système, la consignation des événements met en œuvre deux parties :

- Un serveur de consignation qui reçoit tous les événements de cybersécurité du système via le protocole Syslog.
- Des clients de consignation (points de connexion Ethernet où les événements de cybersécurité sont surveillés : équipement, Control Expert).

Description du service de consignation des événements

Chaque client de consignation sert à :

- Détecter et horodater les événements.
Une seule référence NTP doit être configurée dans le système pour horodater les événements de cybersécurité.
- Envoyer les événements détectés au serveur de consignation des événements.
Les événements sont échangés entre le client et le serveur à l'aide du protocole Syslog (spécification RFC 5424).
Les messages Syslog respectent le format décrit dans la spécification RFC 5424.
Les échanges Syslog sont effectués avec le protocole TCP.
Sur les équipements, les événements ne sont pas perdus en cas de défaillance temporaire du réseau. Les événements sont perdus en cas de réinitialisation de l'équipement (sauf pour les contrôleurs Modicon M580 équipés d'un micrologiciel de version ≥ 4.0).

Valeurs de catégorie pour les types d'événement

Valeurs de catégorie des messages Syslog selon la spécification RFC 5424 associée aux types d'événements :

Valeur de catégorie	Description
0	Messages du noyau.
1	Messages de niveau utilisateur.
2	Système de messagerie.
3	Démons du système.
4	Messages de sécurité/d'autorisation.
5	Messages générés en interne par Syslog.
6	Sous-système d'impression en ligne.
7	Sous-systèmes d'actualité du réseau.
8	Sous-système UUCP.
9	Démon d'horloge.
10	Messages de sécurité/d'autorisation.
11	Démon FTP.

Valeur de catégorie	Description
12	Sous-système NTP.
13	Historique de consignation.
14	Alerte de consignation.
15	Démon d'horloge.
16 à 23	Utilisation locale 0 à 7.

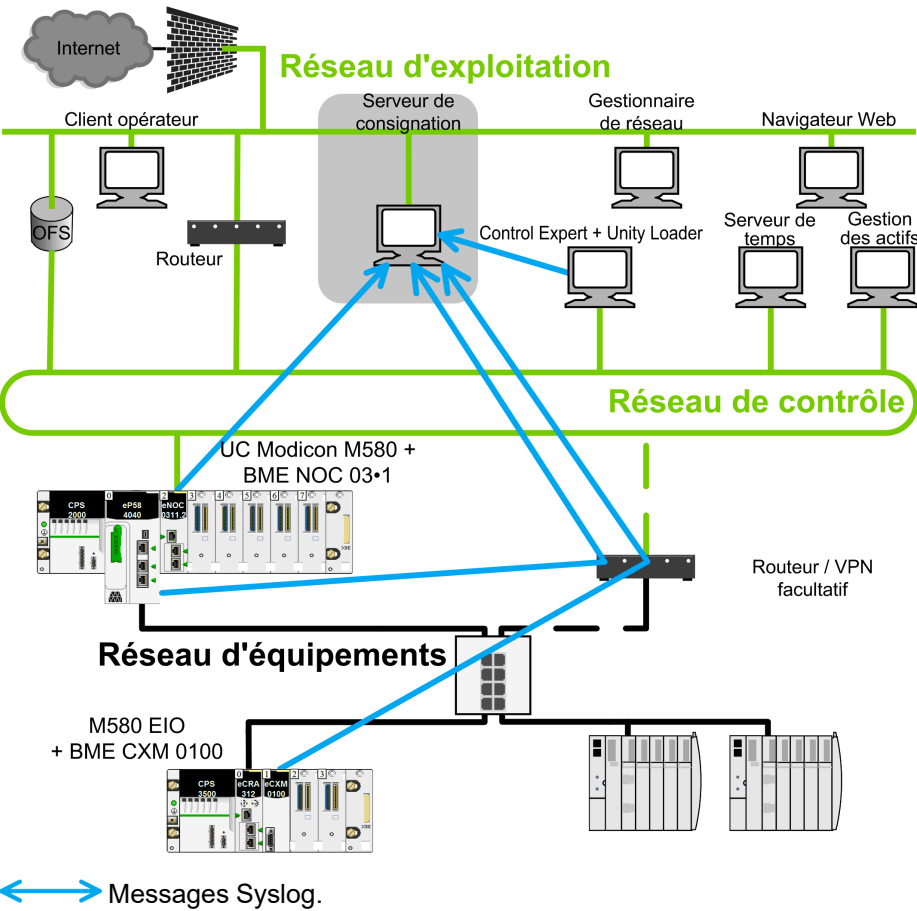
Valeurs de gravité pour les types d'événement

Valeurs de gravité des messages Syslog selon la spécification RFC 5424 associée aux types d'événement :

Valeur de gravité	Mot-clé	Description
0	Emergency	Système inutilisable
1	Alert	Action immédiate requise
2	Critical	Conditions critiques
3	Error	Conditions d'erreur
4	Warning	Conditions consultatives.
5	Notice	Condition normale mais importante
6	Informational	Messages d'information
7	Debug	Messages de mise au point

Exemple d'architecture

La figure suivante montre la position du serveur de consignment dans l'architecture d'un système :



Structure des messages d'événements consignés pour le contrôleur Modicon M580 (à partir de la version 4.10 du micrologiciel) et pour BMENOR2200H (à partir de la version 3.01 du micrologiciel)

Champs	Description
PRI	Informations sur la catégorie et la gravité : "FACILITY" = 10 pour les événements de cybersécurité
VERSION	Version de la spécification du protocole Syslog (Version = 1 pour RFC 5424).
TIMESTAMP	Le format d'horodatage provient de RFC 3339 qui recommande le format de date et d'heure Internet ISO8601 suivant : YYYY-MM-DDThh:mm:ss.nnnZ NOTE: -, T, :, . et Z sont des caractères obligatoires qui font partie du champ d'horodatage. T et Z doivent être écrits en majuscules. Z indique que l'heure est UTC. Description du contenu du champ d'horodatage : • YYYY : Année • MM : Mois • DD : Jour • hh : Heure • mm : Minute • ss : Seconde • nnn : Fraction de seconde en milliseconde (0 si non disponible)
HOSTNAME	Identifie la machine qui a envoyé le message Syslog d'origine : nom de domaine complet (FQDN) ou adresse IP statique source si FQDN n'est pas pris en charge. Adresse @IP source = adresse @IP A OU adresse @IP B dans le cas d'un contrôleur à redondance d'UC (HSBY)
APP-NAME	Identifie l'application qui crée le message Syslog. Il contient des informations qui identifient l'entité qui envoie le message (par exemple, sous-ensemble de référence commerciale).
PROCID	Nom du processus ou du protocole à l'origine du message (par exemple, Modbus, HTTPS, LocalHMI)
MSGID	Identificateur du type de l'événement (par exemple, CONNECTION_FAILURE_AND_BLOCK).
Informations sur l'événement	<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="30296255-e8b7-4cf1-982e-2c45b17b1f06"><ac:plain-text-body><![CDATA[[authn@3833], [authz@3833], [config@3833], [cred@3833], [backup@3833], [plc@3833] [system@3833] Voir la description de STRUCTURED-DATA ci-dessous.
MSG	Message contenant le résultat spécifique à l'événement (voir Description des messages du journal des événements pour Control Expert, page 62)

- Description de **STRUCTURED-DATA** : informations obligatoires sur l'événement.
 - **[meta]** : données structurées obligatoires pour fournir des méta-informations sur le message. Où le paramètre est :
 - **sequenceId** : identifiant de l'événement (passe à 1 lorsque la valeur maximale 2147483647 est atteinte).
 - **sysUpTime** : cette valeur doit être incluse lorsque le composant n'est pas capable d'obtenir l'heure système (entier contenant l'heure au 1/100e de seconde près depuis la dernière réinitialisation du système).

- Description de **STRUCTURED-DATA** : informations sur l'événement en fonction de sa catégorie.
 - **[authn@3833]** : données structurées utilisées pour les événements d'authentification. Où les paramètres sont :
 - **itf** : interface à laquelle l'utilisateur est connecté ; soit un port réseau, soit une interface locale (IHM, USB, etc.).
 - **peer** : nom de domaine complet (FQDN) ou adresse IP du composant à partir duquel l'utilisateur est connecté, plus son port (ipAddress:port), facultatif en cas d'interface locale
 - **user** : nom d'utilisateur (composant ou humain), facultatif si le nom d'utilisateur est inconnu.
 - **[authz@3833]** : données structurées utilisées pour les événements d'autorisation. Où les paramètres sont :
 - **user** : nom d'utilisateur (composant ou humain).
 - **object** : accès à l'objet par l'utilisateur, objet dépendant du produit.
 - **action** : action effectuée sur l'objet : création, lecture, mise à jour, suppression (CRUD)
 - **[config@3833]** : données structurées utilisées pour les événements de configuration. Où les paramètres sont :
 - **object** : nom de l'objet de sécurité à configurer (micrologiciel, RBAC, stratégie de sécurité, paramètres d'équipement, ancre d'approbation, objets dépendants du produit).
 - **value** : version ou valeur facultative du nouvel objet.
 - **[cred@3833]** : données structurées utilisées pour les événements de gestion des informations d'identification. Où les paramètres sont :
 - **name** : nom commun du certificat ou identifiant de connexion de l'utilisateur.
 - **[system@3833]** : données structurées pour les événements système. Où les paramètres sont :
 - **object** : nom de l'objet système qui change (contrôleur, module, commutateur rotatif, carte SD, objet dépendant du produit)
 - **[backup@3833]** : données structurées utilisées pour la sauvegarde. Où les paramètres sont :
 - **object** : partie du composant qui a été sauvegardée/restaurée, objet dépendant du produit.
 - Des données structurées peuvent également être définies par chaque application pour des événements spécifiques.

Structure des messages d'événement consignés pour le contrôleur Modicon M580 (micrologiciel antérieur à la version 4.10), BMENUA0100 (versions de micrologiciel 1.10 et 2.0) et BMENOR2200H (micrologiciel antérieur à la version 3.01)

Structure des messages Syslog pour le contrôleur Modicon M580 et BMENUA0100 :

Champ	Description
PRI	Informations sur la catégorie et la gravité (description fournie dans les tableaux suivants).
VERSION	Version de la spécification du protocole Syslog (Version = 1 pour RFC 5424.).
TIMESTAMP	Le format d'horodatage provient de RFC 3339 qui recommande le format de date et d'heure Internet ISO8601 suivant : YYY-MM-DDThh:mm:ss.nnnZ NOTE: -, T, :, . et Z sont des caractères obligatoires qui font partie du champ d'horodatage. T et Z doivent être écrits en majuscules. Z indique que l'heure est UTC. Description du contenu du champ d'horodatage : • YYY : Année • MM : Mois • DD : Jour • hh : Heure • mm : Minute • ss : Seconde • nnn : Fraction de seconde en milliseconde (0 si non disponible)
HOSTNAME	Identifie la machine qui a envoyé le message Syslog d'origine. Nom de domaine complet (FQDN) ou adresse IP statique source si FQDN n'est pas pris en charge.
APP-NAME	Identifie l'application à l'origine du message Syslog. Il contient des informations identifiant l'entité qui envoie le message (par exemple, un sous-ensemble de la référence commerciale).
PROCID	Nom du processus ou du protocole à l'origine du message (par exemple, Modbus, HTTPS, LocalHMI, etc.) Reçoit la valeur NILVALUE si non utilisé.

Champ	Description
MSGID	Identifie le type de message auquel l'événement est lié, par exemple HTTP, FTP, Modbus. Reçoit la valeur NILVALUE si non utilisé.
MESSAGE TEXT	Ce champ contient : • Adresse de l'émetteur : Adresse IP de l'entité qui génère le journal. • ID d'homologue : ID d'homologue si un homologue est impliqué dans l'opération (par exemple, nom d'utilisateur pour une opération de journalisation). Reçoit la valeur Null s'il n'est pas utilisé. • Adresse de l'homologue : Adresse IP de l'homologue si un homologue est impliqué dans l'opération. Non utilisé (null). • Type : Numéro unique pour identifier un message. • Commentaire : Chaîne décrivant le message (voir Description des messages du journal des événements pour les contrôleurs M580 (à partir de la version de micrologiciel V4.10) et pour BMENOR2200H (à partir de la version de micrologiciel 3.01), page 68).

Configuration d'un serveur Syslog dans l'architecture du système

Plusieurs serveurs Syslog sont disponibles pour différents systèmes d'exploitation.

NOTE: Les serveurs Syslog doivent être conformes à la spécification RFC 5424.

Exemples de fournisseurs de serveurs Syslog :

- WinSyslog : Pour système d'exploitation Windows.
Lien : www.winsyslog.com/en/.
- Kiwi Syslog : Pour système d'exploitation Windows.
Lien : www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx.
- Splunk : Pour systèmes d'exploitation Windows et Unix.
Lien : www.splunk.com/.
- Rsyslog : Pour système d'exploitation Unix.
Lien : www.rsyslog.com/.
- Syslog-ng : Open Source pour système d'exploitation Unix.
Lien : www.balabit.com/network-security/syslog-ng/opensource-logging-system.
- Syslog Server : Open Source pour système d'exploitation Windows.
Lien : sourceforge.net/projects/syslog-server/.

Configuration de clients Syslog dans l'architecture du système

La consignation des événements est gérée dans Control Expert pour tous les équipements et gestionnaires de type d'équipement (DTM).

La fonction de consignation des événements, l'adresse du serveur et le numéro de port sont configurés dans Control Expert comme suit, et ces paramètres sont envoyés à chaque client du système après l'action **Générer** :

Etape	Action
1	Cliquez sur Outils > Options du projet .
2	Cliquez sur Options du projet > Général > Diagnostics automate .
3	Cochez la case Consignation des événements (désactivée par défaut). NOTE: Un projet avec cette option sélectionnée ne peut être ouvert qu'à partir de Unity Pro 10.0. Unity Pro est l'ancien nom de Control Expert pour les versions 13.1 et antérieures.
4	Entrez une valeur valide pour Adresse du serveur SYSLOG et Numéro de port du serveur SYSLOG .
5	Effectuez une action Générer après avoir configuré ce paramètre (il n'est pas obligatoire de sélectionner Analyser le projet).

Diagnostic de la consignation des événements

Le tableau suivant indique les diagnostics de la consignation des événements qui sont disponibles pour différents équipements :

Equipements	Informations de diagnostic
Control Expert	En cas d'erreur de communication avec le serveur Syslog, l'erreur détectée est enregistrée dans l'observateur d'événements. Pour activer l'observateur d'événements dans Control Expert, cochez la case Audit dans l'onglet Règles de Security Editor (voir EcoStruxure™ Control Expert - Security Editor - Guide d'exploitation).
DDT d'équipement BMENOC0301 and BMENOC0311 (paramètre <i>SERVICE_STATUS2</i>)	Deux informations de diagnostic sont disponibles : - EVENT_LOG_STATUS : Valeur = 1 si le service de consignation des événements est opérationnel. Valeur = 0 si le service de consignation des événements n'est pas opérationnel. - LOG_SERVER_NOT_REACHABLE : Valeur = 1 si le client Syslog ne reçoit pas d'acquittement des messages TCP de la part du serveur Syslog. Valeur = 0 si l'acquittement est reçu.
DDT d'équipement du contrôleur Modicon M580	
DDT d'équipement BMECXM	

Description des messages du journal des événements pour Control Expert

Événement consigné : Action sur l'application

Le tableau suivant décrit les messages lorsque l'événement consigné est : Action sur l'application.

MSG ⁽¹⁾	Catégorie	Gravité	Description
créer un projet	10	6	Création d'une application Control Expert
ouvrir un projet existant	10	6	Ouverture d'une application Control Expert existante
enregistrer un projet	10	6	Enregistrement de l'application actuellement ouverte
enregistrer un projet sous	10	6	Enregistrement de l'application actuellement ouverte dans un fichier différent
importer un projet	10	6	Importation d'une application
générer hors ligne	10	6	Génération d'une application en mode déconnecté (hors ligne)
générer en ligne - Stop	10	6	Génération de l'application en mode connecté (en ligne) avec contrôleur en mode Stop
générer en ligne - Run	10	6	Génération de l'application en mode connecté (en ligne) avec contrôleur en mode Run
démarrer, arrêter ou initialiser le PAC	10	6	Démarrer/arrêter/initialiser le contrôleur
Mettre à jour les valeurs d'initialisation avec les valeurs actuelles	10	6	Mettre à jour les valeurs initiales avec les valeurs actuelles
transférer le projet depuis le PAC	10	6	Chargement de l'application à partir du contrôleur
transférer le projet vers le PAC	10	6	Téléchargement de l'application vers le contrôleur
transférer les valeurs de données du fichier vers le PAC	10	6	Transfert de valeurs de données d'un fichier vers le contrôleur
restaurer la sauvegarde du projet dans le PAC	10	6	Restauration d'une sauvegarde du projet dans le contrôleur
enregistrer dans la sauvegarde du projet dans le PAC	10	6	Enregistrer dans la sauvegarde du projet dans le contrôleur

MSG ⁽¹⁾	Catégorie	Gravité	Description
Définir l'adresse	10	6	Modifier l'adresse de connexion du contrôleur
Modifier les options	10	6	Modifications des options de Control Expert
Modifier les valeurs de variable	10	6	Modification de valeurs de variable dans le contrôleur
Forcer les bits internes	10	6	Modification de la valeur de forçage des variables dans le contrôleur : bits internes
Forcer les sorties	10	6	Modification de la valeur de forçage des variables dans le contrôleur : sorties
Forcer les entrées	10	6	Modification de la valeur de forçage des variables dans le contrôleur : entrées
Gestion des tâches	10	6	Gestion des tâches
Modification de la durée de cycle de la tâche	10	6	Modification de la durée de cycle de la tâche
Supprimer le message dans le visualiseur de diagnostic	10	6	Supprimer le message dans le visualiseur de diagnostic
Déboguer le code exécutable	10	6	Déboguer le code exécutable
Remplacer une variable du projet	10	6	Remplacer une variable du projet
Créer des bibliothèques ou des familles	10	6	Créer des bibliothèques ou des familles dans la bibliothèque
Supprimer des bibliothèques ou des familles	10	6	Supprimer des bibliothèques ou des familles de la bibliothèque
Placer l'objet dans la bibliothèque	10	6	Copier l'élément (DFB/DDT) de l'application dans la bibliothèque
Supprimer l'objet de la bibliothèque	10	6	Supprimer l'élément (DFB/DDT) de la bibliothèque
Obtenir l'objet de la bibliothèque	10	6	Copier l'élément (DFB/DDT/EF/EFB) de la bibliothèque dans l'application
Modifier la documentation	10	6	Modifier la documentation (impression de l'application)
Modifier la vue fonctionnelle	10	6	Modifier la vue fonctionnelle
Modifier les tables d'animation	10	6	Modifier les tables d'animation
Modifier les valeurs constantes	10	6	Modifier les valeurs constantes
Modifier la structure du programme	10	6	Modifier la structure du programme
Modifier les sections du programme	10	6	Modifier les sections du programme
Modifier les paramètres du projet	10	6	Modifier les paramètres du projet

MSG ⁽¹⁾	Catégorie	Gravité	Description
Ajout/suppression de variable	10	6	Variable créée/supprimée dans l'éditeur de données
Modification des attributs principaux des variables	10	6	Attribut de variable modifié
Modification des attributs mineurs des variables	10	6	Attribut de variable modifié
Ajout/suppression de DDT	10	6	DDT créé/supprimé dans l'éditeur de données
Modification de DDT	10	6	DDT modifié dans l'éditeur de données
Ajout/suppression de type DFB	10	6	DFB créé/supprimé dans l'éditeur de données
Modification de la structure de type DFB	10	6	Structure de DFB modifiée dans l'éditeur de données
Modification des sections de type DFB	10	6	Sections de DFB modifiées
Modification d'instance de DFB	10	6	Modification d'instance de DFB dans l'éditeur de données
Modification des attributs mineurs de l'instance de DFB	10	6	Modification des attributs mineurs de l'instance de DFB dans l'éditeur de données
Modifier la configuration	10	6	Modification de la configuration du contrôleur
Apprentissage automatique de la configuration des E/S	10	6	Apprentissage automatique des E/S du contrôleur
Modifier la configuration des E/S	10	6	Modification de la configuration des E/S du contrôleur
Réglage des E/S	10	6	Réglage de la configuration des E/S du contrôleur
Enregistrer les paramètres	10	6	Enregistrement des paramètres de configuration des E/S du contrôleur à partir de l'écran des E/S
Restauration de paramètres	10	6	Enregistrement des paramètres de configuration des E/S du contrôleur à partir de l'écran des E/S
Modifier les écrans	10	6	Modification des écrans d'exploitation
Modifier les messages	10	6	Modifier les messages
Ajout/suppression d'écrans ou de familles	10	6	Ecrans d'exploitation : Famille/écran ajouté/supprimé
Déplacer un composant	13	6	Déplacement de bloc FFB
Déplacer un composant	13	6	Déplacer le contact/la bobine

MSG ⁽¹⁾	Catégorie	Gravité	Description
Insérer un composant	13	6	Insérer un bloc FFB
Insérer un composant	13	6	Insérer le contact/la bobine
Supprimer un composant	13	6	Supprimer un bloc FFB
Supprimer un composant	13	6	Supprimer le contact/la bobine
Ajouter une variable	13	6	Définir le paramètre Effectif sur le bloc FFB
Ajouter une variable	13	6	Définir le paramètre Effectif sur le contact/la bobine
Supprimer une variable	13	6	Supprimer le paramètre Effectif sur le bloc FFB
Supprimer une variable	13	6	Supprimer le paramètre Effectif sur le contact/la bobine
Modifier une variable	13	6	Modifier le paramètre Effectif sur le bloc FFB
Modifier une variable	13	6	Modifier le paramètre Effectif sur le contact/la bobine
Lier la broche	13	6	Etablir une liaison entre deux broches
Mettre à l'échelle un composant	13	6	Modifier la taille d'un bloc FFB extensible
Mettre à l'échelle un composant	13	6	Modifier la taille de la liaison verticale/horizontale
Renommer variable	13	6	Renommer le paramètre effectif
Supprimer ligne	13	6	Supprimer une seule ligne
Supprimer des lignes de	13	6	Supprimer plusieurs lignes
Supprimer colonne	13	6	Supprimer une seule colonne
Supprimer des colonnes de	13	6	Supprimer plusieurs colonnes
Insérer ligne	13	6	Insérer une seule ligne
Insérer des lignes à partir de	13	6	Insérer plusieurs lignes
Insérer colonne	13	6	Insérer une seule colonne
Insérer des colonnes à partir de	13	6	Insérer plusieurs colonnes
⁽¹⁾ Le contenu du message MSG comprend une concaténation du nom d'utilisateur, du PID de Control Expert et du message.			

NOTE: Les champs HOSTNAME, APP-NAME, PROCID, MSGID et STRUCTURED-DATA ne s'appliquent pas aux messages Control Expert.

Événement consigné : action DTM

Le tableau suivant décrit les messages lorsque l'événement consigné est : action DTM.

MSG ⁽¹⁾	Catégorie	Gravité	Description
Le service de téléchargement des paramètres vers l'équipement a rencontré une erreur	9	6	Téléchargement de paramètres DTM terminé en erreur
Le service de téléchargement des paramètres vers l'équipement s'est terminé sans erreur	9	6	Téléchargement de paramètres DTM terminé sans erreur
Le service de chargement des paramètres depuis l'équipement a rencontré une erreur	9	6	Chargement de paramètres dans DTM terminé en erreur
Le service de chargement des paramètres depuis l'équipement s'est terminé sans erreur	9	6	Chargement de paramètres dans DTM terminé sans erreur
Echec du service de mise en ligne	9	6	La connexion au DTM n'est pas établie
Service de mise en ligne réussi	9	6	Connexion au DTM réussie
Echec du service de mise hors ligne	9	6	La connexion au DTM n'est pas fermée
Service de mise hors ligne réussi	9	6	Connexion au DTM fermée avec succès
Echec du service de téléchargement de paramètres FDR	9	6	Le service FDR de téléchargement de paramètres de DTM n'est pas exécuté
Service de téléchargement de paramètres FDR réussi	9	6	Le service FDR de téléchargement de paramètres de DTM a réussi
Echec du service de chargement de paramètres FDR	9	6	Le service FDR de chargement de paramètres de DTM n'est pas exécuté
Service de chargement de paramètres FDR réussi	9	6	Le service FDR de chargement de paramètres de DTM a réussi
Echec du téléchargement de paramètres vers l'équipement	9	6	Le téléchargement de paramètres vers l'équipement n'est pas effectué
Téléchargement de paramètres vers l'équipement réussi	9	6	Téléchargement de paramètres vers l'équipement réussi
Echec du chargement de paramètres depuis l'équipement	9	6	Le chargement de paramètres depuis l'équipement n'est pas effectué
Chargement de paramètres depuis l'équipement réussi	9	6	Chargement de paramètres depuis l'équipement réussi
Événement de la fonction Trace d'audit	9	6	Événement de la fonction Trace d'audit
Événement d'état d'équipement Trace d'audit	9	6	Événement d'état d'équipement Trace d'audit
Aucun message d'état d'équipement	9	6	Aucun message d'état d'équipement

MSG ⁽¹⁾	Catégorie	Gravité	Description
Informations sur le statut	9	6	Informations sur le statut
Droit d'accès : Lecture / Ecriture	9	6	Droit d'accès : Lecture / Ecriture
Entrée d'énumérateur	9	6	Entrée d'énumérateur
⁽¹⁾ Le contenu du message MSG comprend une concaténation du nom d'utilisateur, du PID de Control Expert et du message.			

Événement consigné : Action de mot de passe

Le tableau suivant décrit les messages lorsque l'événement consigné est : Action de mot de passe.

MSG ⁽¹⁾	Catégorie	Gravité	Description
Cybersécurité - Modification du mot de passe > Mot de passe incorrect	2	6	Problème lors de la modification du mot de passe d'application
Cybersécurité - Vérification du mot de passe > Mot de passe incorrect	2	6	Problème lors de la vérification du mot de passe d'application
Cybersécurité - Vérification du mot de passe de section > Mot de passe incorrect	2	6	Problème lors de la vérification du mot de passe de section
Cybersécurité - Mot de passe de stockage des données modifié	2	6	Mot de passe de stockage des données modifié
Cybersécurité - Mot de passe du micrologiciel modifié	2	6	Mot de passe de téléchargement de micrologiciel modifié
Cybersécurité - Vérification du mot de passe > Mot de passe incorrect	2	6	Problème lors de la vérification du mot de passe d'application
⁽¹⁾ Le contenu du message MSG comprend une concaténation du nom d'utilisateur, du PID de Control Expert et du message.			

Événement consigné : Configuration SYSLOG modifiée

Le tableau suivant décrit les messages lorsque l'événement consigné est : Configuration SYSLOG modifiée.

MSG ⁽¹⁾	Catégorie	Gravité	Description
Adresse SYSLOG modifiée	-	-	Cybersécurité - Le paramètre de projet Consignation des événements a été modifié - Enregistrement des événements, adresse du serveur SYSLOG, port ou protocole
⁽¹⁾ Le contenu du message MSG comprend une concaténation du nom d'utilisateur, du PID de Control Expert et du message.			

Événement consigné : Action de fichier

Le tableau suivant décrit les messages lorsque l'événement consigné est : Action de fichier.

MSG ⁽¹⁾	Catégorie	Gravité	Description
Le fichier XXXXX a été ouvert	0	6	Fichier XXXXX ouvert
Déconnexion du PAC @=XXXXXX pilote = YYYY	0	6	Contrôleur déconnecté = @XXXXXX pilote = YYYY
Fermer l'application XXXXXX	0	6	Fermeture de l'application XXXXXX
Le projet a été transféré du PAC vers le PC	0	6	Transfert du contrôleur vers le PC
⁽¹⁾ Le contenu du message MSG comprend une concaténation du nom d'utilisateur, du PID de Control Expert et du message.			

Description des messages du journal des événements pour les contrôleurs M580 (à partir de la version de micrologiciel V4.10) et pour BMENOR2200H (à partir de la version de micrologiciel 3.01)

Cette rubrique décrit les messages du journal des événements pour :

- Contrôleurs M580 à partir de la version 4.10 du micrologiciel (abréviation **CPU** dans la colonne **Equipements**)
- Modules RTU BMENOR2200H à partir de la version 3.01 du micrologiciel (abréviation "eNOR" dans la colonne **Equipements**)

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURED-DATA	MSG	Équipements
Connexion établie	Toute connexion établie entre un utilisateur (être humain ou composant) et un composant, que ce soit via un protocole chiffré ou un protocole non chiffré si la stratégie de sécurité du client l'autorise	Connexion établie (serveur Web via HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceld=num] [auth-n@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom d'utilisateur]	Connexion	CPU eNOR
		Connexion établie (mise à niveau du micrologiciel via HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceld=num] [auth-n@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom d'utilisateur]	Ouvrir la session	CPU eNOR
		Connexion établie (OPC-UA)	6	OPC-UA	CONNECTION_SUCCESS	[meta sequenceld=num] [auth-n@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom d'utilisateur]	Connexion de socket	CPU
		Connexion établie (mot de passe de l'application Unity via Modbus-Umas) Mode standard	6	MOD-BUS-UMAS	CONNECTION_SUCCESS	[meta sequenceld=num] [auth-n@3833 itf=localPort localInterfa- cepeer=peerFQDN:	Connexion	CPU

Événe- ment consigné	Descrip- tion	Descrip- tion supplé- mentaire	Gravi- té	PROCID	MSGID	STRUCTU- RED-DATA	MSG	Equipe- ments
		unique- ment				<i>peerPort user=nom d'utilisa- teur]</i>		
		Connexion Modbus TCP établie (aucun utilisateur)	6	MODBUS	CON- NEC- TION_ SUC- CESS	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Connexion de socket	CPU eNOR
		Connexion HTTP/ DPWS établie	6	HTTP	CON- NEC- TION_ SUC- CESS	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Connexion de socket	CPU
		Connexion TCP explicite EIP établie (aucun utilisateur)	6	EIP	CON- NEC- TION_ SUC- CESS	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Connexion de socket	CPU
		Connexion DNP3 établie (aucun utilisateur)	6	DNP3	CON- NEC- TION_ SUC- CESS	[meta sequen- celd=num] [auth- n@3833	Connexion de socket	eNOR

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURE- RED-DATA	MSG	Équipements
						itf=localPort localInterface peer= peerFQDN: peerPort user= username]		
		Connexion CEI 60870 établie (aucun utilisateur)	6	IEC60870	CON- NEC- TION_ SUC- CESS	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterface peer= peerFQDN: peerPort user= username]	Connexion de socket	eNOR
Problème de connexion	Toute tentative infructueu- se de connexion d'un utilisateur (être humain ou compo- sant) à un compo- sant, que ce soit via un protocole chiffré ou un protocole non chiffré si la stratégie de sécurité du client l'autorise	Problème de connexion (mot de passe d'applica- tion Unity via Modbus- Umas)	5	MOD- BUS- UMAS	CON- NEC- TION FAILURE	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterface peer= peerFQDN: peerPort user=nom d'utilisa- teur]	Mot de passe non valide	CPU
		Problème de connexion Modbus TCP (aucun utilisateur)	5	MODBUS	CON- NEC- TION FAILURE	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterface peer= peerFQDN: peerPort user=nom d'utilisa- teur]	Nombre max. de connexions atteint" "Flux de données filtré	CPU eNOR
		Problème de	5	EIP	CON-	[meta	Nombre max. de	CPU

Événement consigné	Descrip- tion	Descrip- tion supplé- mentaire	Gravi- té	PROCID	MSGID	STRUCTU- RED-DATA	MSG	Equipe- ments
		connexion TCP EIP explicite (aucun utilisateur)			NEC- TION_ FAILURE	sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	connexions atteint, flux de données filtré	
		Problème de connexion DNP3 (aucun utilisateur)	5	DNP3	CON- NEC- TION_ FAILURE	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- ce peer= peerFQDN: peerPort user= username]	Nombre max. de connexions atteint"	eNOR
		Problème de connexion CEI 60870 (aucun utilisateur)	5	IEC60870	CON- NEC- TION_ FAILURE	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- ce peer= peerFQDN: peerPort user= username]	Nombre max. de connexions atteint	eNOR
Verrouilla- ge de compte utilisateur humain en raison d'un trop grand nombre de problèmes lors des tentatives	La stratégie de sécurité peut demander le blocage d'un compte utilisateur humain après un nombre	Problème de connexion (serveur Web via HTTPS). Verrouillage de compte d'utilisateur humain en raison d'un trop grand nombre de	1	HTTPS	CON- NEC- TION_ FAILU- RE_ AND_ BLOCK	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom	Certificat non valide, mot de passe non valide	CPU eNOR

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURED-DATA	MSG	Équipements
d'authentification	configurable de tentatives. Cet événement informe l'administrateur d'une attaque potentielle et indique que le compte d'utilisateur humain doit être verrouillé.	problèmes lors des tentatives d'authentification				<i>d'utilisateur</i>		
		Problème de connexion (mise à niveau du micrologiciel via HTTPS). Verrouillage du compte d'utilisateur humain en raison d'un trop grand nombre de tentatives d'authentification infructueuses	1	HTTPS	CONNECTION_FAILURE_BLOCK	[meta sequenceld=num] [authn@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom d'utilisateur]	Certificat non valide" "Mot de passe non valide	CPU eNOR
		Problème de connexion (OPC-UA). Verrouillage de compte d'utilisateur humain en raison d'un trop grand nombre de problèmes lors des tentatives d'authentification	1	OPC-UA	CONNECTION_FAILURE_BLOCK	[meta sequenceld=num] [authn@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom d'utilisateur]	Certificat non valide, mot de passe non valide	—
Connexion refusée (compte bloqué)	Un utilisateur humain tente de se connecter sur un compte qui est déjà bloqué.	Problème de connexion (serveur Web via HTTPS). Connexion refusée (compte bloqué)	1	HTTPS	CONNECTION_FAILURE_BLOCKED	[meta sequenceld=num] [authn@3833 itf=localPort localInterfa- cepeer=peerFQDN: peerPort user=nom		CPU eNOR

Événement consigné	Descrip- tion	Descrip- tion supplé- mentaire	Gravi- té	PROCID	MSGID	STRUCTU- RED-DATA	MSG	Equipe- ments
						<i>d'utilisateur]</i>		
		Problème de connexion (mise à niveau du micrologiciel via HTTPS). Connexion refusée (compte bloqué)	1	HTTPS	CON- NEC- TION_ FAILU- RE_ON_ BLOC- KED	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisateur]		CPU
		Problème de connexion (OPC-UA). Connexion refusée (compte bloqué)	1	OPC-UA	CON- NEC- TION_ FAILU- RE_ON_ BLOC- KED	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisateur]		—
Déconne- xion	Déconne- xion manuelle d'une personne ou d'un compo- sant après un timeout dû à une inactivité.	Déconne- xion HTTPS (serveur Web)	6	HTTPS	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisateur]	Déconne- xion manuelle	CPU eNOR
		Déconne- xion HTTPS (mise à niveau du micrologi- ciel)	6	HTTPS	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort 	Déconne- xion manuelle	CPU eNOR

Événe- ment consigné	Descrip- tion	Descrip- tion supplé- mentaire	Gravi- té	PROCID	MSGID	STRUCTU- RED-DATA	MSG	Equipe- ments
						<i>localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]</i>		
		Déconne- xion OPC- UA	6	OPC-UA	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconne- xion de socket	CPU
		Déconne- xion Modbus	6	MODBUS	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconne- xion de socket	CPU
		Déconne- xion EIP explicite	6	EIP	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconne- xion de socket	CPU

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURE- RED-DATA	MSG	Équipements
		Déconnexion HTTP (DPWS)	6	HTTP	DISCONNECTION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconnexion de socket	CPU
		Déconnexion HTTPS déclenchée par un timeout	6	HTTPS	DISCONNECTION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconnexion par timeout	CPU eNOR
		Déconnexion OPC-UA déclenchée par un timeout	6	OPC-UA	DISCONNECTION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- cepeer= peerFQDN: peerPort user=nom d'utilisa- teur]	Déconnexion par timeout	—
		Déconnexion DNP3	6	DNP3	DISCONNECTION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- ce peer= peerFQDN:	Déconnexion de socket	eNOR

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURE- RED-DATA	MSG	Équipements
						peerPort user= username]		
		Déconnexion CEI 60870	6	IEC60870	DISCON- NEC- TION	[meta sequen- celd=num] [auth- n@3833 itf=localPort localInterfa- ce peer= peerFQDN: peerPort user= username]	Déconnex- ion de socket	eNOR
Modifica- tion majeure des paramè- tres lors de l'exécution	Modifica- tion majeure de paramè- tres à l'exécution pouvant avoir un impact significatif sur le système	Modification des paramètres de l'application du contrôleur : temps de cycle	6	Configu- ration	PARA- METER_ SET	[meta sequen- celd=num] [con- fig@3833 object= "application API" value= valeur]	Temps de scrutation	CPU
Opération de sauvegar- de	Sauvegar- de d'une partie ou de l'ensemble d'un composant	Télécharge- ment de l'application à partir du contrôleur	6	Sauve- garde	BACKUP	[meta sequen- celd=num] [bac- kup@3833 object= "application automate"]		CPU
		Exportation de la configura- tion de la Cybersécu- rité à partir des pages Web BME NUA ou BME NOR	6	Sauve- garde	BACKUP	[meta sequen- celd=num] [bac- kup@3833 object= "configura- tion de la Cybersécu- rité"]		eNOR
Opération de	Restaura- tion d'une partie ou	Charge- ment de	6	Configu- ration	CONFI- GURA- TION_	[meta sequen- celd=num]		CPU

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURED-DATA	MSG	Équipements
restauration	de la totalité d'un composant	l'application/la configuration du contrôleur dans le contrôleur			CHANGE	[config@3833 object= <i>Objet</i> <i>Objet</i> = "Application de l'automate" ou "Configuration de l'automate"		
6	Sauvegarde	Restauration de l'application du contrôleur dans le contrôleur						
RESTORE		[meta sequen- celd= <i>num</i>] [back- kup@3833 object= "application automate"]		CPU				
Importation de la configuration de la Cybersécurité à partir des pages Web BME NUA ou BME NOR		6	Sauvegarde	RESTORE	[meta sequen- celd= <i>num</i>] [back- kup- p@3833 object= "Configu- ration de Cybersé- curité"]		eNOR	
Mise à jour du micrologiciel	Un nouveau micrologiciel a été vérifié et installé.	Chargement d'un nouveau micrologiciel dans le contrôleur, le coprocesseur, les pages Web	6	Configuration	FIRMWARE_UPDATE	[meta sequen- celd= <i>num</i>] [con- fig@3833 object= <i>Objet</i> value= <i>version</i> <i>n</i>]"Objet = "micrologiciel",		CPU eNOR

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURED-DATA	MSG	Équipements
						"coprocesseur de sécurité", "pages Web"		
Mise à jour de micrologiciel non valide	Le nouveau micrologiciel n'a pas été installé en raison d'une erreur.	Le nouveau micrologiciel n'a pas été installé en raison d'une version incompatible ou d'une signature non valide.	1	Configuration	FIRMWARE_INVALID	[meta sequenceld=num] [config@3833 object=Objet value=version]"Objet = "micrologiciel", "coprocesseur de sécurité", "pages Web"	Version incompatible, signature non valide	CPU eNOR
Modification de l'heure de l'équipement	Demande de modification de la date et de l'heure par un utilisateur humain.	—	5	Configuration	TIME_CHANGE	[meta sequenceld=num] [config@3833 object="Heure" value=date et heure]		CPU
Signal horaire hors tolérance	Le composant doit valider les messages de synchronisation horaire reçus via les canaux de synchronisation d'horloge et l'alarme si le message de synchronisation	—	1	Configuration	TIME_UNEXPECTED	[meta sequenceld=num] [config@3833 object="Heure" value=date et heure]	Signal horaire hors tolérance	

Événement consigné	Description	Description supplémentaire	Gravité	PROCID	MSGID	STRUCTURE-DATA	MSG	Équipements
	horaire n'est pas dans les tolérances de l'horloge interne/ locale du composant (heure passée, éloignée, etc.).							
Modification matérielle	Modification détectée dans la topologie du réseau	Modification du port physique du réseau : liaison de port active/ inactive	6	Système	HARDWARE_CHAN-GE	[system@3833 object= <i>Objet</i>]Objet = "eth" suivi d'un nombre décimal	Liaison du port active, liaison du port inactive	CPU
		Toute modification de topologie détectée par RSTP / HSR / PRP	6	Système	HARDWARE_CHAN-GE	[system@3833 object= <i>Objet</i>]Objet = "eth" suivi d'un nombre décimal	Activation de port, désactivation de port, apprentissage de port, transfert de port, blocage de port	CPU
	Modification détectée dans le matériel	Insertion/ extraction de la carte SD M580	6	Système	HARDWARE_CHAN-GE	[system@3833 object= "SDCard"]	Insertion, extraction	CPU
Modification du mode de fonctionnement	Modification du mode de fonctionnement du programme (Run, Stop, Init, Halt)Mode Maintenance / SafeRun / Arrêt de la	—	5	Système	OPERATING_MODE_CHAN-GE	[system@3833 object= Object] Object = "Automate" ou "tâche Safe automate" ou "Module"	"Init" "Run" "Stop" "Halt" "Mode maintenance" "Mode Safe" "Primaire redondant" "Secondaire redondant" "Attente"	CPU

Événement consigné	Descrip- tion	Descrip- tion supplé- mentaire	Gravi- té	PROCID	MSGID	STRUCTU- RED-DATA	MSG	Equipe- ments
	tâche SAFE						redondant" "Maître" "Non maître"	
Configura- tion non valide (hors Cybersé- curité)	Une nouvelle configura- tion (non liée à la Cybersé- curité) n'a pas été installée en raison d'une erreur.	Erreur d'intégrité des données (application du contrôleur, etc.)	1	Configu- ration	CONFI- GURA- TION_ INVALID	[meta sequen- celd=num] [con- fig@3833 object= Objet value= versio- n]"Objet= "Application automate" ou "Configura- tion de module"	Format non valide, version incompati- ble	
Redémar- rer	Réinitiali- sation matérielle ou réinitialisa- tion automati- que après charge- ment du micrologi- ciel	—	1	Système	REBOOT	—	Mise à jour du micrologi- ciel, bouton de réinitialisa- tion	CPU
Modifica- tion du certificat (et/ou des clés) du produit	Gestion des certificats : création de certificat auto-signé de produit SL1	—	6	Informa- tions d'identifi- cation	CERTIFI- CATE_ CHAN- GE	[meta sequen- celd=num] [cre- d@3833 name=Nom commun]	Création de certificat	CPU

NOTE: Outre la structure décrite ci-dessus, chaque message contiendra également les champs et valeurs suivants :

- Catégorie = 10
- HOSTNAME = Nom de domaine complet (FQDN) ou adresse IP locale
- APPNAME = nom de référence commerciale, par exemple BMEP584040

Exemple de messages Syslog Server

Date	Time	Priority	Hostname	Message
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="331"][@auth@3833 if="eth" peer="192.168.11.50:52470"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="330"][@auth@3833 if="eth" peer="192.168.11.50:52468"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="329"][@auth@3833 if="eth" peer="192.168.11.50:52466"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="328"][@auth@3833 if="eth" peer="192.168.11.50:52464"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="327"][@auth@3833 if="eth" peer="192.168.11.50:52462"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="326"][@auth@3833 if="eth" peer="192.168.11.50:52460"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="325"][@auth@3833 if="eth" peer="192.168.11.50:52458"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="324"][@auth@3833 if="eth" peer="192.168.11.50:52456"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="323"][@auth@3833 if="eth" peer="192.168.11.50:52454"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="322"][@auth@3833 if="eth" peer="192.168.11.50:52452"] Socket connection
11-08-2021	11:55:03	System0:Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="321"][@auth@3833 if="eth" peer="192.168.11.50:52450"] Socket connection
11-08-2021	11:54:33	System0:Info	192.168.11.1	1 2021-08-26T11:22:12.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="320"][@auth@3833 if="eth" peer="192.168.11.50:52442"] Socket connection
11-08-2021	11:54:26	System0:Info	192.168.11.1	1 2021-08-26T11:22:07.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="319"][@auth@3833 if="eth" peer="192.168.11.50:34246"] Socket connection
11-08-2021	11:54:26	System0:Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="318"][@auth@3833 if="eth" peer="192.168.11.50:52440"] Socket connection
11-08-2021	11:54:28	System0:Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequencelid="317"][@config@3833 object="Module"]
11-08-2021	11:54:28	System0:Info	192.168.11.1	1 2021-08-26T11:22:04.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequencelid="316"][@config@3833 object="Module"]
11-08-2021	11:54:24	System0:Notice	192.168.11.1	1 2021-08-26T11:22:03.000Z 192.168.11.1 BMEP585040 System OPERATING_MODE_CHANGE [meta sequencelid="315"][@system@3833 object="PLC"] Init
11-08-2021	11:54:13	System0:Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequencelid="314"][@config@3833 object="PLC application"]
11-08-2021	11:54:13	System0:Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Backup RESTORE [meta sequencelid="313"][@backup@3833 object="PLC application"]
11-08-2021	11:54:07	System0:Info	192.168.11.1	1 2021-08-26T11:21:46.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequencelid="312"][@auth@3833 if="eth" peer="192.168.11.50:34235"] Socket connection
11-08-2021	11:53:20	System0:Info	192.168.11.1	1 2021-08-26T11:20:59.000Z 192.168.11.1 BMEP585040 Backup BACKUP [meta sequencelid="311"][@backup@3833 object="PLC application"]

Description des messages du journal des événements des contrôleurs M580 (micrologiciel antérieur à la version 4.10), BMENUA0100 et BMENOR2200H (micrologiciel antérieur à la version 3.01)

Cette rubrique décrit les messages du journal des événements pour :

- Contrôleurs M580 avec micrologiciel antérieur à la version 4.10 (abréviation "CPU" dans la colonne **Equipements**)
- Modules de communication OPC UA BMENUA0100 (abréviation "NUA" dans la colonne **Equipements**)
- Terminal déporté BMENOR2200H (abréviation "eNOR" dans la colonne **Equipements**).

Evéne- ment consigné	Descrip- tion	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
Connexion établie à ou depuis un outil ou un équipe- ment : * Connexion établie * Connexion TCP établie	Connexion établie (stockage des données via FTP, serveur FDR via FTP, charge- ment du micrologi- ciel via FTP)	10	6	FTP	adresse IP distante	Li1 : Connexion établie (MNT_ ENG_ MSG_ TYP_ CNCTN_ SUC- CESS)	"Conne- xion établie"	CPU
	Connexion établie (serveur Web via HTTPS)			HTTPS	"(null)"		"Conne- xion établie"	NUA
	Connexion établie (mise à niveau du micrologi- ciel via HTTPS)			HTTPS	"(null)"		"Conne- xion établie"	NUA
	Connexion établie (OPC-UA)			OPC-UA	"(null)"		"Conne- xion établie"	NUA
	Connexion établie (mot de passe de l'applica- tion Unity utilisant Modbus- Umas)			DEVICE_ MANA- GER	"(null)"		"Conne- xion établie"	CPU
	Connexion établie (serveur Web via HTTP)			HTTP	"(null)"		"Conne- xion établie" OU "Conne- xion établie" (si aucun utilisateur ne se connecte aux pages	CPU

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
							Web du M580)	
	Connexion TCP établie (aucun utilisateur).			MODBUS	adresse ip distante		"Connexion établie"	CPU
	Connexion TCP établie (aucun utilisateur).			EIP	"(null)"		"Connexion établie"	CPU
	Connexion établie sur le protocole de communication DNP3 (à propos du maître et du poste DNP3)			DNP3	adresse IP distante		"Connexion établie"	eNOR
	Connexion établie sur le protocole de communication CEI 60870 (à propos du client et du serveur CEI 60870)			IEC60870	adresse IP distante		"Connexion établie"	eNOR
Problème de connexion à ou depuis un outil ou un équipement : *Problème de connexion	Problème de connexion (stockage des données utilisant FTP, serveur FDR utilisant FTP,	10	4	FTP	adresse IP distante	Li2 : Echec de connexion (identifiants erronés) (MNT_ ENG_ MSG_ TYP_ CNCTN FAILURE)	"Echec de connexion"	CPU

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
TCP dû à la vérification de l'ACL (filtrage de l'adresse IP source/ du port TCP) * Problème de connexion	charge- ment du micrologi- ciel utilisant FTP)							
	Problème de connexion (serveur Web utilisant HTTPS)			HTTPS	"(null)"		"Echec de conne- xion"	NUA
	Problème de connexion (mise à niveau du micrologi- ciel utilisant HTTPS)			HTTPS	"(null)"		"Echec de conne- xion"	NUA
	Problème de connexion (OPC-UA)			OPC-UA	"(null)"		"Echec de conne- xion"	NUA
	Problème de connexion (serveur Web utilisant HTTP)			HTTP	adresse IP distante		"Echec de conne- xion" OU "Echec de conne- xion" (si aucune connexion utilisateur n'est établie)	CPU
	Problème de connexion (mot de passe d'applica- tion Unity utilisant Modbus- Umas)			DEVICE_ MANA- GER	adresse IP distante		"Echec de conne- xion"	CPU
	Problème de connexion			MODBUS	adresse IP distante		"Echec de conne- xion"	CPU

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
	TCP (aucun utilisateur)							
	Problème de connexion TCP (aucun utilisateur)			EIP	adresse IP distante		"Echec de conne- xion"	CPU
	Problème de connexion sur le protocole de communi- cation DNP3 (à propos du maître et du poste DNP3)			DNP3	adresse IP distante		"Echec de conne- xion"	eNOR
	Problème de connexion au protocole de communi- cation CEI 60870 (à propos du client et du serveur CEI 60870)			IEC60870	adresse IP distante		"Echec de conne- xion"	eNOR
Déconne- xion déclen- chée par une demande locale ou un homolo- gue : * Déconne- xion TCP	Déconne- xion déclen- chée par l'homolo- gue/ l'utilisa- teur/le système local	10	6	FTP	"(null)"	Li5 : déconne- xion déclen- chée par l'homolo- gue/ l'utilisateur (MNT_ ENG_ MSG_ TYP_ DISCON- NEC- TION)	"Déconne- xion"	—

Évène- ment consigné	Descrip- tion	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
* Déconne- xion à la demande	Déconne- xion déclen- chée par l'homolo- gue/ l'utilisa- teur/le système local			HTTPS	"(null)"		"Déconne- xion"	NUA
	Déconne- xion déclen- chée par l'homolo- gue/ l'utilisa- teur/le système local			OPC-UA	"(null)"		"Déconne- xion"	NUA
	Déconne- xion déclen- chée par l'homolo- gue/ l'utilisa- teur/le système local			MODBUS	adresse IP distante		"Déconne- xion"	CPU
	—			DNP3	"(null)" ou adresse ip distante		"Déconne- xion"	eNOR
	—			IEC60870	"(null)" ou adresse IP distante		"Déconne- xion"	eNOR
Déconne- xion automati- que (délai d'inactivi- té) HTTPS OPC-UA	Déconne- xion déclen- chée par un timeout	10	6	HTTPS	"(null)"	Li6 : Déconne- xion déclen- chée par un timeout (MNT_ ENG_ MSG_ TYP_ DSCNCT_ TI- MEOUT)	"Déconne- xion automati- que"	NUA
	Déconne- xion			OPC-UA			"Déconne- xion	NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
	déclenchée par un timeout						automatique	
Modifications majeures dans le système : Modification de l'exécution des paramètres en dehors de la configuration	Modification majeure du temps de cycle ou du chien de garde, modification des paramètres de l'application du contrôleur (temps de cycle, chien de garde)	13	5	DEVICE_MANAGER	"(null)"	Li87 : Mise à jour des paramètres système (MNT_ENG_MSG_TYP_PARAMETER_UPDATE)	"Mise à jour du paramètre XXXX" (XXXX identifiant le paramètre) XXXX = "Temps de cycle" Exemple : Mise à jour du paramètre Temps de cycle	CPU
Modifications majeures dans le système : * Téléchargement d'application ou de configuration depuis l'équipement * Exportation (enregistrement) des fichiers de configuration de la cybersécurité à partir de l'équipement	Téléchargement d'un fichier de configuration à partir de l'équipement	13	6	MODBUS	"(null)"	Li8 : Téléchargement d'un fichier de configuration à partir de l'équipement (MNT_ENG_MSG_TYP_CONF_DL)	"Téléchargement d'application" ou "Téléchargement de configuration"	CPU
				HTTPS			"Sauvegarde de la configuration de la Cybersécurité"	NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
l'équipement								
Modifications majeures du système	Chargement de l'application/ configuration ou de la configuration unique- ment dans l'équipement (y compris CCOTF)	13	6	MODBUS	"(null)"	Li9 : Chargement d'un fichier de configuration dans l'équipement (MNT_ ENG_ MSG_ TYP_ CONF_ UL)	"Chargement de l'application" ou "Chargement de la configuration"	CPU NUA
	Importation (restauration) du fichier de configuration de la cybersécurité dans l'équipement			HTTPS			"Restauration de la configuration de la Cybersécurité"	NUA
Modifications majeures dans le système	Chargement de pages Web vers l'équipement	13	6	FTP	"(null)"	Li10 : Chargement d'un nouveau micrologiciel dans l'équipement (MNT_ ENG_ MSG_ TYP_ FIRMWARE_ UPDATE)	"Téléchargement de pages Web"	CPU
	Chargement d'un nouveau micrologiciel de coprocesseur de sécurité			FTP			"Chargement du micrologiciel du coprocesseur de sécurité"	CPU

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
	Chargement d'un nouveau micrologiciel dans l'équipement			FTP			"Chargement de micrologiciel"	CPU
	Chargement d'un nouveau micrologiciel dans l'équipement			HTTPS			"Chargement de micrologiciel"	NUA
Modifications majeures dans le système	Modification de l'heure de l'équipement	13	6	DEVICE_ MANA- GER	"(null)"	LI15 : Modification de l'heure de l'IED	"Mise à jour majeure de l'heure"	NUA
Temps d'exécution des paramètres de communication Modification réussie en dehors de la configuration	Activation/désactivation des services de communication	10	4	DEVICE_ MANA- GER	"(null)"	LI18 : Activation/désactivation d'un port physique (série, USB) ou logique (Telnet, FTP) (MNT_ ENG_ MSG_ TYP_ PORT_ MANAGE- MENT)	"Mise à jour majeure des paramètres de communication : XXXX YYYY"XX- XX = "EIP" ou "DHCP" ou "FTP" ou "MOD-BUS" ou "SNMP" ou "HTTP" ou "SECURITY" ou "NTP" ou "IPSEC" ou "DEVICE_ MANA- GER" Pour NUA uniquement : XXXX = "Flux de	CPU NUA eNOR

Évène- ment consigné	Descrip- tion	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
							données Control Expert vers le contrôleur unique- ment" ou "Flux de données Control Expert vers le réseau d'équipe- ments" ou "Flux de données CPU vers CPU" Pour NOR unique- ment : XXXX = "DNP3 sur voie TLS [<i>nom de voie</i>]" ou "IE- C60870 sur TLS" YYY- Y= "activer" ou "désacti- ver" Exemple :"Mise à jour majeure des paramè- tres de communi- cation : activer FTP"	
Modifica- tion du port physique du réseau : liaison de port	Tout change- ment d'état de port physique du réseau. Il peut	10	4	DEVICE_ MANA- GER	"(null)"	LI19 : Tout change- ment d'état du port physique du réseau. Il peut	CHG).	"Modifica- tion majeure de l'état du port physique du réseau :

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
active/ inactive	s'agir de l'état simple d'un port Ethernet ou d'informations collectées par l'algorithme RSTP / HSR / PRP pour les systèmes redondants.					s'agir de l'état simple d'un port Ethernet ou d'informations collectées par l'algorithme RSTP / HSR / PRP pour les systèmes redondants (MNT_ ENG_ MSG_ TYP_ NETWK_ PORT_ CHG).		Liaison XXXX YYY" XXXX = "ETH" suivi d'un nombre décimal pour le port ou "Port FRONT" YYYY = "liaison active" ou "liaison interrom- pue" Exemple : "Modifica- tion majeure d'état de port physique du réseau : Liaison ETH1 active)
CPU NUA								
Toute modifica- tion de topologie détectée :	Toute modifica- tion de topologie détectée par RSTP / HSR / PRP	10	4	RSTP	"(null)"	LI20 : Toute modifica- tion de topologie détectée par les algorith- mes RSTP / HSR / PRP pour les systèmes redon- dants (MNT_ ENG_ MSG_ TYP_ NETWK_	"Modifica- tion de topologie détectée" ou "Modifica- tion de topologie détectée : XXXX YYYY" XXXX = "ETH" suivi d'un nombre décimal pour le port ou "FRONT port" YYYY =	CPU NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
						TPLGY_ CHG).	"activer", "désactiver", "apprentissage", "transfert", "blocage"	
Erreur de la vérification d'intégrité : * Erreur de signature numérique, * Intégrité unique- ment (hachage mac)	Erreur d'intégrité du micrologi- ciel	10	6	DEVICE_ MANA- GER	"(null)"	LI84 : Erreur d'intégrité des données MNT_ ENG_ MSG_ DATA_ INTEGRI- TY_ ERROR	"Erreur d'intégrité du micrologi- ciel"	CPU NUA
	Erreur d'intégrité des données : Conf CS, cert, liste blanche ou RBAC)			DEVICE_ MANA- GER			"Erreur d'intégrité des données"	NUA
Modifica- tions majeures dans le système : Redémarrer	Redémar- rage après charge- ment du micrologi- ciel	13	4	DEVICE_ MANA- GER	"(null)"	LI14 : MNT_ ENG_ MSG_ TYP_ RE- BOOT ORDER	"Redémarrer"	CPU NUA
Modifica- tions majeures dans le système	Modifica- tion du mode de fonction- nement du contrôleur (Run, Stop, Init, Halt) Mode Mainte- nance Modifica- tion des modes de fonction- nement liés à la sécurité (tâche	13	5	DEVICE_ MANA- GER	"(null)"	LI85 : Change- ment du mode de fonction- nement MNT_ ENG_ MSG_ OPERAT- ING MODE_ CHANGE	"Mise à jour de l'état de XXXX : YYYY" (avec XXXX identifiant l'objet dont l'état change et YYYY identifiant le nouvel état) XXXX = "Automa- te" ou "tâche Safe de l'automa- te" ou	CPU

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
	Safe Run, Stop Safe)						"Équipement" YYYY = "INIT" ou "STOP" ou "RUN" ou "HALT" ou "Mode maintenance" ou "Mode sécurité" <u>EXEM- PLES :</u> "Mise à jour de l'état de l'automate : RUN" "Mise à jour de l'état de l'automate : Mode de maintenance"	
Modifications majeures dans le système : Modification matérielle	Fonctionnement sur carte SD	13	6	DEVICE_ MANA- GER	"(null)"	LI26 : Modification matérielle MNT_ ENG_ MSG_ HARDWARE_ CHANGE	"Mise à jour du matériel : XXXX" (avec XXXX décrivant la mise à jour) XXXX = "insertion de carte SD" ou "extraction de carte SD"	CPU
	Modification de la position du volant rotatif : Réinitialisation, Avancée			DEVICE_ MANA- GER			"Mise à jour du matériel : XXXX" (avec XXXX décrivant la mise à jour) XXXX = "retour en	NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
							mode usine" ou "mode sécurisé"	
Modification majeure du contrôle RBAC de Cybersécurité (via les pages Web de configuration de la Cybersécurité).	Créer un compte utilisateur Supprimer le compte utilisateur Mettre à jour le compte utilisateur			HTTPS	"(null)"	Li11 : MNT_ ENG_ MSG_ TYP_ RBAC_ UPDATE	"Mettre à jour RBAC"	NUA
Modification manœuvre de la stratégie de Cybersécurité (via les pages Web de configuration de la Cybersécurité).	Services réseau Journal des événements Stratégie de sécurité Bannière de sécurité	10	4	HTTPS	"(null)"	Li12: MNT_ ENG_ MSG_ TYP_ SECURITY_ UPDATE_ UPDATE	"Mise à jour majeure des paramètres de cybersécurité : services réseau" "Mise à jour majeure des paramètres de cybersécurité : journal des événements" "Mise à jour majeure des paramètres de cybersécurité : stratégie de sécurité" "Mise à jour majeure	NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
							des paramètres de cybersécurité : bannière de sécurité"	
Modification majeure des paramètres de Cybersécurité propres à l'équipement (via les pages Web de configuration de la Cybersécurité).	Activer/désactiver et configurer IPSEC Activer/désactiver et configurer OPC-UA Activer/désactiver et configurer DNP3	10	4	HTTPS	"(null)"	Li13 : MNT_ ENG_ MSG_ TYP_ DSS_ UPDATE	"Mise à jour majeure des paramètres de cybersécurité : IPSEC" "Mise à jour majeure des paramètres de cybersécurité : OPC-UA"	NUA
Problème d'autorisation	Une action sur une ressource d'un utilisateur ou d'une machine n'est pas autorisée.	10	4	HTTPS	"(null)"	Li21 : MNT_ ENG_ MSG_ TYP_ AUTH_ REQ	"Échec de l'autorisation"	—
Gestion de certificats	Ajouter/supprimer un certificat client	10	4	HTTPS	"(null)"	Li89 : Gestion des certificats (MNT_ ENG_ MSG_ TYP_ CERT_ MGT)	"Ajouter un certificat client" "Supprimer un certificat client"	NUA
Gestion des certificats : * Certificat expiré	Détection de l'expiration du certificat serveur au	10	3	DEVICE_ MANA- GER	"(null)"	Li29 : Gestion des certificats (MNT_ ENG_ MSG_	"Certificat expiré"	NUA

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
	redémarrage					TYP_CERT_EXPIRE)		
Spécifique du projet eNOR :								
Problème d'authentification	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li100 : MNT_ ENG_ MSG_ TYPE_ AUTHENTICATION_FAILURE	"échec de l'authentification de la voie ["nom de la voie"]"	eNOR
réponse inattendue	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li101 : MNT_ ENG_ MSG_ TYPE_ UNEXPECTED_RESPONSE	"réponse inattendue de la voie ["nom de la voie"]"	eNOR
Pas de réponse	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li102 : MNT_ ENG_ MSG_ TYPE_ NO_RESPONSE	"pas de réponse de la voie ["nom voie"]"	eNOR
Mode agressif non pris en charge	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li103 : MNT_ ENG_ MSG_ TYPE_ AGGRESSIVE_MODE_NOT_SUPPORTED	"mode agressif de la voie ["nom de la voie"] non pris en charge"	eNOR
Algorithme MAC non pris en charge	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li104 : MNT_ ENG_ MSG_ TYPE_ MAC_ALGORITHM_NOT_	"algorithme MAC de la voie ["nom de la voie"] non pris en charge"	eNOR

Événement consigné	Description	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Équipements
						SUPPORT- TED		
Algorithme d'enveloppement de clé non pris en charge	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li105 : MNT_ ENG_ MSG_ TYPE_ KEYW- RAP_ ALGO- RITHM_ NOT_ SUPPORT- TED	"algorithme d'enveloppement de clé de la voie [<i>"nom de la voie"</i>] non pris en charge"	eNOR
Problème d'autorisation	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li86 : MNT_ ENG_ MSG_ TYP_ AUTHO- RIZA- TION_ FAILURE)	"échec de l'autorisation de la voie [<i>"nom de la voie"</i>]"	eNOR
Méthode de modification de clé de mise à jour non autorisée	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li106 : MNT_ ENG_ MSG_ TYPE_ UPDATE_ KEY_ CHAN- GE_ ME- THOD_ NOT_ PERMIT- TED	"méthode de modification de la clé de mise à jour de la voie [<i>"nom de la voie"</i>] non autorisée"	eNOR
Signature non valide	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li107 : MNT_ ENG_ MSG_ TYPE_ INVALID_ SIGNATU- RE	"signature non valide de la voie [<i>"nom de la voie"</i>]"	eNOR
Données de certification non valides	—	10	4	"DNP3_Master" ou "DNP3_Outstation"	adresse IP distante	Li108 : MNT_ ENG_ MSG_ TYPE_ INVALID_	"données de certification de la voie [<i>"nom de la"</i>]"	eNOR

Évène- ment consigné	Descrip- tion	Catégorie	Gravité	MSGID	MSG : peerAddr	MSG : type	MSG : appMsg	Equipe- ments
						CERTIFI- CATION_ DATA	voie"] non valides"	
Utilisateur inconnu	—	10	4	"DNP3_ Master" ou "DNP3_ Outsta- tion"	adresse IP distante	Li109 : MNT_ ENG_ MSG_ TYPE_ UNK- NOWN_ USER_	"utilisateur inconnu de la voie ["nom de la voie"]"	eNOR
Dépasse- ment du nombre maximal de requêtes d'état de clé de session	—	10	4	"DNP3_ Master" ou "DNP3_ Outsta- tion"	adresse IP distante	Li110 : MNT_ ENG_ MSG_ TYPE_ MAX_ SES- SION_ KEY_ STATUS_ REQ_ EXCÉED	"le nombre maximum de requêtes d'état de la clé de session sur la voie ["nom de la voie"] est dépassé"	eNOR
Clé de session modifiée	—	10	6	"DNP3_ Master" ou "DNP3_ Outsta- tion"	adresse IP distante	Li111 : MNT_ ENG_ MSG_ TYPE_ SES- SION_ KEY_ CHAN- GE_ SUC- CESS	"clé de session modifiée sur la voie ["nom de la voie"]"	eNOR

NOTE: Outre la structure décrite ci-dessus, chaque message contiendra également les champs et valeurs suivants à la suite du champ Gravité :

- HOSTNAME = Adresse IP locale ou Null.
- APPNAME = nom de référence commerciale, par exemple BMEP584040.
- PROCID n'est pas utilisé.
- MSG:IssuerAddress = Adresse IP locale.
- MSG Peer n'est pas utilisé.

Identification et authentification

Gestion des comptes

Les meilleures pratiques de gestion des comptes sont les suivantes :

- Créez un compte utilisateur standard sans droits d'administrateur.
- Utilisez le compte utilisateur standard pour lancer des applications. Réservez les comptes avec des droits étendus pour lancer une application requérant des droits d'administration particuliers.
- Utilisez un compte avec des droits d'administration pour installer des applications.

Gestion des contrôles de compte utilisateur (UAC) avec Windows 10

Pour réduire les modifications non autorisées du système d'exploitation de l'ordinateur, Windows 10 accorde aux applications les niveaux d'autorisation d'un utilisateur normal sans privilèges d'administration. Dans ce contexte, les applications ne peuvent pas modifier le système. UAC invite l'utilisateur à octroyer ou refuser des autorisations supplémentaires à une application. Configurez UAC avec le niveau maximum. Au niveau maximum, le contrôle UAC affiche un message pour demander à l'utilisateur d'autoriser une application à effectuer des modifications nécessitant des droits d'administration.

Pour accéder aux paramètres du contrôle UAC dans Windows 10, sélectionnez **Panneau de configuration > Comptes et protection des utilisateurs > Comptes d'utilisateur > Modifier les paramètres du contrôle de compte utilisateur** ou entrez **UAC** dans le champ de recherche du Windows 10 **menu Démarrer**.

Gestion des mots de passe

La gestion des mots de passe est un des outils fondamentaux de la sécurisation renforcée des équipements, processus consistant à configurer un équipement afin qu'il ne soit pas impacté par les menaces basées sur la communication. Une bonne pratique consiste à appliquer les recommandations de gestion des mots de passe suivantes :

- Activez l'authentification par mot de passe sur tous serveurs de messagerie et Web, les contrôleurs et les modules d'interface Ethernet.

- Changez tous les mots de passe par défaut immédiatement après l'installation, y compris pour les éléments suivants :
 - comptes d'utilisateur et d'application sur Windows, SCADA, HMI et d'autres systèmes
 - scripts et code source
 - équipement de contrôle réseau
 - équipements avec comptes d'utilisateur
 - serveurs FTP
 - équipements SNMP et HTTP
 - Control Expert
- Accordez uniquement des mots de passe aux personnes qui ont besoin d'un accès. N'autorisez pas le partage des mots de passe.
- N'affichez pas les mots de passe lors de leur saisie.
 - Exigez des mots de passe difficiles à deviner. Ils doivent contenir au moins huit caractères et combiner des majuscules, des minuscules, des chiffres et des caractères spéciaux s'ils sont autorisés.
- Exigez des utilisateurs et applications qu'ils modifient les mots de passe selon un intervalle planifié.
- Supprimez les comptes d'accès des employés lorsqu'ils ne font plus partie de l'organisation.
- Exigez des mots de passe différents pour différents comptes, systèmes et applications.
- Conservez une liste principale sécurisée des mots de passe de compte administrateur, afin qu'ils soient rapidement accessibles en cas d'urgence.
- Implémentez la gestion des mots de passe afin qu'elle ne compromette pas la capacité d'un opérateur à répondre à un événement tel qu'un arrêt d'urgence.
- Ne transmettez pas de mots de passe par e-mail ou d'une autre manière sur l'internet non sécurisé.

Gestion de HTTP

HTTP (*hypertext transfer protocol*) est le protocole sous-jacent du Web. Il est employé dans les systèmes de contrôle pour prendre en charge les serveurs Web intégrés dans les produits de contrôle. Les serveurs Web Schneider Electric utilisent des communications HTTP pour afficher les données et envoyer des commandes via des pages Web.

Si le serveur HTTP n'est pas nécessaire, désactivez-le. Sinon, utilisez si possible à la place de HTTP le protocole HTTPS *hypertext transfer protocol secure*, une combinaison du protocole HTTP et d'un protocole cryptographique. N'autorisez que le trafic vers certains

équipements, en mettant en place des mécanismes de contrôle d'accès comme une règle de parefeu qui limite l'accès de certains équipements à d'autres équipements.

Vous pouvez configurer HTTPS comme serveur Web par défaut sur les produits qui prennent en charge cette fonctionnalité.

Importez et approuvez les certificats auto-signés de vos contrôleurs M580 dans vos navigateurs Web à partir d'un réseau approuvé. Vous éviterez ainsi l'affichage de la notification de sécurité lors de la connexion aux pages Web de vos contrôleurs approuvés.

NOTE: Ce processus doit être répété lors du renouvellement des certificats des contrôleurs, par exemple lorsque vous changez les adresses IP de votre contrôleur à partir de l'application.

Gestion de FTP

Le protocole FTP (*file transfer protocol*) fournit des services de gestion de fichiers distants via un réseau de base TCP/IP comme Internet. FTP utilise une architecture client-serveur ainsi que des connexions de contrôle et de données distinctes entre le client et le serveur.

Tenez compte du comportement suivant du service FTP fourni par Schneider Electric :

- Le protocole FTP est désactivé par défaut.
- Le protocole FTP n'est nécessaire que pour des activités de maintenance et de configuration spécifiques. Une bonne pratique consiste à désactiver l'ensemble des services FTP lorsqu'ils ne sont pas nécessaires.
- FTP est un protocole non sécurisé qui doit être utilisé avec précaution pour éviter la divulgation d'informations sensibles et l'accès non autorisé aux contrôleurs :
 - Modifiez si possible les mots de passe par défaut de tous les équipements qui prennent en charge FTP.
 - Utilisez la liste de contrôle d'accès (ACL) pour restreindre la communication aux adresses IP autorisées. Pour plus d'informations sur le module concerné, consultez la section "Services de Cybersécurité par système".
 - Si vous utilisez un module BMENOC, configurez la fonction IPSEC ([Configuration de la communication chiffrée](#), page 36).
 - Bloquez tous les trafics FTP entrants et sortants à la frontière du réseau d'entreprise et du réseau d'exploitation de la salle de contrôle.
 - Filtrez les commandes FTP entre le réseau de contrôle et le réseau d'exploitation pour certains hôtes ou communiquez-les sur un réseau de gestion distinct implémentant une fonction de chiffrement.
 - Utilisez un module externe pour configurer un VPN entre les modules impactés du contrôleur et le poste d'ingénierie sur le réseau de contrôle.

- Les modules BMENOC0301 and BMENOC0311 ne prennent pas en charge le transfert IP vers le réseau d'équipements.

Si la transparence est requise entre réseau de contrôle et réseau d'équipement, un routeur externe / VPN est nécessaire pour chiffrer la communication entre les deux réseaux (voir l'illustration dans [Cible de sécurité CSPN, page 43](#)).

Dans le protocole FTP, la transparence est requise pour effectuer les opérations suivantes à partir du réseau de contrôle :

- Mise à jour du micrologiciel du contrôleur M580 à l'aide d'EcoStruxure Automation Device Maintenance.
- Diagnostic réseau du contrôleur M580 exécuté à partir d'un outil de gestion de réseau via le service SNMP.

Gestion de SNMP

Le protocole SNMP (*Simple Network Management Protocol*) fournit des services de gestion de réseau entre une console de gestion centrale et des équipements réseau tels que des routeurs, des imprimantes et des contrôleurs. Ce protocole est constitué de trois parties :

- Gestionnaire : application qui gère les agents SNMP sur un réseau par l'envoi de requêtes, la réception des réponses, l'écoute et le traitement des interruptions (traps) émises par les agents.
- Agent : module de gestion réseau situé sur un équipement géré. L'agent permet aux gestionnaires de modifier les paramètres de configuration. Les équipements gérés peuvent entre autres être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs (hubs), des contrôleurs ou des équipements périphériques.
- Système de gestion de réseau (NMS) : terminal via lequel les administrateurs peuvent effectuer des tâches d'administration.

Les équipements Ethernet de Schneider Electric disposent d'une fonction de service SNMP pour la gestion de réseau.

SNMP est souvent installé automatiquement avec la propriété de lecture **publique** et la propriété d'écriture **privée**. Ce type d'installation laisse à un utilisateur malveillant la possibilité de s'authentifier sur un système et de créer un refus de service.

Pour réduire le risque d'attaque via SNMP :

- Si SNMP v1 est nécessaire, utilisez les paramètres d'accès pour limiter les équipements (adresses IP) pouvant accéder au commutateur. Attribuez des mots de passe de lecture et de lecture/écriture différents aux équipements.
- Modifiez les mots de passe par défaut de tous les périphériques qui prennent en charge SNMP.
- Bloquez tout le trafic SNMP entrant et sortant à la frontière du réseau d'entreprise et du réseau d'exploitation de la salle de contrôle.

- Filtrez les commandes SNMP v1 entre le réseau de contrôle et le réseau d'exploitation sur des hôtes spécifiques ou communiquez-les sur un réseau de gestion distinct et chiffré.
- Contrôlez l'accès en identifiant l'adresse IP autorisée à interroger un équipement SNMP.
- Utilisez un module externe pour configurer un VPN entre les modules concernés du contrôleur et la station de travail d'ingénierie du réseau de contrôle.

Gestion des mots de passe Control Expert d'application, de section, de stockage des données et de micrologiciel

Dans Control Expert, les mots de passe s'appliquent aux éléments suivants (selon le contrôleur) :

- **Application**

La protection de l'application de Control Expert et du contrôleur par un mot de passe permet d'empêcher la modification, le téléchargement et l'ouverture indésirables de l'application (fichiers .STU, .STA and .ZEF). Le mot de passe est stocké de manière chiffrée dans l'application.

En plus de cette protection par mot de passe, vous pouvez chiffrer les fichiers .STU, .STA et .ZEF. La fonction Control Expert de chiffrement de fichiers permet d'empêcher les modifications par du personnel non qualifié sans autorisation et renforce la protection contre le vol de propriété intellectuelle et d'autres actes de malveillance. L'option de chiffrement de fichier est protégée par un mécanisme de mot de passe.

NOTE: Lorsqu'un contrôleur est géré dans le cadre d'un projet système, le mot de passe de l'application et le chiffrement des fichiers sont désactivés dans l'éditeur Control Expert et doivent être gérés à l'aide de Topology Manager.

Pour plus d'informations, consultez la rubrique *Protection de l'application* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

- **Section**

La fonction de protection des sections est accessible à partir de l'écran **Propriétés** du projet en mode local (non connecté). Cette fonction permet de protéger les sections du programme. Pour plus d'informations, consultez la rubrique *Protection des sections et des sous-programmes* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

NOTE: La protection des sections n'est pas active tant que la protection n'a pas été activée dans le projet.

- **Stockage de données/Web**

La protection du stockage des données par un mot de passe peut empêcher les accès indésirables à la zone de stockage des données de la carte mémoire SD (si une carte valide est insérée dans le contrôleur). Elle peut également empêcher l'accès indésirable aux diagnostics Web (pour les versions de micrologiciel du contrôleur M580 égales ou supérieures à 4.0). Pour plus d'informations, consultez la rubrique *Protection du stockage des données* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

- **Micrologiciel**

La protection du téléchargement de micrologiciel par un mot de passe permet d'empêcher le téléchargement de micrologiciels malveillants. Pour plus d'informations, consultez la rubrique *Protection du micrologiciel* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

Autorisations de contrôle

Control Expert Security Editor

Un outil de configuration de la sécurité permet de définir les utilisateurs du logiciel et leurs autorisations respectives. La sécurité d'accès EcoStruxure Control Expert concerne le ou les terminaux sur lesquels le logiciel est installé et non pas le projet, lequel dispose de son propre système de protection.

Pour plus d'informations, consultez *EcoStruxure™ Control Expert, Security Editor, Operation Guide*.

Il est recommandé d'établir un mot de passe dédié à l'administrateur de la sécurité (*SecurityAdmin*) et de limiter les autorisations des autres utilisateurs à l'aide d'un profil restrictif.

Modes programmation et surveillance

Deux modes sont disponibles pour accéder au contrôleur dans le mode **En ligne** :

- **Mode Programmation** : Le programme du contrôleur peut être modifié. Lorsqu'un terminal se connecte pour la première fois au contrôleur, celui-ci devient réservé et aucun autre terminal ne peut s'y connecter tant qu'il est réservé.
- **Mode Surveillance** : Le programme du contrôleur n'est pas modifiable, mais les variables le sont. Le mode surveillance ne réserve pas le contrôleur, de sorte qu'un contrôleur réservé reste accessible en mode surveillance.

Pour choisir un mode dans EcoStruxure Control Expert, sélectionnez : **Outils > Options... > Connexion > Mode de connexion par défaut**.

Pour plus d'informations sur ces modes, consultez la rubrique *Services en mode en ligne* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

Il est recommandé de définir le mode d'accès **En ligne** du contrôleur sur **Surveillance** dans la mesure du possible.

Protection des sections de programme

La fonction de protection des sections de programme est accessible dans l'écran **Propriétés** du projet en mode hors ligne (non connecté). Elle permet de protéger les sections du programme. Pour plus d'informations, consultez la rubrique *Protection des sections et des sous-programmes* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

NOTE: La protection des sections n'est pas active tant qu'elle n'a pas été activée dans le projet.

Il est recommandé d'activer la protection des sections.

Protection de la mémoire du contrôleur

La protection de la mémoire interdit le transfert d'un projet vers le contrôleur et les modifications en mode En ligne, quelle que soit la voie de communication.

NOTE: La protection de la mémoire du contrôleur ne peut pas être configurée avec des contrôleurs à redondance d'UC (Hot Standby). Dans ce cas, utilisez une communication chiffrée IPsec.

La protection de la mémoire est activée comme suit :

- Contrôleur Modicon M340 : Bit d'entrée. Pour plus d'informations, consultez la section *Configuration des processeurs Modicon M340 du Modicon* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).
- Contrôleur Modicon M580 : Bit d'entrée. Pour plus d'informations, consultez la section *Gestion de l'entrée Run/Stop* (voir Modicon M580 - Manuel de référence du matériel).
- Contrôleur Modicon Quantum : Commutateur à clé physique sur le module contrôleur, que ce soit pour un contrôleur d'entrée de gamme (voir Quantum avec EcoStruxure™ Control Expert - Manuel de référence du matériel) ou un contrôleur haut de gamme (voir Quantum avec EcoStruxure™ Control Expert - Manuel de référence du matériel).
- Contrôleur Modicon Premium : Bit d'entrée. Pour plus d'informations, consultez la section *Configuration des processeurs Premium* (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

- Contrôleur Modicon MC80 : Bit d'entrée. Pour plus d'informations, consultez le Manuel utilisateur du contrôleur logique programmable Modicon MC80 .
- Contrôleur Modicon Momentum MDI : Bit d'entrée. Pour plus d'informations, consultez le document EcoStruxure™ Control Expert - Processeurs 171CBU78090, 171CBU98090, 171CBU98091 - Guide utilisateur.

Il est recommandé d'activer la protection de la mémoire du contrôleur chaque fois que cela est possible.

Accès Run/Stop à distance au contrôleur

La gestion de l'accès Run/Stop à distance définit comment un contrôleur peut être démarré ou arrêté à distance et dépend du système.

NOTE: L'accès Run/Stop à distance ne peut pas être configuré avec les contrôleurs à redondance d'UC (Hot Standby). Dans ce cas, utilisez une communication chiffrée IPsec.

Contrôleur	Accès
Modicon M580:	L'accès à distance aux modes Run/Stop du contrôleur permet l'une des actions suivantes : • Arrêter ou lancer le contrôleur à distance via une requête. • Arrêter le contrôleur à distance via une requête. Rejeter les commandes de lancement du contrôleur à distance via une requête. Seule une commande d'exécution contrôlée par l'entrée est possible lorsqu'une entrée valide est configurée. • Rejeter les commandes d'exécution ou d'arrêt du contrôleur à distance via une requête. Consultez la section <i>Gestion de l'entrée Run/Stop</i> pour les options de configuration du contrôleur qui empêchent les commandes distantes d'accéder aux modes Run/ Stop (voir Modicon M580 - Manuel de référence du matériel).
Modicon M340:	L'accès à distance aux modes Run/Stop du contrôleur permet l'une des actions suivantes : • Arrêter ou lancer le contrôleur à distance via une requête. • Arrêter le contrôleur à distance via une requête. Rejeter les commandes de lancement du contrôleur à distance via une requête. Seule une commande d'exécution contrôlée par l'entrée est possible lorsqu'une entrée valide est configurée. Consultez la section <i>Configuration des processeurs Modicon M340</i> (voir EcoStruxure™ Control Expert - Modes de fonctionnement).

Modicon Premium:	L'accès à distance aux modes Run/Stop du contrôleur permet l'une des actions suivantes : • Arrêter ou lancer le contrôleur à distance via une requête. • Arrêter le contrôleur à distance via une requête. Rejeter les commandes de lancement du contrôleur à distance via une requête. Seule une commande d'exécution contrôlée par l'entrée est possible lorsqu'une entrée valide est configurée. Consultez la section <i>Configuration des processeurs Premium/Atrium</i> (voir EcoStruxure™ Control Expert - Modes de fonctionnement).
Modicon Quantum:	L'accès à distance aux modes Run/Stop du contrôleur permet les actions suivantes : • Arrêter ou lancer le contrôleur à distance à l'aide d'une requête.
Modicon MC80:	L'accès à distance aux modes Run/Stop du contrôleur permet l'une des actions suivantes : • Arrêter ou lancer le contrôleur à distance via une requête. • Arrêter le contrôleur à distance via une requête. Rejeter les commandes de lancement du contrôleur à distance via une requête. Seule une commande d'exécution contrôlée par l'entrée est possible lorsqu'une entrée valide est configurée. • Rejeter les commandes de lancement ou d'arrêt du contrôleur à distance via une requête. Reportez-vous à la section <i>Configuration des processeurs Modicon MC80</i> dans le Manuel utilisateur du contrôleur logique programmable (PLC) Modicon MC80.
Modicon Momentum MDI	L'accès à distance aux modes Run/Stop du contrôleur permet l'une des actions suivantes : • Arrêter ou lancer le contrôleur à distance via une requête. • Arrêter le contrôleur à distance via une requête. Rejeter les commandes de lancement du contrôleur à distance via une requête. Seule une commande d'exécution contrôlée par l'entrée est possible lorsqu'une entrée valide est configurée. Consultez la section <i>Configuration des processeurs Modicon Momentum MDI</i> dans le document Modicon Momentum pour EcoStruxure™ Control Expert - Processeurs 171CBU78090, 171CBU98090, 171CBU98091- Guide utilisateur.

Il est recommandé de refuser les commandes d'exécution ou d'arrêt du contrôleur à distance via une requête.

Accès aux variables du contrôleur

Pour protéger les données du contrôleur contre tout accès non autorisé en lecture ou en écriture, observez autant que possible les bonnes pratiques suivantes :

- Utilisez des données non localisées.

- Configurez EcoStruxure Control Expert pour stocker uniquement les variables IHM : **Outils > Options du projet... > Données intégrées de l'automate > Dictionnaire de données > Variables HMI seulement.**

L'option **Variables HMI seulement** ne peut être sélectionné que si **Dictionnaire de données** est sélectionné.

- Marquez comme *IHM* les variables accessibles à partir de l'IHM ou de SCADA. Les clients externes n'ont pas accès aux variables non déclarées comme *IHM*.
- La connexion avec SCADA doit s'appuyer sur OFS.

Protection de la mémoire des données

Vous pouvez activer la protection de la mémoire des données dans EcoStruxure Control Expert en accédant à **Outils > Options du projet > Données intégrées de l'automate** et en sélectionnant **Appliquer**. Cette fonction permet de protéger les données localisées et non localisées.

Pour plus d'informations sur la fonction de protection de la mémoire des données, consultez la rubrique Protection de la mémoire des données dans le document EcoStruxure Control Expert - Modes de fonctionnement.

Gestion des vérifications d'intégrité des données

Introduction

La fonction de vérification automatique d'intégrité disponible dans Control Expert permet d'empêcher toute modification des fichiers et logiciels Control Expert par un virus ou un logiciel malveillant. Vous pouvez également lancer manuellement la vérification d'intégrité.

Vérification d'intégrité automatique

Control Expert avec Topology Manager repose sur une architecture client/serveur.

Les serveurs sont configurés pour démarrer automatiquement lorsque l'ordinateur est mis sous tension ou redémarré. Avant de redémarrer, les deux serveurs sont soumis à une vérification d'intégrité.

Le serveur démarre uniquement si la vérification d'intégrité s'est terminée sans détecter d'altération des données. Si la vérification d'intégrité détecte une altération des données,

une erreur est consignée et vous pouvez la consulter à l'aide de l'**Observateur d'événements**.

Une fenêtre de message indique les fichiers corrompus. Cliquez sur **OK** pour fermer l'instance Control Expert. Pour plus d'informations, consultez le document *EcosSruxure Control Expert - Manuel d'installation* et la rubrique *Activation de la communication avec les clients distants et renforcement de la sécurité*.

Vérification d'intégrité manuelle avec Control Expert Classic

Procédez comme suit pour effectuer manuellement une vérification d'intégrité au démarrage d'une instance de Control Expert Classic :

Etape	Action
1	Cliquez sur Aide > A propos de Control Expert XXX .
2	Dans le champ Vérification de l'intégrité, cliquez sur Effectuer un auto-test. Résultat : La vérification d'intégrité s'exécute en arrière-plan. Control Expert crée un journal des connexions réussies et infructueuses de composants. Le fichier journal contient l'adresse IP, la date et l'heure ainsi que le résultat de la connexion. NOTE: Si une vérification d'intégrité affiche un échec de connexion pour un composant, l'Observateur d'événements affiche un message. Cliquez sur OK. Corrigez manuellement les éléments dans le journal.

Vérification manuelle de l'intégrité avec Control Expert

Pour effectuer une vérification manuelle de l'intégrité au démarrage d'une instance de Control Expert, procédez comme suit :

Etape	Action
1	Cliquez sur Aide > A propos de... dans la barre d'outils de Topology Manager.
2	Dans la zone A propos, cliquez sur le lien Effectuer un autotest. Résultat : La vérification d'intégrité s'exécute en arrière-plan. Les analyses sont effectuées sur les serveurs (locaux ou distants) auxquels le client est connecté. Le client et les serveurs continuent de s'exécuter jusqu'à ce que le résultat de la vérification d'intégrité soit renvoyé. Consultez le tableau suivant pour connaître les conséquences du contrôle d'intégrité.

Si	Alors
Aucune corruption de données n'est détectée	Un message indique que l'autotest s'est terminé avec succès. Cliquez sur OK .
Des données endommagées sont détectées sur le client	Une fenêtre de message indique les fichiers corrompus. Cliquez sur OK pour fermer le client Control Expert.
Des données endommagées sont détectées sur l'un des serveurs	Le serveur s'arrête. Une erreur est consignée et vous pouvez la consulter à l'aide de l' Observateur d'événements .

Vérification d'intégrité du micrologiciel M580

La vérification de l'intégrité du micrologiciel du contrôleur M580 s'effectue automatiquement après le chargement d'un nouveau micrologiciel ou le redémarrage du Modicon M580 PAC.

Gestion de la carte SD

Activez la signature de l'application pour éviter d'exécuter une application incorrecte à partir d'une carte SD.

La signature de la carte SD est gérée à l'aide des fonctions `SIG_WRITE` et `SIG_CHECK` (voir *EcoStruxure™ Control Expert, Communication, Block Library*).

Configuration de la protection du port de carte SD

Un mécanisme de protection de carte SD est disponible pour les contrôleurs équipés de la version 4.30 ou ultérieure du micrologiciel.

Cette fonctionnalité peut être activée ou désactivée à partir de l'onglet **Configuration** dans les pages Web du contrôleur.

Pour ouvrir la page **Accueil** :

Etape	Action
1	Ouvrez un navigateur Internet.
2	Dans la barre d'adresse, entrez l'adresse IP du contrôleur.
3	Entrez le nom d'utilisateur modbususer et le mot de passe de l'application.
4	Appuyez sur Entrée et attendez que la page s'ouvre.

Etape	Action
5	Sélectionnez Configuration > Cybersécurité .
6	Dans la liste déroulante, sélectionnez Port de carte SD pour configurer la fonction : • Activé (les cartes SD ne sont pas prises en compte par le contrôleur). • Désactivé (les cartes SD sont prises en compte par le contrôleur). NOTE: Si une carte SD est déjà insérée dans le contrôleur, la protection est activée lorsque la carte SD est retirée ou que le contrôleur est arrêté puis redémarré. NOTE: Lorsque la protection du port de carte SD est activée, la zone de mémoire de sauvegarde du contrôleur est NAND. Par conséquent, si vous effacez la zone de sauvegarde alors que la protection est activée, la zone NAND du contrôleur est effacée.

Configurer une liaison d'ingénierie sécurisée entre Control Expert et un contrôleur Ethernet M580

Compatibilité

- M580 avec PV < 25 (contrôleurs blancs) et PV >= 25 (contrôleurs gris).
- Control Expert Classic et Control Expert Topology Manager versions V16.0 et ultérieures.
- Micrologiciel M580 V4.20 et versions ultérieures.
- Application Control Expert V4.20 et versions ultérieures.

Objectif d'une connexion sécurisée

Avec les versions de logiciel, de matériel et d'application référencées ci-dessus, vous pouvez configurer une connexion sécurisée entre Control Expert et un contrôleur Ethernet M580. Cette connexion s'appuie sur le protocole TLS (Transport Layer Security) et assure une communication chiffrée de bout en bout.

Une liaison d'ingénierie sécurisée permet de protéger le contrôleur M580 contre les cyberattaques en fournissant les fonctions suivantes :

- Authentification du contrôleur basée sur un certificat M580 auto-signé.
- Chiffrement des flux de données entre Control Expert et le contrôleur M580.
- Authentification du client Control Expert via l'exigence d'un identifiant et d'un mot de passe pour établir le tunnel HTTPS.

Une connexion sécurisée protège contre les attaques de réseau suivantes :

- Attaques de reproduction.
- Récupération de mot de passe (hachage).
- Récupération du code binaire de l'application.
- Attaques de type "homme du milieu" (MitM - Man-in-the-middle) pouvant modifier les données ou l'application.

Caractéristiques d'une connexion sécurisée

Les fonctionnalités suivantes ont été ajoutées à **Security Editor**, au micrologiciel du contrôleur M580 et à Control Expert pour prendre en charge la création d'une liaison d'ingénierie sécurisée :

- Pilotes de protocole de communication sécurisée, page 114
- Trois modes de liaison d'ingénierie, page 114

Pilotes de protocole de communication

HTTPS et **HTTPS via USB** sont de nouveaux pilotes qui prennent en charge les liaisons d'ingénierie sécurisées.

NOTE: Pour plus de clarté, deux pilotes préexistants ont été renommés :

- **TCPIP** est devenu **Modbus TCP**
- **USB** est devenu **Modbus TCP via USB**

Modes de liaison d'ingénierie

En fonction du niveau de cybersécurité ciblé, vous pouvez sélectionner l'une des trois options suivantes comme **mode de liaison d'ingénierie** :

- **Accès complet :**

Le contrôleur fonctionne comme dans les versions précédentes du micrologiciel. Les communications sécurisées et non sécurisées sont acceptées.

- Pour la communication Control Expert, le contrôleur accepte les pilotes non sécurisés **Modbus TCP** et **Modbus TCP via USB** et les pilotes sécurisés **HTTPS** et **HTTPS via USB**.
- Pour la communication SCADA ou contrôleur à contrôleur, **Modbus TCP** (port 502) est accepté.

- **Filtré** (par défaut) :

Mode hybride que vous pouvez utiliser pour appliquer la cybersécurité sur la liaison d'ingénierie et la connectivité non sécurisée sur les liaisons vers SCADA ou d'autres contrôleurs.

- Pour la communication Control Expert, le contrôleur accepte les pilotes sécurisés **HTTPS** et **HTTPS via USB**.
- Pour la communication SCADA ou contrôleur à contrôleur, **Modbus TCP** (port 502) ou **UMAS** (OFS) sont acceptés.

NOTE: En mode **Filtré**, le contrôleur accepte les pilotes non sécurisés **Modbus TCP** et **Modbus TCP via USB**, mais uniquement si le **Mode de connexion** est réglé sur **surveillance** dans les options du projet. Le mode surveillance est un mode en lecture seule qui ne permet pas de télécharger une application sur le contrôleur ou d'arrêter le contrôleur.

- **Imposé** (par défaut) :

Ce mode offre le niveau de sécurité le plus élevé. Seuls les protocoles sécurisés sont acceptés par le contrôleur.

- Pour la communication Control Expert, le contrôleur accepte uniquement les pilotes sécurisés **HTTPS** et **HTTPS via USB**.
- Pour la communication SCADA ou contrôleur à contrôleur, **Modbus TCP** (port 502) et **UMAS** (OFS) ne sont **PAS** acceptés.

NOTE: Le temps de téléchargement de l'application peut être considérablement impacté si le mode **Accès complet** est configuré et qu'un pilote sécurisé **HTTPS** ou **HTTPS via USB** est utilisé. Si vous envisagez d'utiliser des pilotes sécurisés, choisissez plutôt le mode **Filtré** ou **Imposé** pour préserver les performances.

Récapitulatif de disponibilité des protocoles

Chaque option de **mode de liaison d'ingénierie** prend en charge certaines combinaisons de ports logiques et de protocoles de communication, à savoir :

Fonction de la liaison :		Liaison d'ingénierie sécurisée	Liaison d'ingénierie non sécurisée		IHM / SCADA
Pilotes :		HTTPS ou HTTPS via USB	Modbus TCP et Modbus TCP via USB		Modbus TCP/IP ou UMAS
Port logique de communication :		443	502		502
Mode de connexion :		Surveillance ou Programmation	Programma-tion	Surveillance	N/A
Mode de liaison d'ingénierie :	Imposé	✓	✗	✗	✗
	Filtré	✓	✗	✓	✓
	Accès complet	✓	✓	✓	✓

Liste autorisée de certificats Security Editor

Une **Liste autorisée de certificats** est introduite dans **Security Editor**, avec les fonctionnalités suivantes :

- **Ajouter** : Utilisez cette commande pour configurer l'adresse IP du contrôleur M580 sur lequel vous souhaitez créer une liaison d'ingénierie sécurisée.
- **Obtenir un certificat** : Utilisez cette commande pour récupérer le certificat HTTPS sur l'appareil.
- Boîte de dialogue qui vous permet d'approuver le certificat et de l'ajouter au magasin de certificats Windows.
- **Afficher le certificat** : Utilisez cette commande pour afficher et vérifier le certificat.
- **Supprimer** : Utilisez cette commande pour supprimer un certificat de la liste.

NOTE: Dans cette version, seuls les certificats auto-signés sont pris en charge.

Procédure de configuration d'une connexion sécurisée

La configuration de la liaison d'ingénierie sécurisée est effectuée à l'aide de Control Expert et de Security Editor en exécutant les tâches décrites ci-après.

Tâches préliminaires

1. Mettez à niveau votre contrôleur vers :
 - a. V4.20 ou une version ultérieure pour les contrôleurs standard.
 - b. V4.21 ou une version ultérieure pour les contrôleurs de sécurité.
2. Mettez à niveau Control Expert vers la version 16.0 ou ultérieure.
3. Ouvrez un projet existant et changez le niveau d'application pour la version V4.20 ou ultérieure, ou créez un projet avec le niveau d'application V4.20 ou version ultérieure.
4. S'il est désactivé, activez le service HTTPS dans l'onglet Sécurité du contrôleur.
5. Sélectionnez un mode de liaison d'ingénierie (voir *Modes de liaison d'ingénierie*).
6. Configurez les paramètres d'adresse IP définitifs du contrôleur Ethernet M580, si ce n'est pas déjà fait.

NOTE: Comme le certificat d'un contrôleur M580 contient son adresse IP, le contrôleur renouvelle son certificat chaque fois que vous modifiez son adresse IP. Vous devez à chaque fois approuver le certificat dans Security Editor.
7. Créez un mot de passe d'application pour le nouveau projet.
8. Créez des mots de passe de micrologiciel et d'accès Web pour le nouveau projet.
9. Téléchargez l'application sur le contrôleur à l'aide de **Modbus TCP** ou **Modbus TCP via USB**.

Tâche 1 : Approuver le certificat M580 dans Security Editor

1. Ouvrez Security Editor.
2. Lors du premier lancement de Security Editor, configurez un mot de passe pour SecurityAdmin et attendez que Security Editor s'installe.
3. Connectez-vous en tant que SecurityAdmin avec le mot de passe configuré.
4. Sélectionnez l'onglet **Liste autorisée de certificats**.

5. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une configuration de connexion** s'ouvre.
6. Sélectionnez **HTTPS** ou **HTTPS sur USB** comme **Protocole de communication**. Définissez ensuite le paramètre **Adresse IP** avec l'adresse IP configurée du contrôleur.
7. Cliquez sur **OK**.
8. Sélectionnez la ligne correspondant au contrôleur.
9. Cliquez sur **Approuver le certificat**, puis cliquez sur **Oui** pour effectuer l'ajout.
La colonne d'état du certificat est mise à jour et indique :
 - valide : Le certificat a bien été ajouté.
 - inconnu : Aucun certificat n'a été ajouté. Utilisez l'info-bulle pour afficher les détails des erreurs détectées.
10. Si le certificat est valide, cliquez sur le bouton affichant des points de suspension (...) pour afficher son nom et ses détails.

Tâche 2 : Configurer une connexion sécurisée

1. Sélectionnez **Automate > Définir l'adresse...** dans Control Expert.
2. Dans la zone Automate, saisissez l'adresse IP du contrôleur M580 ou SYS si vous utilisez un câble USB.
3. Dans la zone **Protocole de communication**, sélectionnez **HTTPS** ou **HTTPS via USB**.
4. Cliquez sur **OK**.
5. Dans Control Expert, sélectionnez **Automate > Connexion**.
6. Entrez le mot de passe de l'application.

Considérations relatives au mode de fonctionnement

Communication prête à l'emploi

Lorsque vous démarrez pour la première fois un contrôleur M580 prêt à l'emploi, les restrictions suivantes s'appliquent :

- Une connexion HTTPS entre Control Expert et le contrôleur M580 n'est pas prise en charge.
- La communication n'est possible qu'en utilisant USB ou TCPIP.

Réinitialisation d'un contrôleur M580 en mode NOCONF

Vous pouvez mettre votre contrôleur M580 en mode NOCONF de plusieurs manières :

- Réglez le commutateur rotatif pour réinitialiser un contrôleur M580 à redondance d'UC (Hot Standby).
- Utilisez une carte SD comme suit :
 1. Créez une application sans mot de passe.
 2. Chargez l'application dans un autre contrôleur M580 de référence identique.
 3. Insérez la carte SD dans ce contrôleur.
 4. Réglez %S66 sur TRUE pour sauvegarder l'application sur la carte SD.
 5. Insérez la carte SD dans le contrôleur M580 d'origine et redémarrez ce dernier.

Réinitialisation du mot de passe d'application

La réinitialisation du mot de passe de l'application via le support technique est toujours possible pour les options **Filtré** et **Accès complet** du **Mode de liaison d'ingénierie**.

La modification en ligne du mot de passe est prise en charge.

Compatibilité et limites de la programmation sécurisée imposée

Compatibilité

Consultez la rubrique Configurer une liaison d'ingénierie sécurisée entre Control Expert et un contrôleur Ethernet M580, page 113.

Limites du mode de liaison d'ingénierie

Pour toute connexion physique, les restrictions suivantes s'appliquent pour l'option **Imposé** du **mode de liaison d'ingénierie** :

- La fonctionnalité Dictionnaire de données n'est pas opérationnelle.
- BMENUA0100•• n'est pas pris en charge en mode pour le mode de liaison d'ingénierie Imposé.

- Effectuez une mise à niveau vers M580 avec une version de produit (PV) 3 ou ultérieure.
- Le contrôleur n'est pas accessible à l'aide des blocs fonction suivants :
 - READ_VAR
 - WRITE_VAR
 - DATA_EXCH
 - READ_REMOTE
- Le contrôleur ne peut pas être scruté par un scrutateur Modbus.
- Le scrutateur Modbus du contrôleur M580 ne peut pas scruter les équipements Modbus.
- Selon le protocole de communication sélectionné (Modbus TCP ou EtherNet/IP), certains services de diagnostic de DTM ne sont pas disponibles, à savoir :

Services DTM	Protocole	Disponibilité
Connexion DTM EtherNet/IP	EtherNet/IP	✓
Déconnexion DTM EtherNet/IP	EtherNet/IP	✓
Connexion DTM Modbus	Modbus TCP	✗
Déconnexion DTM Modbus	Modbus TCP	✗
Diagnostic Ethernet	EtherNet/IP	✓
Diagnostic de bande passante	Modbus TCP	✗
Diagnostic RSTP	Modbus TCP	✗
Diagnostic du service de temps réseau	EtherNet/IP	✓

Compatibilité des adaptateurs de communication

Le tableau suivant récapitule les services disponibles sur un contrôleur ou un adaptateur de communication en fonction du mode d'ingénierie sélectionné.

Les lignes correspondent aux services disponibles :

- Liaison d'ingénierie : Connexion entre Control Expert et le contrôleur.
- Communication en mode client : Scrutateur, Modbus, EtherNet/IP (implicite ou explicite), OPCUA, DNP3, IEC 61850.
- Communication en mode serveur : Modbus, EtherNet/IP, OPCUA, DNP3, IEC 61850.

Les colonnes correspondent aux différentes configurations possibles. Par exemple :

- Contrôleur seul : un contrôleur utilisé sans adaptateur de communication.
- Contrôleur + NOC avec embase activée : un contrôleur et un module BMENOC03•• dans le rack principal ; port d'embase du BMENOC03•• activé ; Control Expert connecté au BMENOC03••.
- Contrôleur + embase NOC désactivée : un contrôleur et un BMENOC03•• dans le rack principal ; port d'embase du BMENOC03•• désactivé ; Control Expert connecté au BMENOC03••.

Lorsqu'un adaptateur de communication est utilisé, certains services sont disponibles sur l'adaptateur de communication lui-même ou par son intermédiaire sur le contrôleur. Pour distinguer ces deux cas, les lettres "C" (pour contrôleur) et "M" (pour module) sont utilisées. Par exemple :

- Si la connexion entre Control Expert et le contrôleur peut être établie à l'aide de l'adresse IP du contrôleur, la lettre "C" est indiquée.
- Si la connexion à partir de Control Expert est établie à l'aide de l'adresse IP du module BMENUA0100, la lettre "M" est indiquée dans la colonne relative au module.

Système modicon M580			Contrôleur seul			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + NOC321			Contrôleur + NUA (mode sécurité)			Contrôleur + BMXNOR			Contrôleur + BMENOR étape 3			Contrôleur + NOP			Contrôleur + NOP		
Paramètre de l'adaptateur de communication						Port d'embase activé			Port d'embase désactivé			Port d'embase désactivé Transfert IP			Transfert IP			Embase isolée			Port d'embase désactivé			Port d'embase activé Sans transfert IP			Port d'embase désactivé Transfert IP		
Topologie																													
Mode sécurité			  			  			  			  			  			  			  			  			  		
Liaison d'ingénierie	HTTPS	C	C	C	C	C	C	X	X	X	C	C	C	C* M	C* M	X	X	X	X	X	X	X	C	C	C	X	X	X	
	Modbus TCP Surveillance	C	C	X	C M	C M	X	C	C	X	C	C	X	C* M	C* M	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X	
	Modbus TCP Programmation	C	X	X	C M	X	X	C	X	X	C	X	X	C* M	X	X	M	X	X	M**	X	X	C M	X	X	M	X	X	

Système modicon M580					Contrôleur seul			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + NOC321			Contrôleur + NUA (mode sécurité)			Contrôleur + BMXNOR			Contrôleur + BMENOR étape 3			Contrôleur + NOP			Contrôleur + NOP				
Paramètre de l'adaptateur de communication					Port d'embase activé			Port d'embase désactivé			Port d'embase désactivé Transfert IP			Transfert IP			Embase isolée			Port d'embase désactivé			Port d'embase activé Sans transfert IP			Port d'embase désactivé Transfert IP							
Topologie																																	
Mode sécurité																																	
Mode client		Scrutateur d'E/S Modbus			C	C	X	C	C	M	M	M	M	C	C	M	C*	C*	X	-	-	-	-	-	-	C	C	X	-	-	-		
		Scrutateur EIP			C	C	C	C	C	M	C	M	M	M	C	C	M	C	C	C*	-	-	-	-	-	-	C	C	C	-	-	-	
		EFB Modbus			C	C	X	C	C	X	C	C	C	X	C	C	X	C*	C*	X	C	C	X	C	C	X	C	C	X	C	C	X	
		EFB EIP			C	C	C	C	C	C	C	C	C	C	C	C	C	C	C*	C*	C*	C	C	C	C	C	C	C	C	C	C	C	C
		EFB OPCUA			C	C	C	-	-	-	-	-	-	-	C	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	C	C	C
		DNP3 IEC 60870			-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-	-
		IEC 61850			-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	
Mode serveur		Serveur Modbus /UMAS			C	C	X	M	M	X	M	M	X	C	C	X	C*	C*	X	M	M	X	M**	M**	X	C	C	X	M	M	X		

Système modicon M580					Contrôleur seul			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + modules NOC (NOC301, NOC311, NOC321)			Contrôleur + NOC321			Contrôleur + NUA (mode sécurité)			Contrôleur + BMXNOR			Contrôleur + BMENOR étape 3			Contrôleur + NOP			Contrôleur + NOP				
Paramètre de l'adaptateur de communication								Port d'embase activé			Port d'embase désactivé			Port d'embase désactivé Transfert IP			Transfert IP			Embase isolée			Port d'embase désactivé			Port d'embase activé Sans transfert IP			Port d'embase désactivé Transfert IP				
Topologie																																	
Mode sécurité																																	
Communication SCADA					Serveur OPCUA			-	-	-	-	-	-	-	M	M	X	-	-	-	-	-	-	-	-	-	-	-	-				
					Adaptateur EtherNet/IP (serveur local)			C	C	C	M	M	M	M	M	M	C M	C M	C M	-	-	-	-	-	-	-	-	-	-	-	-	-	-
					Serveur Web HTTPS du contrôleur			C	C	C	C	C	C	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	C	C	C	-	-	-
					DNP3 - IEC 60870			-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-	-
					IEC 61850			-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	M

Symbole	Description
	Mode de liaison d'ingénierie réglé sur Accès complet
	Mode de liaison d'ingénierie réglé sur Filtré
	Mode de liaison d'ingénierie réglé sur Imposé
C	- En mode client, "C" indique que la communication est initiée par le contrôleur. - En mode serveur, "C" indique que l'adresse IP de destination est le contrôleur.
M	- En mode client, "M" indique que la communication est initiée par l'adaptateur de communication. - En mode serveur, "M" indique que l'adresse IP de destination est l'adaptateur de communication. Dans les deux cas, le module communique avec le contrôleur via XBUS.
X	Pas de prise en charge
*	En fonction des règles de transfert configurées dans le module BMENUA0100.
**	Si le serveur Modbus est activé dans le BMENOR00200
-	Non applicable

Ports et services Ethernet du système M580

Cette rubrique présente les services Ethernet M580 disponibles et leur état par défaut dans l'application Control Expert.

La mention "Prêt à l'emploi" indique que la configuration s'applique à un contrôleur sorti d'usine, sans application installée. Une fois qu'une application a été installée sur le contrôleur, cette configuration "prête à l'emploi" ne peut plus jamais être réalisée.

"Par défaut" indique que la configuration s'applique à une application Control Expert par défaut.

Contrôleurs M580 avec version de micrologiciel ≥ 4.10

Service	Numéro de port	Prêt à l'emploi	Par défaut	Remarques
HTTP	80/tcp	Fermé	Fermé	Serveur Web.
Modbus TCP	502/tcp	Ouvert	Ouvert	-
EtherNet/IP	44818/tcp-udp	Fermé	Fermé	EtherNet/IP explicite (classe 3)
DHCP	67/udp	Fermé	Fermé	-
FTP	21/tcp	Ouvert	Fermé	Micrologiciel, stockage de données, FDR
TFTP	69/udp	Fermé	Fermé	FDR (X80)
SNMP	161/udp	Fermé	Fermé	-
EtherNet/IP	2222/udp	Fermé	Fermé	EtherNet/IP implicite (classe 1)
NTP/SNTP	123/udp	Fermé	Fermé	NTPV4 ou SNTP

Contrôleurs M580 avec version de micrologiciel < 4.10

Service	Numéro de port	Prêt à l'emploi	Par défaut	Remarques
HTTPS	443/tcp	Ouvert	Ouvert	Web, micrologiciel, stockage de données
Modbus TCP	502/tcp	Ouvert	Ouvert	REMARQUE ⁽¹⁾
EtherNet/IP	44818/tcp-udp	Fermé	Fermé	EtherNet/IP explicite (classe 3)
DHCP	67/udp	Fermé	Fermé	-

Service	Numéro de port	Prêt à l'emploi	Par défaut	Remarques
FTP	21/tcp	Fermé	Fermé	FDR
TFTP	69/udp	Fermé	Fermé	FDR (X80)
SNMP	161/udp	Fermé	Fermé	-
EtherNet/IP	2222/udp	Fermé	Fermé	EtherNet/IP implicite (classe 1)
NTP/SNTP	123/udp	Fermé	Fermé	NTPV4 ou SNTP
DPWS	9867/tcp	Ouvert	Ouvert	Mise à jour de micrologiciel, REMARQUE ⁽¹⁾
WS-Discovery	3702/udp	Fermé	Fermé	Synchronisation d'état avec SNMP
REMARQUE ⁽¹⁾ : Le port et le service associé sont essentiels pour le client afin de s'assurer que les fonctions fondamentales sont opérationnelles dans l'environnement industriel souhaité. Le port reste ouvert pour des raisons de sécurité et de disponibilité. Les utilisateurs ne peuvent pas désactiver le port.				

Services de Cybersécurité par système

Introduction

Ce chapitre répertorie les principaux services de cybersécurité disponibles pour chaque système et indique où trouver des informations détaillées dans l'aide de Control Expert.

Services de Cybersécurité

Présentation

Les logiciels, DTM ou équipements assurent des services de cybersécurité dans un système global. Les services de cybersécurité disponibles sont répertoriés pour les éléments suivants :

- Logiciel Control Expert, page 129
- Contrôleur Modicon M340, page 129
- Contrôleur Modicon M580, page 130
- Contrôleurs et modules de communication Modicon Quantum, page 131
- Modules Modicon X80, page 132
- Contrôleurs et modules de communication Modicon Premium/Atrium, page 133
- Modicon Momentum MDI, page 135
- Modicon MC80, page 135

Les services de cybersécurité répertoriés ci-dessous sont décrits dans le chapitre précédent :

- Désactivation des services inutilisés, page 32
- Contrôle d'accès, page 33
- Configuration de la communication chiffrée, page 36
- Consignation des événements, page 52
- Authentification, page 100
- Autorisations, page 105
- Vérifications d'intégrité, page 109

Services de Cybersécurité du logiciel Unity Pro/Control Expert

Unity Pro est l'ancien nom de Control Expert pour les versions 13.1 et antérieures.

Disponibilité des services de Cybersécurité

Logiciel	Services de Cybersécurité							
Référence	Désacti- vation des services inutilisés	Contrôle d'accès	Commu- nication chiffrée	Commu- nication chiffrée avec confiden- tialité	Consi- gnation des évène- ments	Authenti- fication	Autorisa- tions	Vérifica- tions d'intégre- té
Unity Pro v8.1	–	N.A.	–	–	–	X	X	X
Unity Pro ≥ v10.0	–	N.A.	X	–	X	X	X	X
Unity Pro ≥ v13.0	–	N.A.	X	X	X	X	X	X
Control Expert ≥ v14.0	X	X	X	X	X	X	X	X
X Disponible, au moins un service est mis en œuvre. – Non disponible N.A. Non applicable								

Des mécanismes de récupération de mot de passe plus robustes sont disponibles avec les versions de Control Expert égales au supérieures à v.15.1 ciblant des applications pour versions de micrologiciel M580 égales ou supérieures à v4.01.

Services de Cybersécurité du contrôleur Modicon M340

Version minimum de micrologiciel et disponibilité des services de cybersécurité dans le contrôleur Modicon M340 :

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–
X Disponible, au moins un service est mis en œuvre.								
– Non disponible								

Services de Cybersécurité du contrôleur Modicon M580

Version minimum de micrologiciel et disponibilité des services de cybersécurité dans le contrôleur Modicon M580 :

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
BME P58 5040	2.10	X	X	–	X	X	X	X

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
BME P58 6040	2.10	X	X	–	X	X	X	X
BME H58 2040	2.10	X	X	–	X	X	X	X
BME H58 4040	2.10	X	X	–	X	X	X	X
BME H58 6040	2.10	X	X	–	X	X	X	X
X Disponible, au moins un service est mis en œuvre.								
– Non disponible								

Services de Cybersécurité des contrôleurs et modules Modicon Quantum

Version minimum de micrologiciel et disponibilité des services de cybersécurité dans le contrôleur Modicon Quantum :

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
140CPU31110	3.20	–	–	–	–	X	X	–
140CPU43412•	3.20	–	–	–	–	X	X	–
140CPU53414•	3.20	–	–	–	–	X	X	–
140CPU651•0	3.20	X	X	–	–	X	X	–
140CPU65260	3.20	X	X	–	–	X	X	–
140CPU65860	3.20	X	X	–	–	X	X	–
140CPU67060	3.20	X	X	–	–	X	X	–
140CPU67160	3.20	X	X	–	–	X	X	–
140CPU6726•	3.20	X	X	–	–	X	X	–

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérfications d'intégrité
140CPU67861	3.20	X	X	–	–	X	X	–
X Disponible, au moins un service est mis en œuvre. – Non disponible								

Modules Modicon Quantum prenant en charge les services de cybersécurité :

Module		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérfications d'intégrité
140NOC7710•	1.00	–	X	–	–	X	–	–
140NOC78000	2.00	X	X	–	–	X	–	–
140NOC78100	2.00	X	X	–	–	X	–	–
140NOE771••	X	X	–	–	–	X	–	–
140NWM10000	–	X	–	–	–	–	–	–
X Disponible, au moins un service est mis en œuvre. – Non disponible								

Services de Cybersécurité des modules Modicon X80

Modules Modicon X80 prenant en charge les services de cybersécurité :

Module		Services de Cybersécurité							
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Communication chiffrée avec confidentialité	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
BMECXM0100	1.01	X	X	–	–	X	–	–	X
BMENOC0301	1,01	X	X	X	–	X	X	–	X
BMENOC0311	1,01	X	X	X	–	X	X	–	X
BMXNOC0401.2	2.05	X	X	–	–	–	–	–	–
BMXNOE0100.2	2.90	X	X	–	–	–	–	–	–
BMXNOE0110.2	6.00	X	X	–	–	–	–	–	–
BMXPRA0100	2.60	X	X	–	–	–	X	–	–
BMENOC0301	2.11	X	X	X	X	X	X	–	X
BMENOC0311	2.11	X	X	X	X	X	X	–	X
X Disponible, au moins un service est mis en œuvre.									
– Non disponible									

Services de Cybersécurité des contrôleurs et modules Modicon Premium/Atrium

Version minimum de micrologiciel et disponibilité des services de cybersécurité dans le contrôleur Modicon Premium/Atrium :

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
TSXH57•4M	3.10	–	–	–	–	X	X	–
TSXP570244M	3.10	–	–	–	–	X	X	–
TSXP57•04M	3.10	–	–	–	–	X	X	–
TSXP57•54M	3.10	–	–	–	–	X	X	–

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
TSXP571634M TSXP572634M TSXP573634M (via port ETY)	3.10	X	X	–	–	X	X	–
TSXP574634M TSXP575634M TSXP576634M (port Ethernet intégré)	3.10	X	X	–	–	X	X	–
X Disponible, au moins un service est mis en œuvre. – Non disponible								

Modules Modicon Premium/Atrium prenant en charge les services de cybersécurité :

Module		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–
TSXETY5103	5.90	X	X	–	–	–	–	–
X Disponible, au moins un service est mis en œuvre. – Non disponible								

Services de cybersécurité du contrôleur et des modules Modicon Momentum MDI

Version minimale du micrologiciel et disponibilité des services de cybersécurité dans Modicon Momentum MDI:

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
171CBU78090	1.0	X	X	–	–	X	X	–
171CBU98090	1.0	X	X	–	–	X	X	–
171CBU98091	1.0	X	X	–	–	X	X	–
X Disponible, au moins un service est mis en œuvre.								
– Non disponible								

Services de cybersécurité du contrôleur et des modules Modicon MC80

Version minimale du micrologiciel et disponibilité des services de cybersécurité dans Modicon MC80:

Contrôleur		Services de Cybersécurité						
Référence	Version min. micro-logiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication chiffrée	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
BMKC8020301	1.2	X	X	–	–	X	X	–
BMKC8020310	1.0	X	X	–	–	X	X	–
BMKC8030311	1.2	X	X	–	–	X	X	–
X Disponible, au moins un service est mis en œuvre.								
– Non disponible								

Services de sécurité Modicon M340

Présentation

Les paramètres des services de sécurité de la communication sont décrits pour le contrôleur Modicon M340 dans différents manuels comme indiqué dans la rubrique suivante.

Contrôleur Modicon M340 avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Paramètres de configuration de messagerie</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).

Services de sécurité Modicon M580

Contrôleur Modicon M580

La description des paramètres de communication liés à la cybersécurité est fournie dans la rubrique qui décrit l'*onglet Sécurité* (voir Modicon M580 - Manuel de référence du matériel).

Services de sécurité Modicon Quantum

Présentation

Les paramètres des services de sécurité de communication pour le contrôleur Modicon Quantum et les modules Ethernet sont décrits dans différents manuels indiqués dans les rubriques suivantes.

Contrôleur Modicon Quantum avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité (activer/désactiver HTTP, FTP et TFTP)</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Modicon Quantum avec Control Expert - Configuration de la messagerie du contrôleur Ethernet</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).

Module 140 NOC 771 0x

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité (activer/désactiver HTTP, FTP et TFTP)</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Configuration du contrôle d'accès</i> (voir Quantum avec EcoStruxure™ Control Expert - Module de communication Ethernet 140 NOC 771 01 - Manuel utilisateur).

Module 140 NOC 780 00

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Quantum EIO - Réseau de contrôle - Guide d'installation et de configuration).
Contrôle d'accès :	Consultez la section <i>Configuration du contrôle d'accès</i> (voir Quantum EIO - Réseau de contrôle - Guide d'installation et de configuration).

Module 140 NOC 781 00

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Quantum EIO - Réseau de contrôle - Guide d'installation et de configuration).
Contrôle d'accès :	Consultez la section <i>Configuration du contrôle d'accès</i> (voir Quantum EIO - Réseau de contrôle - Guide d'installation et de configuration).

Module 140 NOE 771 xx

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité (activer/désactiver HTTP, FTP et TFTP)</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur), la section <i>Sécurité</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur) et la section <i>Définition des mots de passe HTTP et d'écriture</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
--------------------------	--

Module 140 NWM 100 00

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité (activer/désactiver HTTP, FTP et TFTP)</i> (voir Quantum avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
--------------------------	---

Services de sécurité Modicon X80

Présentation

Les paramètres des services de sécurité de communication sont décrits pour les modules Ethernet Modicon X80 dans différents manuels, comme indiqué dans les rubriques suivantes.

Module BMXNOC0401.2

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).
Contrôle des accès :	Consultez la section <i>Configuration du contrôle d'accès</i> (voir Modicon M340 - Module de communication Ethernet BMX NOC 0401 - Manuel utilisateur).

Modules BMXNOE0100.2 et BMXNOE0110.2

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Paramètres de configuration de messagerie</i> (voir Modicon M340 pour Ethernet -Modules de communication et processeurs - Manuel utilisateur).

Module BMXPRA0100

Le module BMXPRA0100 est configuré comme un contrôleur Modicon M340. Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Paramètres de configuration de messagerie</i> (voir Modicon M340 pour Ethernet - Modules de communication et processeurs - Manuel utilisateur).

Module BMXNOR0200H

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Modicon X80 - Module RTU BMXNOR0200H - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Paramètres de configuration de messagerie</i> .

Module BMENOR2200H

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la section <i>Sécurité</i> .
Contrôle d'accès :	Consultez la section <i>Paramètres de configuration de messagerie</i> .

Module BMECXM0100

Les paramètres de communication liés à la cybersécurité sont décrits dans le chapitre *Configuration des services Ethernet* (voir Modicon M580 - Modules CANopen BMECXM - Manuel utilisateur).

Modules BMENOC0301 and BMENOC0311

Les paramètres de communication liés à la cybersécurité sont décrits dans la rubrique *Configuration des services de sécurité* (voir Modicon M580 BMENOC0301 / BMENOC0311 - Module de communication Ethernet - Guide d'installation et de configuration).

Module BMENUA0100

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques répertoriées :

Communication Ethernet :	Consultez la rubrique Paramètres de Cybersécurité (voir M580 - Module intégré OPC UA BMENUA0100 - Guide d'installation et de configuration).
Contrôle d'accès :	Consultez la rubrique <i>Contrôle d'accès</i> .

Services de sécurité Modicon Premium/Atrium

Présentation

Les paramètres des services de sécurité de communication pour le contrôleur Modicon Premium/Atrium et les modules Ethernet sont décrits dans différents manuels indiqués dans les rubriques suivantes.

Contrôleur Modicon Premium/Atrium avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Paramètres de configuration des services de sécurité</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Configuration de la messagerie TCP/IP (TSX P57 6634/5634/4634)</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).

Contrôleur Modicon Premium/Atrium via des ports ETY

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Paramètres de configuration des services de sécurité</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Configuration de la messagerie TCP/IP</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).

Module TSX ETC 101.2

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Sécurité</i> (voir Premium avec EcoStruxure™ Control Expert - Module de communication Ethernet TSX ETC 101 - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Configuration du contrôle d'accès</i> (voir Premium avec EcoStruxure™ Control Expert - Module de communication Ethernet TSX ETC 101 - Manuel utilisateur).

Module TSX ETY x103

Les paramètres de communication liés à la cybersécurité sont décrits aux emplacements indiqués :

Communication Ethernet :	Consultez la section <i>Paramètres de configuration des services de sécurité</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).
Contrôle d'accès :	Consultez la section <i>Configuration de la messagerie TCP/IP</i> (voir Premium et Atrium avec EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur).

Services de sécurité Modicon Momentum MDI

Les paramètres des services de sécurité de la communication sont décrits pour le contrôleur Modicon Momentum MDI dans le document *Momentum pour EcoStruxure™ Control Expert - Processeurs 171CBU78090, 171CBU98090, 171CBU98091 - Guide utilisateur*.

Services de sécurité Modicon MC80

Les paramètres des services de sécurité de la communication sont fournis pour le contrôleur MC80 dans le document *Modicon MC80 - Contrôleur logique programmable (PLC) - Manuel utilisateur*.

Comment protéger les architectures M580, M340, Momentum MDI et MC80 avec EAGLE40 en utilisant un VPN

Introduction

Ce chapitre explique comment renforcer la protection des contrôleurs contre les cyberattaques en utilisant un pare-feu tel que EAGLE40-07 de Belden configuré pour établir des connexions VPN. Le déploiement d'un tel dispositif dans une architecture peut atténuer les vulnérabilités existant dans les équipements et réduire la surface d'attaque des différents produits.

Il est recommandé de renforcer la protection du réseau, des stations de travail et des équipements comme indiqué dans le document *Cybersécurité des systèmes de contrôleur Modicon - Guide utilisateur*, téléchargeable à l'adresse : <https://www.se.com/us/en/download/document/EIO0000001999/>

Pare-feu EAGLE40

Pourquoi utiliser un pare-feu ?

L'utilisation d'un pare-feu pour renforcer la cybersécurité d'une architecture présente les avantages suivants :

- La cybersécurité des réseaux de contrôle et des équipements est renforcée.
- Le renforcement de la cybersécurité repose sur le protocole IPSEC.
- L'impact sur l'architecture et les performances existantes peut être minimisé.

Principales fonctionnalités du pare-feu EAGLE40

Le pare-feu EAGLE40 est une solution permettant de résoudre ou de limiter les problèmes résiduels de cybersécurité.

- Grâce au puissant VPN IPSEC, le pare-feu EAGLE40 assure la confidentialité du trafic réseau de manière à prévenir les attaques de type *homme du milieu*. Il garantit l'authentification de l'expéditeur en contribuant à empêcher les attaques par usurpation d'identité. L'intégrité des messages est renforcée par des méthodes cryptographiques et ne peut pas être altérée.
- Des fonctions de filtrage usuelles sont disponibles pour contrôler le trafic et les protocoles en fonction de l'adresse IP, de l'adresse Mac et du port des équipements réseau.
- Le pare-feu EAGLE40 est un produit évolutif qui peut être intégré dans des architectures multipoints, avec des performances de débit et de bande passante qui permettent d'assurer la transparence du réseau.

Prérequis

Installation du logiciel

Un logiciel client VPN compatible est nécessaire pour établir un tunnel VPN basé sur le protocole IPSEC entre le client et le pare-feu.

Le pare-feu EAGLE40 requiert l'utilisation du client VPN IPSEC/IKEV2.

NOTE: Utilisez la solution de client VPN fournie par TheGreenBow.

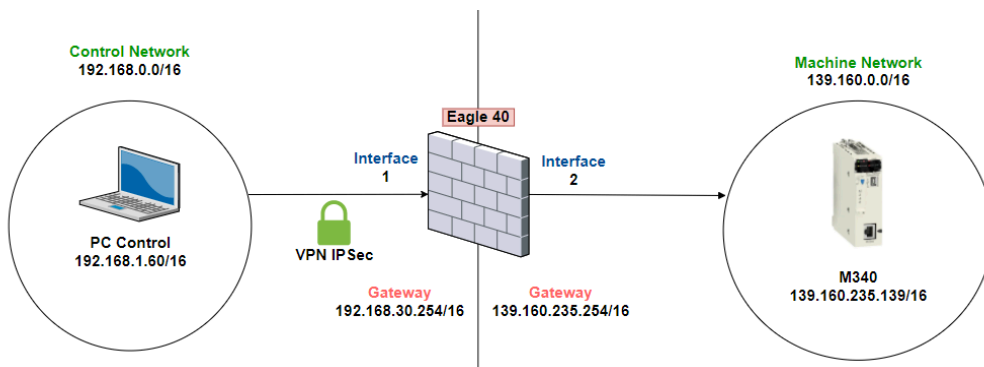
Dans les procédures de configuration décrites ci-dessous, nous utilisons ce logiciel que vous pouvez télécharger à l'adresse suivante :

<https://www.thegreenbow.com/en/>

Machines et systèmes d'exploitation

Avant de configurer le pare-feu, vous devez préparer toutes les adresses IP utilisées dans les architectures.

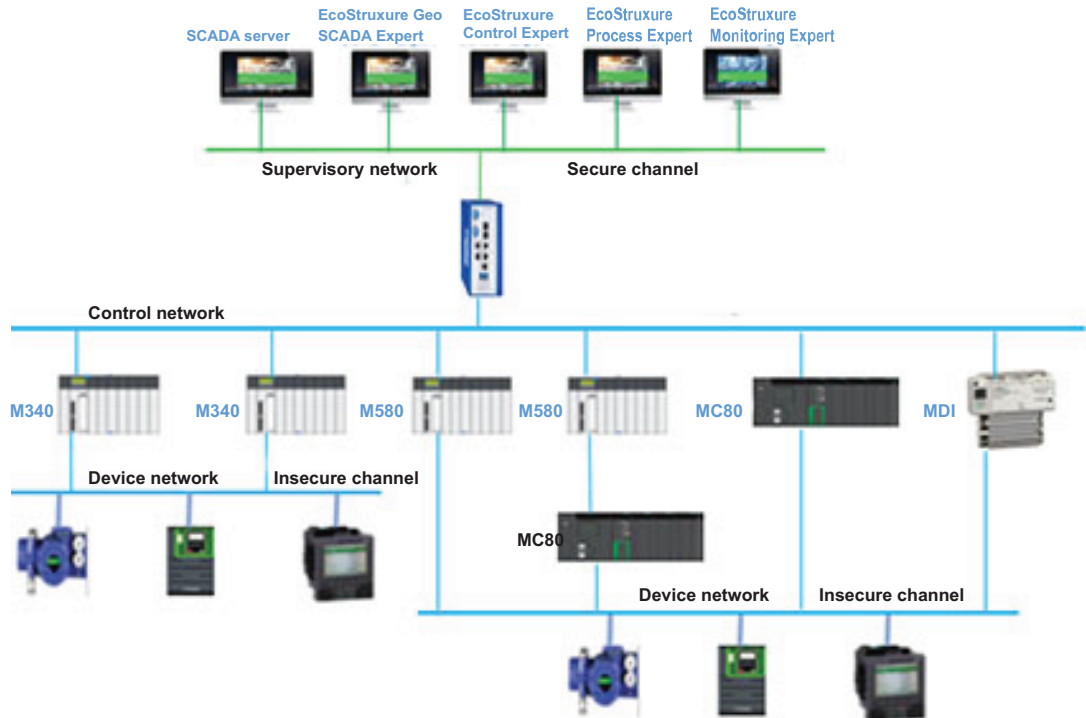
Le diagramme suivant est donné à titre d'exemple :



Architecture standard

Les instructions d'architecture et de configuration de ce document sont fournies à titre d'exemple et peuvent être adaptées à différentes architectures et différents systèmes.

Ainsi, l'architecture mixte ci-après qui combine des contrôleurs Modicon M340, M580, Momentum MDI et MC80 est relativement typique :



NOTE: Installez le pare-feu EAGLE40 à proximité des contrôleurs.

Configuration du pare-feu

Configuration Web

Pour configurer le pare-feu, ouvrez un navigateur Internet et entrez l'URL suivante :

[https://\[IPFirewall\]/admin](https://[IPFirewall]/admin)

Cliquez sur **Entrée** et utilisez la combinaison nom d'utilisateur/mot de passe par défaut
admin/private pour vous connecter.

NOTE: Lors de la première connexion, vous devez modifier le mot de passe.

Configuration des routes

Pour configurer les routes, procédez comme suit :

Etape	Action																																																																																								
1	Navigation File Network Security Virtual Private Network Overview Certificates Connections Switching Routing Global Interfaces Configuration Secondary Interface Address ARP Global Current Static OSPF Routing Table Tracking L2 Relay Loopback Interface Routing Interfaces Configuration <table><tr><th>Port</th><th>Name</th><th>Port on</th><th>Port status</th><th>IP address</th><th>Network</th><th>Routing</th><th>Proxy ARP</th><th>MTU value</th><th>ICMP unreachable</th><th>ICMP redirects</th></tr><tr><td>☐</td><td>1/1</td><td>GE</td><td>up</td><td>192.168.30.254</td><td>255.255.0.0</td><td>GE</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/2</td><td>GE</td><td>up</td><td>139.160.236.254</td><td>255.255.0.0</td><td>GE</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/3</td><td>GE</td><td>down</td><td>0.0.0.0</td><td>0.0.0.0</td><td>☐</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/4</td><td>GE</td><td>down</td><td>0.0.0.0</td><td>0.0.0.0</td><td>☐</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/5</td><td>GE</td><td>down</td><td>0.0.0.0</td><td>0.0.0.0</td><td>☐</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/6</td><td>GE</td><td>down</td><td>0.0.0.0</td><td>0.0.0.0</td><td>☐</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr><tr><td>☐</td><td>1/7</td><td>GE</td><td>down</td><td>0.0.0.0</td><td>0.0.0.0</td><td>☐</td><td>☐</td><td>1,500</td><td>GE</td><td>GE</td></tr></table> Choose the interface of choice to which you want to give an IP (a route), and start the wizard ✓ ↺ 🖨 2 ➡ ⚙ ? 1. Dans le volet Navigation à gauche, ouvrez Routing > Interfaces > Configuration. Choisissez l'interface Ethernet à configurer. 2. Cliquez sur l'icône  pour ouvrir la fenêtre Configure VLAN Router Interface.	Port	Name	Port on	Port status	IP address	Network	Routing	Proxy ARP	MTU value	ICMP unreachable	ICMP redirects	☐	1/1	GE	up	192.168.30.254	255.255.0.0	GE	☐	1,500	GE	GE	☐	1/2	GE	up	139.160.236.254	255.255.0.0	GE	☐	1,500	GE	GE	☐	1/3	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE	☐	1/4	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE	☐	1/5	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE	☐	1/6	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE	☐	1/7	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE
Port	Name	Port on	Port status	IP address	Network	Routing	Proxy ARP	MTU value	ICMP unreachable	ICMP redirects																																																																															
☐	1/1	GE	up	192.168.30.254	255.255.0.0	GE	☐	1,500	GE	GE																																																																															
☐	1/2	GE	up	139.160.236.254	255.255.0.0	GE	☐	1,500	GE	GE																																																																															
☐	1/3	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE																																																																															
☐	1/4	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE																																																																															
☐	1/5	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE																																																																															
☐	1/6	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE																																																																															
☐	1/7	GE	down	0.0.0.0	0.0.0.0	☐	☐	1,500	GE	GE																																																																															
2	Définissez l'ID sur le VLAN que vous souhaitez configurer (1 dans l'exemple), puis cliquez sur Next. Configure VLAN router interface 1. Create or select VLAN 2. Setup VLAN 3. Setup virtual router port ☐ VLAN ID Name ☐ 1 default Put 1 for example: VLAN ID 1 Then click Next Back Next Finish Cancel																																																																																								

Etape	Action																																				
3	Définissez un nom de route sur le VLAN que vous souhaitez configurer (RouteName dans l'exemple), puis cliquez sur Next. Configure VLAN router interface 1. Create or select VLAN VLAN ID2 2. Setup VLAN NameRouteName 3. Setup virtual router port <table><thead><tr><th>Port</th><th>Member</th><th>Untagged</th><th>Port-VLAN ID</th></tr></thead><tbody><tr><td>1/1</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/2</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/3</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/4</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/5</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/6</td><td>☐</td><td>☐</td><td>1</td></tr><tr><td>1/7</td><td>☐</td><td>☐</td><td>1</td></tr></tbody></table> Click Next Back Next Finish Cancel <tr><td>4</td><td> Définissez l'adresse IP du réseau de contrôle et son masque (192.168.30.254/16 dans l'exemple), puis cliquez sur Finish. Configure VLAN router interface 1. Create or select VLAN Primary address Address192.168.30.254 Netmask255.255.0.0 2. Setup VLAN 3. Setup virtual router port Secondary addresses ☒ AddressNetmask Address: Netmask: AddRemove Once you have set the address and mask, click Finish Repeat those steps for the second port Back Next Finish Cancel <tr><td>5</td><td>Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.</td></tr></td></tr>	Port	Member	Untagged	Port-VLAN ID	1/1	☐	☐	1	1/2	☐	☐	1	1/3	☐	☐	1	1/4	☐	☐	1	1/5	☐	☐	1	1/6	☐	☐	1	1/7	☐	☐	1	4	Définissez l'adresse IP du réseau de contrôle et son masque (192.168.30.254/16 dans l'exemple), puis cliquez sur Finish. Configure VLAN router interface 1. Create or select VLAN Primary address Address192.168.30.254 Netmask255.255.0.0 2. Setup VLAN 3. Setup virtual router port Secondary addresses ☒ AddressNetmask Address: Netmask: AddRemove Once you have set the address and mask, click Finish Repeat those steps for the second port Back Next Finish Cancel <tr><td>5</td><td>Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.</td></tr>	5	Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.
Port	Member	Untagged	Port-VLAN ID																																		
1/1	☐	☐	1																																		
1/2	☐	☐	1																																		
1/3	☐	☐	1																																		
1/4	☐	☐	1																																		
1/5	☐	☐	1																																		
1/6	☐	☐	1																																		
1/7	☐	☐	1																																		
4	Définissez l'adresse IP du réseau de contrôle et son masque (192.168.30.254/16 dans l'exemple), puis cliquez sur Finish. Configure VLAN router interface 1. Create or select VLAN Primary address Address192.168.30.254 Netmask255.255.0.0 2. Setup VLAN 3. Setup virtual router port Secondary addresses ☒ AddressNetmask Address: Netmask: AddRemove Once you have set the address and mask, click Finish Repeat those steps for the second port Back Next Finish Cancel <tr><td>5</td><td>Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.</td></tr>	5	Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.																																		
5	Répétez les étapes 1 à 4 pour le réseau machine à l'aide de la deuxième interface Ethernet.																																				

Dans l'exemple ci-dessous, l'interface de passerelle du réseau du pare-feu est 192.168.30.254/16 sur le premier port physique et le réseau machine est 139.160.235.254/16 sur le deuxième port physique.

☐	Port	Name	Port on	Port status	IP address	Netmask	Routing	Proxy ARP	MTU value	ICMP unreachable	ICMP redirects
☐	1/1		☒	up	192.168.30.254	255.255.0.0	☒	☐	1,500	☒	☒
☐	1/2		☒	up	139.160.235.254	255.255.0.0	☒	☐	1,500	☒	☒
☐	1/3		☒	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☒	☒
☐	1/4		☒	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☒	☒
☐	1/5		☒	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☒	☒
☐	1/6		☒	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☒	☒
☐	1/7		☒	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☒	☒

Configuration du VPN dans le pare-feu

Pour configurer le VPN, procédez comme suit :

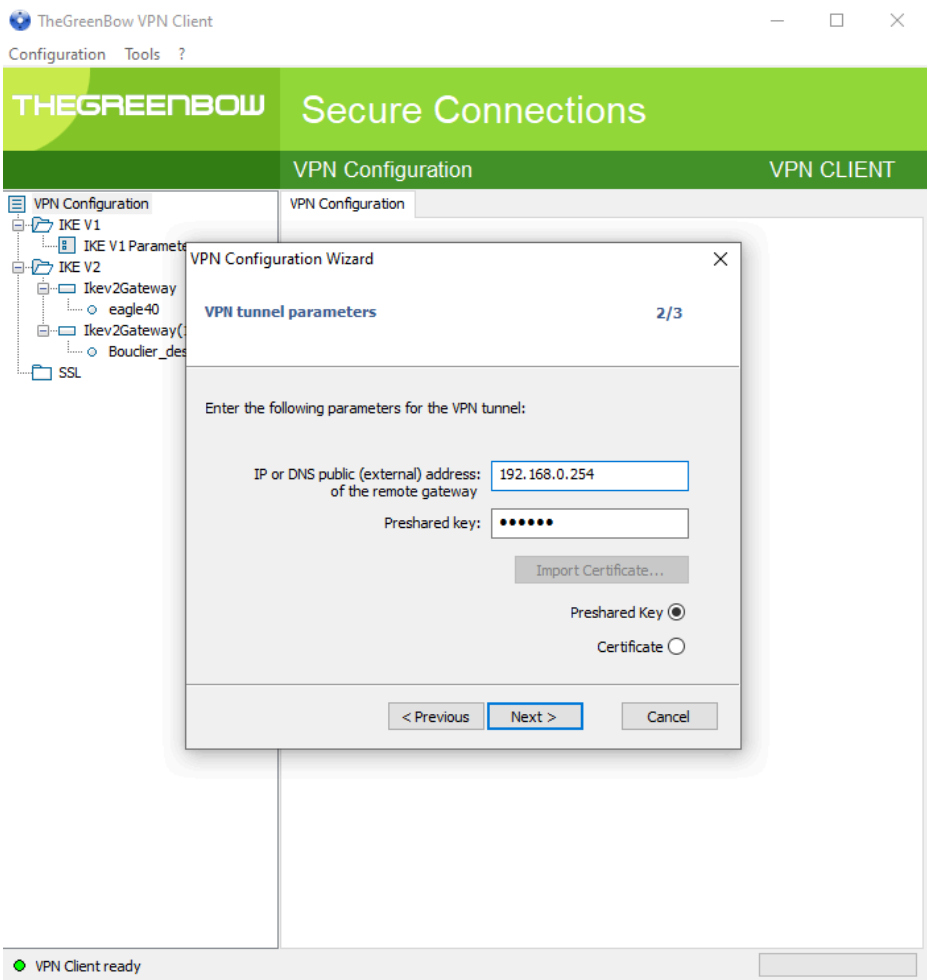
Etape	Action
1	Dans le volet gauche de la page Web, cliquez sur le menu Virtual Private Network > Connections . Cliquez sur l'icône  .
2	Choisissez un numéro d'index et un nom, puis cliquez sur Next .
3	Choisissez un mot de passe (PSK), puis cliquez sur Next .

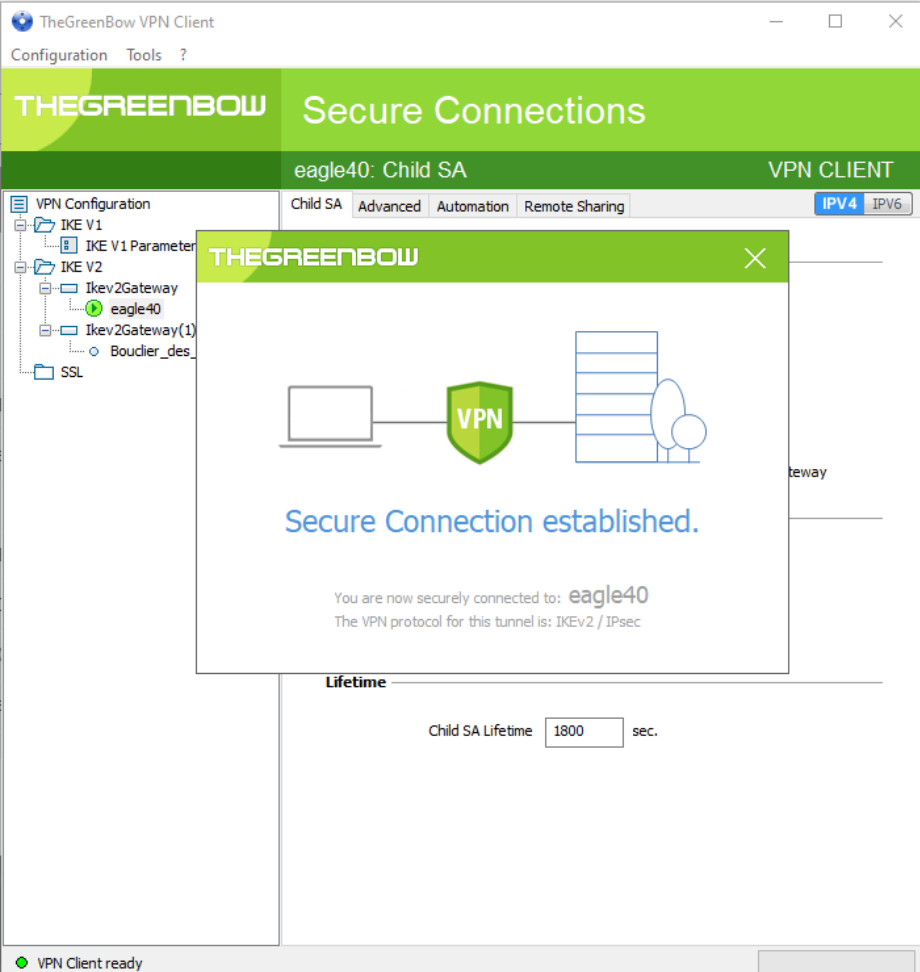
Etape	Action
4	Renseignez les adresses IP et les masques en fonction de votre réseau. • Remote endpoint : Ordinateur qui se connecte au pare-feu à l'aide d'un VPN. • Local endpoint : Passerelle configurée dans les Routes. • Source address (CIDR) : Réseau machine protégé, accessible qu'une fois connecté à l'aide d'un VPN. • Destination address (CIDR) : Ordinateur qui se connecte au pare-feu à l'aide d'un VPN. VPN configuration 1. Create or select entry 2. Authentication 3. Endpoint and traffic selectors 4. Advanced configuration Endpoints Remote endpoint192.168.1.60 Local endpoint192.168.30.254 Add traffic selector ☒ Traffic select... Traffic select... Source addr... Source restri... Destination a... Destination r... Traffic selector index: Traffic selector description: Source address (CIDR): 139.160.0.0/16 Source restrictions: Destination address (CIDR): 192.168.1.60/16 Destination restrictions: AddRemove Back Next Finish Cancel Cliquez sur Next.
5	Définissez un temps de marge. La valeur par défaut est 150. Sélectionnez ikev2 dans IKE Version, puis cliquez sur Finish.

Configuration du client VPN

NOTE: Dans notre exemple, nous utilisons la solution de client VPN fournie par TheGreenBow.

Pour configurer le client VPN, procédez comme suit :

Etape	Action
1	Téléchargez et installez le logiciel client VPN.
2	Dans le volet gauche de la fenêtre du client VPN, cliquez avec le bouton droit sur VPN Configuration et choisissez Wizard .
3	Sélectionnez IKEv2 Tunnel et cliquez sur Next .
4	Définissez l'adresse IP du pare-feu accessible via l'interface du réseau de contrôle (192.168.0.254 dans l'exemple). Saisissez le PSK sélectionné précédemment.  Cliquez sur Next, puis sur Finish.

Etape	Action
5	Dans le volet gauche de la fenêtre du client VPN, cliquez avec le bouton droit sur le tunnel Ikev2 que vous venez de créer et renommez-le.
6	Cliquez avec le bouton droit sur le tunnel Ikev2 que vous devez de renommer et sélectionnez Open Tunnel. Une notification confirme que la connexion sécurisée a été établie.  The screenshot displays the 'TheGreenBow VPN Client' window. The main title bar reads 'TheGreenBow Secure Connections'. Below this, a green header bar contains 'THEGREENBOW' and 'Secure Connections'. The interface is divided into two main sections. On the left, a 'VPN Configuration' tree shows a hierarchy: 'VPN Configuration' > 'IKE V1' > 'IKE V1 Parameter' > 'IKE V2' > 'Ikev2Gateway' > 'eagle40'. The 'eagle40' item is highlighted with a green circle. On the right, the 'Child SA' tab is active, showing 'Advanced' settings. A large, semi-transparent dialog box is overlaid on the right side of the window. It features a green header with 'THEGREENBOW' and a close button. The dialog contains a diagram of a laptop connected to a server via a green shield labeled 'VPN'. Below the diagram, the text reads 'Secure Connection established.' and 'You are now securely connected to: eagle40'. At the bottom of the dialog, it states 'The VPN protocol for this tunnel is: IKEv2 / IPsec'. Below the dialog, the 'Lifetime' section shows 'Child SA Lifetime' set to '1800' seconds. At the bottom of the main window, a status bar indicates 'VPN Client ready' with a green circle icon.

Glossaire

802.1Q:

Désignation de protocole IEEE pour réseau local virtuel (VLAN). Cette norme fournit l'identification du VLAN et les niveaux de qualité de service (QoS).

A

Adaptateur :

L'adaptateur est la cible des requêtes de connexion des données d'E/S en temps réel émises par les scrutateurs. Il ne peut ni envoyer ni recevoir des données d'E/S en temps réel, sauf si un scrutateur l'exige. Il ne conserve, ni ne génère les paramètres de communication des données nécessaires pour établir la connexion. L'adaptateur accepte des requêtes de messages explicites (connectés et non connectés) des autres équipements.

anneau principal:

L'anneau principal d'un réseau RIO Ethernet comprend des modules d'E/S distantes (RIO) et un rack local (contenant un contrôleur avec un service de scrutation d'E/S Ethernet) ainsi qu'un module d'alimentation.

Architecture:

Une architecture décrit une structure permettant de définir un réseau constitué des composants suivants :

- Composants physiques, leur organisation fonctionnelle et leur configuration
- Principes de fonctionnement et procédures
- Formats de données utilisés pour le fonctionnement

ARRAY:

Un ARRAY est un tableau d'éléments de même type. La syntaxe est la suivante : ARRAY [<limites>] OF <Type>

Exemple : ARRAY [1..2] OF BOOL est un tableau à une dimension, composé de deux éléments de type BOOL.

ARRAY [1..10, 1..20] OF INT est un tableau à deux dimensions composé de 10x20 éléments de type INT.

ART:

Acronyme de *application response time* (temps de réaction de l'application). Délai de réaction d'une application de contrôleur à une entrée donnée. L'ART est mesuré depuis l'activation dans le contrôleur d'un signal physique qui déclenche une commande d'écriture jusqu'à l'activation de la sortie distante signalant la réception des données.

AUX:

Une tâche (AUX) est une tâche processeur périodique et facultative qui est exécutée via son logiciel de programmation. La tâche AUX est utilisée pour exécuter une partie de l'application dont le niveau de priorité est faible. Elle n'est exécutée que si les tâches MAST et FAST n'ont rien à accomplir. La tâche MAST comprend deux parties :

- IN : les entrées sont copiées dans la section IN avant l'exécution de la tâche AUX.
- OUT : les sorties sont copiées dans la section OUT après exécution de la tâche AUX.

B**BCD:**

Acronyme de *binary-coded decimal* (décimaux codés en binaire)

BOOL:

Le type *booléen* est le type de données de base en informatique. Une variable de type `BOOL` peut avoir l'une des deux valeurs suivantes : 0 (`FALSE`) ou 1 (`TRUE`).

Un bit extrait d'un mot est de type `BOOL`, par exemple `%MW10 . 4`

BOOTP:

Acronyme de *protocole d'amorçage*. Protocole réseau UDP qu'un client réseau peut utiliser pour obtenir automatiquement une adresse IP à partir d'un serveur. Le client s'identifie auprès du serveur à l'aide de son adresse MAC. Le serveur, qui gère un tableau préconfiguré des adresses MAC des équipements clients et des adresses IP associées, envoie au client son adresse IP définie. Le service BOOTP utilise les ports UDP 67 et 68.

boucle de chaînage simple:

Souvent désignée par l'acronyme SDCL (simple daisy chain loop), une boucle de chaînage simple contient uniquement des modules RIO (pas d'équipements distribués). Cette topologie se compose d'un rack local (contenant un contrôleur avec service de scrutation d'E/S Ethernet) et d'une ou de plusieurs stations d'E/S distantes RIO (chacune contenant un module adaptateur RIO).

C

CCOTF:

Acronyme de *Change Configuration On The Fly* (modification de configuration à la volée). Fonction de Control Expert qui permet la modification du matériel dans la configuration système pendant l'exécution du système. Cette modification n'affecte pas les opérations actives.

CEI 61131-3:

Norme internationale : automates programmables

Partie 3: langages de programmation

Cible:

Dans EtherNet/IP, un équipement est considéré comme la cible lorsqu'il est le destinataire d'une requête de connexion pour des communications de messagerie implicite ou explicite, ou lorsqu'il est le destinataire d'une requête de message en messagerie explicite non connectée.

CIP™:

Acronyme de *Common Industrial Protocol* (protocole industriel commun). Suite complète de messages et de services pour l'ensemble des applications d'automatisation de fabrication (contrôle, sécurité, synchronisation, mouvement, configuration et informations). Le protocole CIP permet aux utilisateurs d'intégrer ces applications de fabrication dans les réseaux Ethernet de niveau entreprise et dans Internet. CIP est le principal protocole d'EtherNet/IP.

client de messagerie explicite:

(*classe de client de messagerie explicite*). Classe d'équipement définie par l'ODVA pour les nœuds EtherNet/IP qui ne prennent en charge la messagerie explicite qu'en tant que client. Les systèmes IHM et SCADA sont des exemples courants de cette classe d'équipements.

cloud DIO:

Groupe d'équipements distribués qui ne sont pas requis pour la prise en charge de RSTP. Les clouds DIO nécessitent uniquement une connexion simple en fil de cuivre (pas d'anneau). Ils peuvent être connectés à certains ports cuivre des commutateurs double anneau (DRS) ou directement au contrôleur ou aux modules de communication Ethernet du *rack local*. Il est **impossible** de connecter les clouds DIO à des *sous-anneaux*.

Commutateur:

Équipement multiport qui permet de segmenter le réseau et de réduire les risques de collisions. Les paquets sont filtrés ou transférés en fonction de leurs adresses source et cible. Les commutateurs peuvent fonctionner en duplex intégral et fournir la totalité de la bande passante à chaque port. Un commutateur peut présenter différentes vitesses d'entrée/sortie (par exemple, 10, 100 ou 1000 Mbits/s). Les commutateurs sont considérés comme des équipements de couche OSI 2 (couche de liaison des données).

connexion de classe 1:

Connexion de transport CIP de classe 1 utilisée pour transmettre des données d'E/S entre équipements EtherNet/IP par voie de messagerie implicite.

Connexion de classe 3:

Connexion de classe 3 de transport CIP utilisée pour la messagerie explicite entre équipements EtherNet/IP.

Connexion de rack optimisée:

Les données issues de plusieurs modules d'E/S sont regroupées en un paquet de données unique qui est présenté au scrutateur dans un message implicite sur un réseau EtherNet/IP.

Connexion:

Circuit virtuel entre plusieurs équipements de réseau, créé avant l'émission des données. Après l'établissement d'une connexion, une série de données est transmise par le même canal de communication, sans qu'il soit nécessaire d'inclure des informations de routage (notamment les adresses source et cible) avec chaque donnée.

convergence réseau:

Activité qui consiste à reconfigurer le réseau en cas de perte de réseau en vue de garantir la disponibilité du système.

CPU:

Acronyme de *central processing unit* (unité centrale de traitement ou UC). On parle également de processeur ou de contrôleur. La CPU est le cerveau d'un processus de fabrication industrielle. Il automatise le processus, par opposition aux systèmes de contrôle à relais. Les CPU sont des ordinateurs conçus pour résister aux conditions parfois difficiles d'un environnement industriel.

Créateur de la connexion:

Nœud réseau EtherNet/IP, qui génère une requête de connexion pour le transfert des données d'E/S ou la messagerie explicite.

D

DDT:

Acronyme de *derived data type*. Un type de données dérivé est un ensemble d'éléments de même type (`ARRAY`) ou de types différents (structure).

Déterminisme:

Pour une application et une architecture données, vous pouvez prévoir que le délai entre un événement (changement de valeur d'une entrée) et la modification correspondante de la sortie d'un contrôleur a une durée t définie, qui est inférieure au délai requis par votre processus.

Device DDT (DDDT):

Un DDT d'équipement est un DDT (type de données dérivé) prédéfini par le constructeur qui ne peut pas être modifié par l'utilisateur. Il contient les éléments de langage d'E/S d'un module d'E/S.

DFB:

Acronyme de *derived function block* (bloc fonction dérivé). Les types DFB sont des blocs fonction programmables par l'utilisateur en langage ST, IL, LD ou FBD.

L'utilisation de ces types DFB dans une application permet :

- de simplifier la conception et la saisie du programme,
- d'accroître la lisibilité du programme,
- de faciliter sa mise au point,
- de diminuer le volume de code généré.

DHCP:

Acronyme de *dynamic host configuration protocol* (protocole de configuration dynamique d'hôtes). Extension du protocole de communication BOOTP, qui permet d'affecter automatiquement les paramètres d'adressage IP, notamment l'adresse IP, le masque de sous-réseau, l'adresse IP de passerelle et les noms de serveur DNS. DHCP ne nécessite pas la gestion d'un tableau identifiant chaque équipement de réseau. Le client s'identifie auprès du serveur DHCP en utilisant son adresse MAC ou un identifiant d'équipement unique. Le service DHCP utilise les ports UDP 67 et 68.

Diffusion:

Message envoyé à tous les équipements d'un domaine de diffusion.

DIO:

(*E/S distribuées*) Egalement appelé équipement distribué. Les DRSs utilisent des ports DIO pour connecter des équipements distribués.

DNS:

Acronyme de *domain name server/service* (serveur/service de noms de domaine). Service capable de traduire un nom de domaine alphanumérique en adresse IP, l'identificateur unique d'un équipement sur un réseau.

DRS:

Acronyme de *dual-ring switch* (commutateur double anneau). Commutateur géré à extension ConneXium qui a été configuré pour fonctionner sur un réseau Ethernet. Des fichiers de configuration prédéfinis sont fournis par Schneider Electric pour téléchargement vers un DRS en vue de prendre en charge les fonctionnalités spéciales de l'architecture à anneau principal/sous-anneau.

DSCP:

Acronyme de *Differentiated Service Code Points* (point de code des services différenciés). Ce champ de 6 bits inclus dans l'en-tête d'un paquet IP sert à classifier le trafic aux fins d'établir les priorités.

DST:

Acronyme de *daylight saving time* (heure d'été). Pratique qui consiste à avancer les horloges vers le début du printemps et à les retarder vers le début de l'automne.

DT:

Acronyme de *date and time* (date et heure). Le type de données DT est codé en BCD sur 64 bits et contient les informations suivantes :

- l'année codée dans un champ de 16 bits
- le mois codé dans un champ de 8 bits
- le jour codé dans un champ de 8 bits
- l'heure codée dans un champ de 8 bits
- les minutes codées dans un champ de 8 bits
- les secondes codées dans un champ de 8 bits

NOTE: les huit bits de poids faible ne sont pas utilisés.

Le type DT est déclaré sous la forme suivante :

DT#<Année>-<Mois>-<Jour>-<Heure>:<Minutes>:<Secondes>

Le tableau ci-après donne les limites inférieure/supérieure de chaque élément :

Champ	Limites	Commentaire
Année	[1990,2099]	Année
Mois	[01,12]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.
Jour	[01,31]	Pour les mois 01/03/05/07/08/10/12
	[01,30]	Pour les mois 04/06/09/11
	[01,29]	Pour le mois 02 (années bissextiles)
	[01,28]	Pour le mois 02 (années non bissextiles)
Heure	[00,23]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.
Minute	[00,59]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.
Seconde	[00,59]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.

DTM:

Acronyme de *device type manager* DTM (gestionnaire de type d'équipement). Pilote d'équipement exécuté sur le PC hôte. Il offre une structure unifiée pour accéder aux paramètres de l'équipement, le configurer et l'utiliser, et pour remédier aux problèmes. Les DTM peuvent présenter différents visages, d'une simple interface graphique permettant de configurer les paramètres de l'équipement jusqu'à une application très perfectionnée susceptible d'effectuer des calculs complexes en temps réel à des fins de diagnostic et de maintenance. Dans le contexte d'un DTM, un équipement peut être un module de communication ou un équipement distant sur le réseau.

Voir FDT.

Duplex intégral:

Capacité de deux équipements en réseau à communiquer indépendamment et simultanément entre eux dans les deux sens.

E

EDS:

Acronyme de *electronic data sheet* (fiche de données électronique). Les EDS sont de simples fichiers texte qui décrivent les fonctions de configuration d'un équipement. Les fichiers EDS sont générés et gérés par le fabricant de l'équipement.

EFB:

Acronyme de *elementary function block* (bloc fonction élémentaire). Bloc utilisé dans un programme pour réaliser une fonction logique prédéfinie.

Les EFB possèdent des états et des paramètres internes. Même si les entrées sont identiques, les valeurs des sorties peuvent différer. Par exemple, un compteur possède une sortie qui indique que la valeur de présélection est atteinte. Cette sortie est mise à 1 lorsque la valeur du compteur est égale à la valeur de présélection.

EF:

Acronyme de *elementary function* (fonction élémentaire). Bloc utilisé dans un programme pour réaliser une fonction logique prédéfinie.

Une fonction ne dispose pas d'informations sur l'état interne. Plusieurs appels de la même fonction à l'aide des mêmes paramètres d'entrée fournissent toujours les mêmes valeurs de sortie. Vous trouverez des informations sur la forme graphique de l'appel de fonction dans le « *[bloc fonctionnel (instance)]* ». Contrairement aux appels de bloc fonction, les appels de fonction comportent uniquement une sortie qui n'est pas nommée et dont le nom est identique à celui de la fonction. En langage FBD, chaque appel est indiqué par un [numéro] unique via le bloc graphique. Ce numéro est généré automatiquement et ne peut pas être modifié.

Vous positionnez et configurez ces fonctions dans le programme afin d'exécuter l'application.

Vous pouvez également développer d'autres fonctions à l'aide du kit de développement SDKC.

EN:

EN correspond à **EN**able (activer) ; il s'agit d'une entrée de bloc facultative. Quand l'entrée EN est activée, une sortie ENO est automatiquement définie.

Si EN = 0, le bloc n'est pas activé, son programme interne n'est pas exécuté et ENO est réglé sur 0.

Si EN = 1, le programme interne du bloc est exécuté et ENO est réglé sur 1. Si une erreur d'exécution est détectée, ENO reprend la valeur 0.

Si l'entrée EN n'est pas connectée, elle est automatiquement réglée sur 1.

ENO:

ENO signifie **E**rror **NO**tification (notification d'erreur). C'est la sortie associée à l'entrée facultative EN.

Si ENO est réglé sur 0 (parce que EN = 0 ou qu'une erreur d'exécution est détectée) :

- L'état des sorties du bloc fonction reste le même que lors du précédent cycle de scrutation correctement exécuté.
- La ou les sorties de la fonction, ainsi que les procédures, sont réglées sur 0.

environnement difficile:

Résistance aux hydrocarbures, aux huiles industrielles, aux détergents et aux copeaux de brasure. Humidité relative pouvant atteindre 100 %, atmosphère saline, écarts de température importants, température de fonctionnement comprise entre -10 °C et +70 °C ou installations mobiles. Pour les équipements renforcés (H), l'humidité relative peut atteindre 95 % et la température de fonctionnement peut être comprise entre -25 °C et +70 °C.

équipement d'E/S Ethernet M580:

Équipement Ethernet qui assure la récupération automatique du réseau et des performances RIO déterministes. Le temps nécessaire à la résolution d'une scrutation logique des E/S distantes (RIO) peut être calculé, et le système peut être rétabli rapidement à la suite d'une rupture de la communication. Les équipements d'E/S Ethernet M580 comprennent :

- rack local (comprenant un contrôleur avec service de scrutation d'E/S Ethernet)
- station RIO (comprenant un module adaptateur X80)
- commutateur double anneau (DRS) avec une configuration prédéfinie

équipement de classe scrutateur:

Un équipement de classe scrutateur est défini par l'ODVA comme un nœud EtherNet/IP capable de déclencher des échanges d'E/S avec d'autres nœuds du réseau.

équipement distribué:

Tout équipement Ethernet (appareil Schneider Electric, PC, serveur ou autre équipement tiers) qui prend en charge l'échange avec un contrôleur ou un autre service scrutateur d'E/S Ethernet.

équipement prêt:

Équipement Ethernet prêt qui fournit des services supplémentaires au module Ethernet/IP ou Modbus, par exemple : entrée d'un paramètre, déclaration dans l'éditeur de bus, transfert système, scrutation déterministe, message d'alerte pour les modifications et droits d'accès utilisateur partagés entre Control Expert et le DTM d'équipement.

esclave local:

Fonctionnalité proposée par les modules de communication EtherNet/IP de Schneider Electric et qui autorise un scrutateur à assurer le rôle d'adaptateur. L'esclave local permet au module de publier des données en utilisant des connexions de messagerie implicite. La fonctionnalité d'esclave local s'utilise généralement pour les échanges d'égal à égal entre PAC.

EtherNet/IP™:

Protocole de communication réseau pour les applications d'automatisation industrielle, qui combine les protocoles de transmission TCP/IP et UDP et le protocole CIP de couche applicative pour prendre en charge l'échange de données à haut débit et la commande industrielle. EtherNet/IP emploie des fichiers EDS pour classer chaque équipement réseau et ses fonctionnalités.

Ethernet:

Réseau local à 10 Mbits/s, 100 Mbits/s ou 1 Gbits/s, CSMA/CD, utilisant des trames, qui peut fonctionner avec une paire torsadée de fils de cuivre, un câble en fibre optique ou sans fil. La norme IEEE 802.3 définit les règles de configuration des réseaux Ethernet filaires, tandis que la norme IEEE 802.11 définit les règles de configuration des réseaux Ethernet sans fil. Les réseaux 10BASE-T, 100BASE-TX et 1000BASE-T sont couramment utilisés. Ils peuvent employer des câbles en cuivre à paire torsadée de 5e catégorie et des prises modulaires RJ45.

F

FAST:

Tâche de processeur périodique facultative qui identifie les requêtes de scrutation de priorité élevée et qui est exécutée via un logiciel de programmation dédié. Vous pouvez utiliser une tâche FAST pour que la logique de modules d'E/S spécifiques soit résolue plusieurs fois par scrutation. La tâche FAST comprend deux parties :

- IN : les entrées sont copiées dans la section IN avant l'exécution de la tâche FAST.
- OUT : les sorties sont copiées dans la section OUT après exécution de la tâche FAST.

FBD:

Acronyme de *function block diagram* (langage à blocs fonction). Langage de programmation graphique IEC 61131-3 qui fonctionne comme un diagramme de flux. Chaque fonction ou bloc fonction du programme est représenté(e) sous cette forme graphique en ajoutant des blocs logiques simples (par exemple AND, OR). Pour chaque bloc, les entrées se situent à gauche et les sorties à droite. Les sorties des blocs peuvent être liées aux entrées d'autres blocs afin de former des expressions complexes.

FDR:

Acronyme de *fast device replacement* (remplacement rapide d'équipement). Service utilisant le logiciel de configuration pour remplacer un produit défaillant.

FDT:

(Acronyme de « *field device tool* » outil d'équipement de terrain). Technologie harmonisant la communication entre les équipements de terrain et l'hôte système.

FTP:

Acronyme de *file transfer protocol* (protocole de transfert de fichiers). Protocole qui copie un fichier d'un hôte vers un autre sur un réseau TCP/IP, comme Internet. Le protocole FTP utilise une architecture client-serveur ainsi qu'une commande et des connexions de données distinctes entre le client et le serveur.

G

GPS:

Acronyme de *Global Positioning System*. Le système GPS standard se compose de signaux de positionnement, de navigation et d'horodatage dans l'espace diffusés dans le monde entier et destinés à une utilisation militaire comme civile. Les performances des services de positionnement standard dépendent des paramètres des signaux de diffusion des satellites, de la conception de la constellation GPS, du nombre de satellites en vue et de divers paramètres environnementaux.

H

HART:

Acronyme de *Highway Addressable Remote Transducer* (transducteur distant adressable par bus). Protocole de communication bidirectionnel pour l'envoi et la réception d'informations numériques sur des câbles analogiques entre un système de contrôle ou de surveillance et des équipements intelligents.

HART est la norme de référence pour l'accès aux données entre des systèmes hôtes et des instruments de terrain intelligents. Un hôte peut être une application logicielle lancée à partir de l'ordinateur portable ou du terminal portatif d'un technicien et qui s'exécute sur le système de contrôle de processus ou de gestion d'actifs d'un site industriel ou un autre système utilisant un système de contrôle quelconque.

horodatage applicatif:

Utilisez la solution d'horodatage applicatif pour accéder aux tampons d'événements d'horodatage avec un système SCADA qui ne prend pas en charge l'interface OPC DA. Dans ce cas, les blocs fonction de l'application Control Expert lisent les événements en mémoire tampon et les formatent pour les envoyer au système SCADA.

HTTP:

Acronyme de *hypertext transfer protocol* (protocole de transfert hypertexte). Le protocole HTTP constitue la base de la communication des données pour le Web.

I

I/O Scanning:

Service Ethernet qui interroge continuellement les modules d'E/S pour collecter des données et des informations d'état, d'événement et de diagnostic. Ce processus permet de surveiller les entrées et les sorties. Ce service prend en charge la scrutation logique des E/S distantes (RIO) comme distribuées (DIO).

%I:

Selon la norme CEI, %I indique un objet langage de type entrée TOR.

IGMP:

Acronyme d'*Internet Group Management Protocol* (protocole de gestion de groupe Internet). Cette norme Internet de multidiffusion permet à un hôte de s'abonner à un groupe de multidiffusion spécifique.

IHM:

Acronyme de *interface homme-machine*. Système qui permet l'interaction entre un humain et une machine.

IL:

Acronyme de *Instruction List* (liste d'instructions). Langage de programmation IEC 61131-3 contenant une série d'instructions de base. Il est très proche du langage d'assemblage utilisé pour programmer les processeurs. Chaque instruction est composée d'un code instruction et d'un opérande.

INT:

Type de données *INteger* (entier) (codé sur 16 bits). Les limites inférieure et supérieure sont : $-(2 \text{ puissance } 15)$ à $(2 \text{ puissance } 15) - 1$.

Exemple : -32768, 32767, 2#1111110001001001, 16#9FA4.

IODDT:

(*input/output derived data type*) Type de données dérivé d'E/S. Type de données structuré représentant un module ou une voie d'un contrôleur. Chaque module expert possède ses propres IODDT.

IPsec:

Acronyme d'*Internet Protocol Security* (sécurité du protocole Internet). Ensemble de normes de protocole ouvertes qui permettent de privatiser et de chiffrer les sessions de communication IP pour le trafic entre les modules utilisant IPsec, développées par l'Internet Engineering Task Force (IETF). Les algorithmes d'authentification et de chiffrement IPsec requièrent des clés cryptographiques définies par l'utilisateur qui traitent chaque paquet de communication dans une session IPsec.

%IW:

Selon la norme CEI, %IW indique un objet langage de type entrée analogique.

L**Langage en blocs fonctionnels:**

Voir FBD.

LD:

Acronyme de *Ladder Diagram* (schéma à contacts)). Langage de programmation IEC 61131-3 qui représente les instructions à exécuter sous forme de schémas graphiques assez semblables à un schéma électrique (contacts, bobines, etc.).

M

Masque de sous-réseau:

Valeur de 32 bits utilisée pour cacher (ou masquer) la portion réseau de l'adresse IP et ainsi révéler l'adresse d'hôte d'un équipement sur un réseau utilisant le protocole IP.

MAST:

Une tâche maître (MAST) est une tâche de processeur déterministe qui est exécutée par le biais du logiciel de programmation. La tâche MAST planifie la logique de module RIO à résoudre lors de chaque scrutation d'E/S. La tâche MAST comprend deux parties :

- IN : les entrées sont copiées dans la section IN avant l'exécution de la tâche MAST.
- OUT : les sorties sont copiées dans la section OUT après l'exécution de la tâche MAST.

MB/TCP:

Abréviation de *Modbus over TCP protocol*. Variante du protocole Modbus utilisée pour les communications réalisées sur les réseaux TCP/IP.

Messagerie connectée:

Dans EtherNet/IP, la messagerie connectée utilise une connexion CIP pour la communication. Un message connecté est une relation logique entre au moins deux objets d'application sur des nœuds différents. La connexion établit à l'avance un circuit virtuel dans un but particulier, par exemple l'envoi de messages explicites fréquents ou transferts de données d'E/S en temps réel.

messagerie explicite,:

Messagerie TCP/IP pour Modbus TCP et EtherNet/IP. Elle est utilisée pour les messages client/serveur point à point contenant des données (généralement des informations non programmées entre un client et un serveur) et des informations de routage. Dans EtherNet/IP, la messagerie explicite est considérée comme une messagerie de classe 3 et peut fonctionner avec ou sans connexion.

messagerie implicite:

Messagerie connectée de classe 1 basée sur le protocole UDP/IP pour EtherNet/IP. La messagerie implicite gère une connexion ouverte pour le transfert programmé de données de contrôle entre un producteur et un consommateur. Comme une connexion est maintenue ouverte, chaque message contient principalement des données (sans la surcharge des informations sur les objets) plus un identificateur de connexion.

MIB:

Acronyme de *management information base* (base d'informations de gestion). Voir SNMP.

%M:

Selon la norme CEI, %M indique un objet langage de type bit mémoire.

Modbus:

Modbus est un protocole de message de couche application. Modbus assure les communications client et serveur entre des équipements connectés via différents types de bus ou de réseaux. Modbus offre plusieurs services indiqués par des codes de fonction.

Mode étendu:

Dans Control Expert, le mode étendu affiche des propriétés de configuration de niveau expert pour la définition de connexions Ethernet. Etant donné que ces propriétés ne doivent être modifiées que par des personnes ayant une compréhension solide des protocoles de communication EtherNet/IP, elles peuvent être masquées ou affichées selon la qualification de l'utilisateur.

Multidiffusion:

Type de diffusion dans lequel des copies du paquet sont remises uniquement à un sous-ensemble de destinations réseau. La messagerie implicite utilise généralement le format de multidiffusion pour les communications dans un réseau EtherNet/IP.

%MW:

Selon la norme CEI, %MW indique un objet langage de type mot mémoire.

N**NIM:**

Acronyme de *network interface module* (module d'interface réseau). Un NIM se trouve toujours en première position de l'îlot STB (position la plus à gauche sur l'îlot physiquement installé). Le NIM possède une interface entre les modules d'E/S et le maître Fieldbus. C'est le seul module de l'îlot dépendant du bus de terrain (un NIM différent est disponible pour chaque bus de terrain).

nom de domaine:

Chaîne alphanumérique qui identifie un équipement sur Internet et qui apparaît comme composant principal d'une adresse URL (Uniform Resource Locator) d'un site Web. Par exemple, le nom de domaine *schneider-electric.com* est le composant principal de l'URL *www.se.com*.

Chaque nom de domaine est attribué en tant que partie du système de noms de domaine, et il est associé à une adresse IP.

Egalement appelé nom d'hôte.

Nom de l'adresse :

Identificateur de 32 bits, constitué d'une adresse réseau et d'une adresse d'hôte, affecté à un équipement connecté à un réseau TCP/IP.

NTP:

Acronyme de *network time protocol* (protocole de temps réseau). Le protocole utilise un tampon de gigue pour résister aux effets de latence variable.

O

O -> T:

Originator to Target (source vers cible). Voir source et cible.

ODVA:

(*Open DeviceNet Vendors Association*) L'ODVA prend en charge des technologies de réseau basées sur CIP.

OFS:

Acronyme de *OPC Factory Server*. OFS permet les communications SCADA en temps réel avec la famille d'automates Control Expert. OFS utilise le protocole d'accès aux données OPC standard.

OPC DA:

Acronyme de *OLE for Process Control Data Access*. La spécification d'accès aux données est la norme OPC la plus fréquemment mise en œuvre. Elle fournit des spécifications pour la communication des données en temps réel entre les clients et les serveurs.

P

PAC:

Acronyme de *Programmable Automation Controller* (contrôleur d'automatisation programmable). L'automate PAC est le cerveau d'un processus de fabrication industriel. Il automatise le processus, par opposition aux systèmes de contrôle à relais. Les PAC sont des ordinateurs conçus pour résister aux conditions parfois difficiles d'un environnement industriel.

Passerelle :

Une passerelle relie deux réseaux, parfois à l'aide de différents protocoles réseau. Lorsqu'elle connecte des réseaux utilisant différents protocoles, la passerelle convertit un datagramme d'une pile de protocole dans l'autre. Lorsqu'elle connecte deux réseaux IP, la passerelle (également appelée routeur) dispose de deux adresses IP distinctes (une sur chaque réseau).

Port 502:

Le port 502 de la pile TCP/IP est le port bien connu qui est réservé aux communications Modbus TCP.

port de service:

Port Ethernet dédié sur les modules RIO M580. Ce port peut prendre en charge les fonctions essentielles suivantes (en fonction du type de module) :

- réplication de port : aux fins de diagnostic
- accès : pour connexion de HMI/Control Expert/ConneXview au contrôleur
- étendu : pour étendre le réseau d'équipements à un autre sous-réseau
- désactivé : désactive le port ; aucun trafic n'est transmis dans ce mode

PTP:

Acronyme de *Precision Time Protocol*. Utilisez ce protocole pour synchroniser toutes les horloges d'un réseau informatique. Sur un réseau local, le protocole PTP assure la précision des horloges à la microseconde près, ce qui permet de les utiliser pour les systèmes de mesure et de contrôle.

Q**%Q:**

Selon la norme CEI, %Q indique un objet langage de type sortie TOR.

QoS:

Acronyme de « *quality of service* » (qualité de service). Dans un réseau industriel, la qualité de service permet d'établir un niveau prévisible de performances du réseau.

%QW:

Selon la norme CEI, %QW indique un objet langage de type sortie analogique.

R

rack local:

Rack M580 contenant le contrôleur et une alimentation. Un rack local se compose d'un ou de deux racks : le rack principal et un rack étendu appartenant à la même famille que le rack principal. Le rack étendu est facultatif.

Redondance d'UC:

Un système de redondance d'UC (Hot Standby) comprend un PAC primaire et un PAC redondant. Les configurations matérielle et logicielle sont identiques pour les deux racks de PAC. Le PAC redondant surveille l'état actuel du système du PAC primaire. Lorsque celui-ci n'est plus opérationnel, un contrôle de haute disponibilité est assuré tandis que le PAC redondant prend la main sur le système.

Réplication de port:

Dans ce mode, le trafic de données lié au port source d'un commutateur réseau est copié sur un autre port de destination. Cela permet à un outil de gestion connecté de contrôler et d'analyser le trafic.

réseau d'équipements:

Réseau Ethernet au sein d'un réseau d'E/S, qui contient des équipements d'E/S distantes et des équipements d'E/S distribués. Les équipements connectés à ce réseau suivent des règles spécifiques pour permettre le déterminisme des E/S distantes.

réseau d'exploitation:

Réseau Ethernet contenant des outils d'exploitation (SCADA, PC client, imprimantes, outils de traitement par lots et EMS, entre autres). Les contrôleurs sont reliés directement ou par routage du réseau inter-contrôleurs. Ce réseau fait partie du réseau de contrôle.

réseau de contrôle:

Réseau Ethernet contenant des PAC, des systèmes SCADA, un serveur NTP, des PC, des AMS et des commutateurs (entre autres). Deux types de topologie sont pris en charge :

- Plate : Tous les modules et équipements de ce réseau appartiennent au même sous-réseau.
- A 2 niveaux : Le réseau est divisé en un réseau d'exploitation et un réseau intercontrôleur. Ces deux réseaux peuvent être indépendants physiquement, mais ils sont généralement reliés par un dispositif de routage.

Réseau DIO isolé:

Réseau Ethernet contenant des équipements distribués qui ne font pas partie d'un réseau RIO

réseau DIO:

Abréviation de Distributed IO (E/S distribuées). Réseau contenant des équipements distribués dans lequel la scrutation des E/S est effectuée par un contrôleur avec un service de scrutation DIO situé sur le rack local. Le trafic du réseau DIO est livré après le trafic RIO, ce dernier étant prioritaire dans un réseau RIO.

réseau EIO:

Abréviation de *Ethernet I/O* (E/S Ethernet). Réseau Ethernet qui contient trois types d'équipements :

- rack local
- Station distante X80 (avec un module adaptateur BM•CRA312•0) ou module de sélection d'options de réseau BMENOS0300
- Commutateur double anneau (DRS) étendu ConneXium

NOTE: Un équipement distribué peut également faire partie d'un réseau d'E/S Ethernet via une connexion à des DRSs ou au port de service de modules X80 distants.

Réseau intercontrôleurs:

Réseau Ethernet qui fait partie du réseau de contrôle et permet l'échange de données entre les contrôleurs et les outils d'ingénierie (programmation, système de gestion des actifs).

réseau RIO:

Abréviation de Remote I/O (E/S distantes). Réseau Ethernet contenant 3 types d'équipements RIO : un rack local, une station RIO et un commutateur double anneau (DRS) étendu ConneXium. Un équipement distribué peut également faire partie d'un réseau RIO via une connexion à des DRSs ou des modules de sélection d'options réseau BMENOS0300.

Réseau:

On distingue deux significations :

- Dans un schéma à contacts :

un réseau est un ensemble d'éléments graphiques interconnectés. La portée d'un réseau est locale, par rapport à l'unité (la section) organisationnelle du programme dans laquelle le réseau est situé.

- Avec des modules de communication experts :

Un réseau est un groupe de stations qui communiquent entre elles. Le terme *réseau* est également utilisé pour désigner un groupe d'éléments graphiques interconnectés. Ce groupe constitue ensuite une partie d'un programme qui peut être composée d'un groupe de réseaux.

RIO S908:

Système d'E/S distantes (RIO) Quantum utilisant des câbles coaxiaux et des terminaisons.

RPI:

Acronyme de *requested packet interval* (intervalle de paquet demandé). Période entre les transmissions de données cycliques demandées par le scrutateur. Les équipements EtherNet/IP publient des données selon l'intervalle spécifié par le RPI que le scrutateur leur a affecté et reçoivent des requêtes de message du scrutateur à chaque RPI.

RSTP:

Acronyme de *rapid spanning tree protocol*. Ce protocole permet à une conception de réseau d'inclure des liens supplémentaires (redondants) qui fournissent des chemins de sauvegarde automatique quand un lien actif échoue, sans avoir à recourir aux boucles ni à activer ou à désactiver les liens de sauvegarde manuellement.

S

Sans connexion:

Décrit une communication entre deux équipements de réseau, grâce à laquelle les données sont envoyées sans disposition préalable entre les équipements. Chaque donnée transmise contient des informations de routage, notamment les adresses source et cible.

SCADA:

Acronyme de *Supervisory Control And Data Acquisition*. Les systèmes SCADA sont des systèmes informatiques qui gèrent et surveillent les processus industriels ou les processus liés à l'infrastructure ou à l'installation (par exemple : transmission d'électricité, transport de gaz et de pétrole via des conduites, distribution d'eau, etc.).

Scrutateur:

Un scrutateur agit comme une source de requêtes de connexion d'E/S pour la messagerie implicite dans EtherNet/IP et de demandes de message pour Modbus TCP.

Service de scrutation d'E/S Ethernet:

Service de scrutation Ethernet intégré aux contrôleurs M580 qui gère les équipements distribués **et** les stations RIO dans un réseau d'équipements M580.

service de scrutation DIO Ethernet:

Le service de scrutation DIO intégré aux contrôleurs M580 gère les équipements distribués d'un réseau d'équipements M580.

service de temps réseau:

Ce service synchronise les horloges système des ordinateurs sur Internet pour enregistrer les événements (séquence d'événements), les synchroniser (déclenchement d'événements simultanés) ou synchroniser les alarmes et les E/S (alarmes d'horodatage).

SFC:

Acronyme de *Sequential Function Chart* (diagramme fonctionnel en séquence). Langage de programmation IEC 61131-3 utilisé pour représenter graphiquement et de manière structurée le fonctionnement d'un contrôleur séquentiel. Cette description graphique du fonctionnement séquentiel du contrôleur et des différentes situations qui en découlent s'effectue à l'aide de symboles graphiques simples.

SFP:

Acronyme de *Small Form-factor Pluggable*. L'émetteur-récepteur SFP joue le rôle d'interface entre un module et des câbles à fibre optique.

SMTP:

Acronyme de *simple mail transfer protocol* (protocole de transfert de courrier simple). Service de notification par messagerie électronique qui permet l'envoi d'alarmes ou d'événements sur les projets utilisant un contrôleur. Le contrôleur surveille le système et peut créer automatiquement un message électronique d'alerte contenant des données, des alarmes et/ou des événements. Les destinataires du message électronique peuvent se trouver sur le réseau local ou à distance.

SNMP:

Acronyme de *simple network management protocol* (protocole de gestion de réseau simple). Protocole utilisé dans les systèmes de gestion de réseau pour surveiller les équipements rattachés au réseau. Ce protocole fait partie de la suite de protocoles Internet (IP) définie par le groupe de travail d'ingénierie Internet (IETF), qui inclut des directives de gestion de réseau, dont un protocole de couche d'application, un schéma de base de données et un ensemble d'objets de données.

SNTP:

Acronyme de *simple network time protocol* (protocole de temps réseau simple). Voir NTP.

SOE:

Acronyme de *sequence of events* (séquence d'événements). Le logiciel SOE permet aux utilisateurs de comprendre une chaîne d'occurrences qui risque d'entraîner des conditions d'insécurité des processus et éventuellement des arrêts. Les SOE peuvent être essentiels pour résoudre ou prévenir de telles conditions.

Source:

Dans EtherNet/IP, un équipement est considéré comme la source lorsqu'il est à l'origine d'une connexion CIP pour la communication de messagerie implicite ou explicite, ou lorsqu'il génère une requête de message pour la messagerie explicite non connectée.

sous-anneau / anneau secondaire:

Réseau Ethernet comportant une boucle reliée à l'anneau principal à l'aide d'un commutateur double anneau (DRS) ou d'un module de sélection d'options de réseau BMENOS0300 situé sur l'anneau principal. Ce réseau contient des équipements RIO ou distribués.

Station d'E/S distante (RIO):

Un des trois types de modules RIO dans un réseau EthernetRIO. Une station d'E/S distantes (RIO) est un rack M580 de modules d'E/S qui sont connectés à un réseau RIO Ethernet et gérés par un module adaptateur distant RIO Ethernet. Une station peut se présenter sous la forme d'un rack unique ou d'un rack principal associé à un rack d'extension.

ST:

Acronyme de *Structured Text* (texte structuré). Langage de programmation IEC 61131-3 élaboré de type langage littéral structuré, qui est proche des langages de programmation informatique. Il permet de structurer des suites d'instructions.

%SW:

Selon la norme CEI, %SW indique un objet langage de type mot système.

T**T->O:**

Target to Originator (cible vers source). Voir cible et source.

TCP/IP:

Egalement connu sous le nom de *suite de protocoles Internet*, le protocole TCP/IP est un ensemble de protocoles utilisés pour conduire les transactions sur un réseau. La suite tire son nom de deux protocoles couramment utilisés : TCP et IP. TCP/IP est un protocole orienté connexion utilisé par Modbus TCP et EtherNet/IP pour la messagerie explicite.

TCP:

Acronyme de *transmission control protocol* (protocole de contrôle de transmission). Protocole clé de la suite de protocole Internet, qui prend en charge les communications orientées connexion en établissant la connexion nécessaire pour transmettre une séquence ordonnée de données sur le même canal de communication.

TFTP:

Acronyme de *Trivial File Transfer Protocol*. Version simplifiée du protocole *file transfer protocol* (FTP), TFTP utilise une architecture client-serveur pour établir des connexions entre deux équipements. A partir d'un client TFTP, il est possible d'envoyer des fichiers au serveur ou de les télécharger en utilisant le protocole UDP (user datagram protocol) pour le transport des données.

TIME_OF_DAY:

Voir `TOD`.

TOD:

Le type `TOD` (acronyme de « *time of day* »), codé en BCD dans un format sur 32 bits, contient les informations suivantes :

- l'heure codée dans un champ de 8 bits
- les minutes codées dans un champ de 8 bits
- les secondes codées dans un champ de 8 bits

NOTE: les huit bits de poids faible ne sont pas utilisés.

Le type `TOD` est saisi au format suivant : `xxxxxxx: TOD#<Heure>:<Minutes>:<Secondes>`

Le tableau ci-après donne les limites inférieure/supérieure de chaque élément :

Champ	Limites	Commentaire
Heure	[00,23]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.
Minute	[00,59]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.
Seconde	[00,59]	Le 0 initial est toujours affiché ; il peut être omis lors de la saisie.

Exemple : `TOD#23:59:45`.

Trap (déroutement):

Un déroutement est un événement dirigé par un agent SNMP qui indique l'un des événements suivants :

- L'état d'un agent a changé.
- Un équipement gestionnaire SNMP non autorisé a tenté d'obtenir (ou de modifier) des données d'un agent SMTP.

TR:

(*transparent ready*) équipement de distribution d'alimentation Web, incluant un appareil de voie moyenne tension et basse tension, des standards, des panneaux, des centres de commande du moteur et des sous-stations d'unité. Les équipements Transparent Ready permettent d'accéder aux compteurs et à l'état des équipements à partir de tout PC du réseau au moyen d'un navigateur Web classique.

U

UDP:

Acronyme de *User Datagram Protocol* (protocole datagramme utilisateur). Protocole de la couche de transport qui prend en charge les communications sans connexion. Les applications fonctionnant sur des nœuds en réseau peuvent utiliser le protocole UDP pour s'échanger des datagrammes. Contrairement au protocole TCP, le protocole UDP ne comprend pas de communication préliminaire pour établir des chemins de données ou assurer le classement et la vérification des données. Toutefois, en évitant le surdébit nécessaire à la fourniture de ces fonctions, le protocole UDP est plus rapide que le protocole TCP. Le protocole UDP peut être privilégié pour les applications soumises à des délais stricts, lorsqu'il vaut mieux que des datagrammes soient abandonnés plutôt que différés. UDP est le transport principal pour la messagerie implicite dans EtherNet/IP.

UMAS:

Acronyme de *Unified Messaging Application Services*. Protocole système propriétaire qui gère les communications entre Control Expert et un contrôleur.

Une boucle de chaînage haute capacité:

Souvent désignée par l'acronyme HCDL (high-capacity daisy chain loop) une boucle de chaînage haute capacité utilise des commutateurs double anneau (DRSsRIODIO) pour connecter des sous-anneaux d'équipements (contenant des stations ou des équipements distribués) et/ou des nuages au réseau EthernetRIO.

UTC:

Acronyme de *universal time coordinated* (temps universel coordonné). Principal standard horaire utilisé pour réguler l'heure à travers le monde (proche de l'ancien standard GMT).

V

Valeur littérale d'entier:

Une valeur littérale d'entier est utilisée pour saisir des valeurs de type entier dans le système décimal. Les valeurs peuvent être précédées d'un signe (+/-). Les signes de soulignement (_) séparant les nombres ne sont pas significatifs.

Exemple :

-12, 0, 123_456, +986

variable:

Entité mémoire de type `BOOL`, `WORD`, `DWORD` (et types similaires) dont le contenu peut être modifié par le programme en cours d'exécution.

VLAN:

Acronyme de *virtual local area network* (réseau local virtuel). Réseau local (LAN) qui s'étend au-delà d'un seul LAN à un groupe de segments LAN. Un VLAN est une entité logique qui est créée et configurée de manière unique à l'aide d'un logiciel approprié.

Index

A

accès	
USB	20
ACL	
sécurité	33
actifs	
critiques, contrôleur CSPN M580	49
critiques, environnement CSPN M580	49
actifs critiques	
PAC, CSPN M580	49
altération des flux	
CSPN	50
altération du micrologiciel	
CSPN	50
altération du mode d'exécution	
CSPN	50
altération du programme en mémoire	
CSPN	50
architecture	19
authentification	
cybersécurité	128
autorisation	
sécurité	105
autorisations	
cybersécurité	128

B

bureau à distance	
cybersécurité	28

C

cartes d'interface réseau	
cybersécurité	28
certification	
CSPN	43
communication sécurisée	
CSPN	50
cybersécurité	128
communication, sécurisée	
CSPN	50

comptes	
cybersécurité	100
consignation	
sécurité	52
consignation des événements	
cybersécurité	128
Control Expert	
password	104
Control Expert Security Editor	46
contrôle d'accès	
cybersécurité	128
sécurité	33
contrôleur, mémoire	
CSPN	50
contrôleur, mode d'exécution	
CSPN	50
CSPN	43
actifs critiques, contrôleur	49
équipements critiques, environnement	49
M580, authentification chiffrée sur interface d'administration	50
M580, communications chiffrées	50
M580, gestion des entrées mal formées	50
M580, intégrité du mode d'exécution du contrôleur	50
M580, intégrité et authenticité de la mémoire du contrôleur	50
M580, modification des flux	50
M580, modification du micrologiciel	50
M580, modification du mode d'exécution	50
M580, modification du programme mémoire	50
M580, refus de service	50
M580, signature du micrologiciel	50
M580, stockage sécurisé des secrets	50
M580, stratégie de contrôle d'accès	50
modes de fonctionnement M580	48
paramètres de cybersécurité M580	48
cybersécurité	17
authentification	128
autorisations	128
bureau à distance	28
cartes d'interface réseau	28
communication sécurisée	128
comptes	100
connexion au réseau local	29
consignation des événements	128
contrôle d'accès	128

CSPN	43
CSPN, M580	43
CSPN, modes de fonctionnement M580	48
désactiver les services inutilisés	128
FTP	102
HTTP	101
LANMAN / NTLM	28
littérature	17
M340	136
M580	136
M580, Control Expert Security Editor	46
micrologiciel	128
mots de passe	100
notifications	17
paramètres CSPN du M580	48
Premium/Atrium	141
Quantum	136
recommandations	17
services	128
SNMP	103
vérifications d'intégrité	128
vulnérabilité	17
X80	138

D

désactiver	
services de communication	32
désactiver les services inutilisés	
cybersécurité	128

E

équipements critiques	
environnement, CSPN M580	49

F

FTP	
cybersecurity	102

G

gestion des entrées mal formées	
CSPN	50

H

HTTP	
cybersecurity	101

I

interface d'administration	
CSPN	50
interface, d'administration	
CSPN	50

L

LAN	
cybersécurité	29
LANMAN / NTLM	
cybersécurité	28
Lecture seule	
M580, profil Control Expert Security Editor	46
littérature	
cybersécurité	17

M

M340	
cybersecurity	136
M580	
cybersecurity	136
mémoire	
protéger	106
mémoire du contrôleur	
CSPN	50
messages du journal des événements	68
BMENOR2200H	82
BMENUA0100	82
Control Expert	62
Contrôleur M580 (micrologiciel antérieur à V4.10)	82
Contrôleur M580 (micrologiciel V4.10 et versions ultérieures prises en charge)	68
micrologiciel	
cybersécurité	128
sécurité	128
micrologiciel, signature	
CSPN	50

mode d'exécution du contrôleur	
CSPN	50
modes de fonctionnement	
CSPN, M580	48
mot de passe	
Control Expert	104
mots de passe	
cybersécurité.....	100

N

notifications	
cybersécurité.....	17

P

PC	
sécurisation renforcée.....	23
Premium/Atrium	
cybersecurity.....	141
profil	
M580, Control Expert Security Editor.....	46
profils d'utilisateur	
sécurité M580, Control Expert Security Editor	46
Programme	
M580, profil Control Expert Security Editor	46
protection	
section.....	106
protection de la mémoire	
sécurité.....	109
protéger	
mémoire.....	106

Q

Quantum	
cybersecurity.....	136

R

refus de service	
CSPN	50
run/stop	
sécurité.....	107

S

section	
protection.....	106
sécurisation renforcée	
PC.....	23
sécurité	
ACL.....	33
autorisation	105
consignation.....	52
contrôle d'accès.....	33
CSPN	43
CSPN, modes de fonctionnement M580 ...	48
M580, Control Expert Security Editor.....	46
micrologiciel.....	128
paramètres CSPN du M580.....	48
protection de la mémoire	109
run/stop	107
services	128
Syslog.....	52
trace d'audit.....	52
vérification d'intégrité	109
services	
cybersécurité.....	128
sécurité	128
services de communication	
désactiver	32
signature du micrologiciel	
CSPN	50
SNMP	
cybersecurity.....	103
stockage des secrets	
CSPN	50
stratégie de contrôle d'accès	
CSPN	50
Syslog	
BMENOR2200H	82
BMENUA0100	82
Control Expert	62
Contrôleur M580 (micrologiciel antérieur à V4.10).....	82
Contrôleur M580 (micrologiciel V4.10 et versions ultérieures prises en charge).....	68
security	52

T

trace d'audit	
---------------	--

sécurité	52
----------------	----

U

USB	
accès	20
Utilisation	
M580, profil Control Expert Security	
Editor	46

V

vérification d'intégrité	
sécurité	109
vérifications d'intégrité	
cybersécurité	128
vulnérabilité	
cybersécurité	17

X

X80	
cybersecurity	138

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre,
veuillez demander la confirmation des informations figurant dans cette publication.

© 2024 Schneider Electric. Tous droits réservés.

EIO0000002001.10