Plates-formes automates Modicon

Cybersécurité
Manuel de référence

(Traduction du document original anglais)

12/2018

EIO0000002001.06

www.schneider-electric.com

Schneider Electric

Le présent document comprend des descriptions générales et/ou des caractéristiques techniques des produits mentionnés. Il ne peut pas être utilisé pour définir ou déterminer l'adéquation ou la fiabilité de ces produits pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur ou intégrateur de réaliser l'analyse de risques complète et appropriée, l'évaluation et le test des produits pour ce qui est de l'application à utiliser et de l'exécution de cette application. Ni la société Schneider Electric ni aucune de ses sociétés affiliées ou filiales ne peuvent être tenues pour responsables de la mauvaise utilisation des informations contenues dans le présent document. Si vous avez des suggestions, des améliorations ou des corrections à apporter à cette publication, veuillez nous en informer.

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

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

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

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

Table des matières

Consignes de sécurité

Informations importantes

AVIS

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

DEMARRAGE 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 REGLAGES

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 (la version anglaise prévaut) :

- 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 déréglé 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.
- Seuls ces réglages fonctionnels, requis par l'opérateur, doivent lui être accessibles. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Présentation

Objectif du document

⚠ AVERTISSEMENT
COMPORTEMENT INATTENDU DE L'EQUIPEMENT, PERTE DE CONTROLE, PERTE DE DONNEES Les propriétaires, concepteurs, opérateurs et personnes chargées d'assurer la maintenance des équipements utilisant le logiciel Control Expert doivent lire et suivre les instructions fournies dans le document *Cybersécurité des plates-formes automate Modicon - Manuel de référence* (référence : EIO0000001999). **Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.**

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

NOTE : Dans ce document, le terme « sécurité » fait référence aux rubriques concernant la cybersécurité.

Champ d'application

Cette documentation est applicable à EcoStruxure™ Control Expert 14.0 ou version ultérieure.

Les caractéristiques techniques des équipements décrits dans ce document sont également fournies en ligne. Pour accéder à ces informations en ligne :

Etape	Action
1	Accédez à la page d'accueil de Schneider Electric *www.schneider-electric.com*.
2	Dans la zone **Search**, saisissez la référence d'un produit ou le nom d'une gamme de produits. ● N'insérez pas d'espaces dans la référence ou la gamme de produits. ● Pour obtenir des informations sur un ensemble de modules similaires, utilisez des astérisques (*).
3	Si vous avez saisi une référence, accédez aux résultats de recherche **Product Datasheets** et cliquez sur la référence qui vous intéresse. Si vous avez saisi une gamme de produits, accédez aux résultats de recherche **Product Ranges** et cliquez sur la gamme de produits qui vous intéresse.
4	Si plusieurs références s'affichent dans les résultats de recherche **Products**, cliquez sur la référence qui vous intéresse.
5	Selon la taille de l'écran, vous serez peut-être amené à faire défiler la page pour consulter la fiche technique.
6	Pour enregistrer ou imprimer une fiche technique au format .pdf, cliquez sur **Download XXX product datasheet**.

Les caractéristiques présentées dans ce document devraient être identiques à celles fournies en ligne. Toutefois, en application de notre politique d'amélioration continue, nous pouvons être amenés à réviser le contenu du document afin de le rendre plus clair et plus précis. Si vous constatez une différence entre le document et les informations fournies en ligne, utilisez ces dernières en priorité.

Informations concernant la cybersécurité

Des informations concernant la cybersécurité sont disponibles sur le site web de Schneider Electric : *http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page*

Document disponible en téléchargement dans la section de support de cybersécurité :

Titre du document	Adresse de la page web
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security Recommendations	*http://www.schneider-electric.com/ww/en/download/document/STN v2*

Document(s) à consulter

Titre de documentation	Référence
Modicon M580 - Guide de planification du système	HRB62666 (anglais), HRB65318 (français), HRB65319 (allemand), HRB65320 (italien), HRB65321 (espagnol), HRB65322 (chinois)
Modicon M580 - Matériel - Manuel de référence	EIO0000001578 (anglais), EIO0000001579 (français), EIO0000001580 (allemand), EIO0000001582 (italien), EIO0000001581 (espagnol), EIO0000001583 (chinois)
Modicon M580 - BMENOC0301/11 - Module de communication Ethernet - Guide d'installation et de configuration	HRB62665 (anglais), HRB65311 (français), HRB65313 (allemand), HRB65314 (italien), HRB65315 (espagnol), HRB65316 (chinois)
Modicon M340 pour Ethernet - Processeurs et modules de communication - Manuel utilisateur	31007131 (anglais), 31007132 (français), 31007133 (allemand), 31007494 (italien), 31007134 (espagnol), 31007493 (chinois)

Titre de documentation	Référence
Quantum sous EcoStruxure™ Control Expert - Configuration TCP/IP - Manuel utilisateurl	33002467 (anglais), 33002468 (français), 33002469 (allemand), 31008078 (italien), 33002470 (espagnol), 31007110 (chinois)
Premium et Atrium sous EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateurl	35006192 (anglais), 35006193 (français), 35006194 (allemand), 31007214 (italien), 35006195 (espagnol), 31007102 (chinois)
EcoStruxure™ Control Expert - Modes de fonctionnement	33003101 (anglais), 33003102 (français), 33003103 (allemand), 33003104 (espagnol), 33003696 (italien), 33003697 (chinois)
Quantum sous EcoStruxure™ Control Expert - Manuel de référence du matériel	35010529 (anglais), 35010530 (français), 35010531 (allemand), 35013975 (italien), 35010532 (espagnol), 35012184 (chinois)
Quantum sous EcoStruxure™ Control Expert - Module de communication Ethernet 140 NOC 771 01 - Manuel de l'utilisateur	S1A33985 (anglais), S1A33986 (français), S1A33987 (allemand), S1A33989 (italien), S1A33988 (espagnol), S1A33993 (chinois)
Premium sous EcoStruxure™ Control Expert - Module de communication Ethernet TSX ETC 101 - Manuel utilisateur	S1A34003 (anglais), S1A34004 (français), S1A34005 (allemand), S1A34007 (italien), S1A34006 (espagnol), S1A34008 (chinois)
Modicon M340 - Module de communication Ethernet BMX NOC 0401 - Manuel de l'utilisateur	S1A34009 (anglais), S1A34010 (français), S1A34011 (allemand), S1A34013 (italien), S1A34012 (espagnol), S1A34014 (chinois)

Titre de documentation	Référence
Quantum EIO - Réseau de contrôle - Guide d'installation et de configuration	S1A48993 (anglais), S1A48994 (français), S1A48995 (allemand), S1A48997 (italien), S1A48998 (espagnol), S1A48999 (chinois)
EcoStruxure™ Control Expert - Communication - Bibliothèque de blocs	33002527 (anglais), 33002528 (français), 33002529 (allemand), 33003682 (italien), 33002530 (espagnol), 33003683 (chinois)
Quantum sous EcoStruxure™ Control Expert - Modules réseau Ethernet - Manuel utilisateur	33002479 (anglais), 33002480 (français), 33002481 (allemand), 31007213 (italien), 33002482 (espagnol), 31007112 (chinois)
Modicon M580 BMECXM - Modules CANopen - Manuel utilisateur	EIO0000002129 (anglais), EIO0000002130 (français), EIO0000002131 (allemand), EIO0000002132 (italien), EIO0000002133 (espagnol), EIO0000002134 (chinois)
Automate MC80 - Manuel utilisateur	EIO0000002071 (anglais)

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

Chapitre 1
Présentation

Recommandations de Schneider Electric

Introduction

Votre système PC peut exécuter différentes applications destinées à renforcer la sécurité dans votre environnement de contrôle. Ses paramètres par défaut nécessitent une reconfiguration en fonction des recommandations de Schneider Electric concernant la défense en profondeur des équipements.

Les instructions suivantes décrivent les procédures dans un système d'exploitation Windows 7. Elles sont fournies à titre d'exemple. Les exigences ou procédures de votre système d'exploitation et de votre application peuvent être différentes.

Une rubrique dédiée à la cybersécurité est disponible dans la zone de support du *Schneider Electric website*.

Approche de défense en profondeur

Outre les solutions présentées dans ce document, il est recommandé de suivre l'approche de défense en profondeur de Schneider Electric décrite dans le guide STN suivant :

- **Titre du document :** How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security 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 notifiées dans la page Web **Cybersecurity support** : *http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page*.

> **> List of Security Notifications**

Si vous rencontrez un incident de cybersécurité ou une vulnérabilité qui ne figure pas dans la liste fournie par Schneider Electric, signalez-le en cliquant sur **Report an incident or vulnerability** dans la page web **Cybersecurity support**.

> **> Report an incident or vulnerability**

Chapitre 2
Comment sécuriser l'architecture

Introduction

Ce chapitre décrit les actions à effectuer dans l'architecture de plate-forme des contrôleurs Modicon pour la sécuriser.

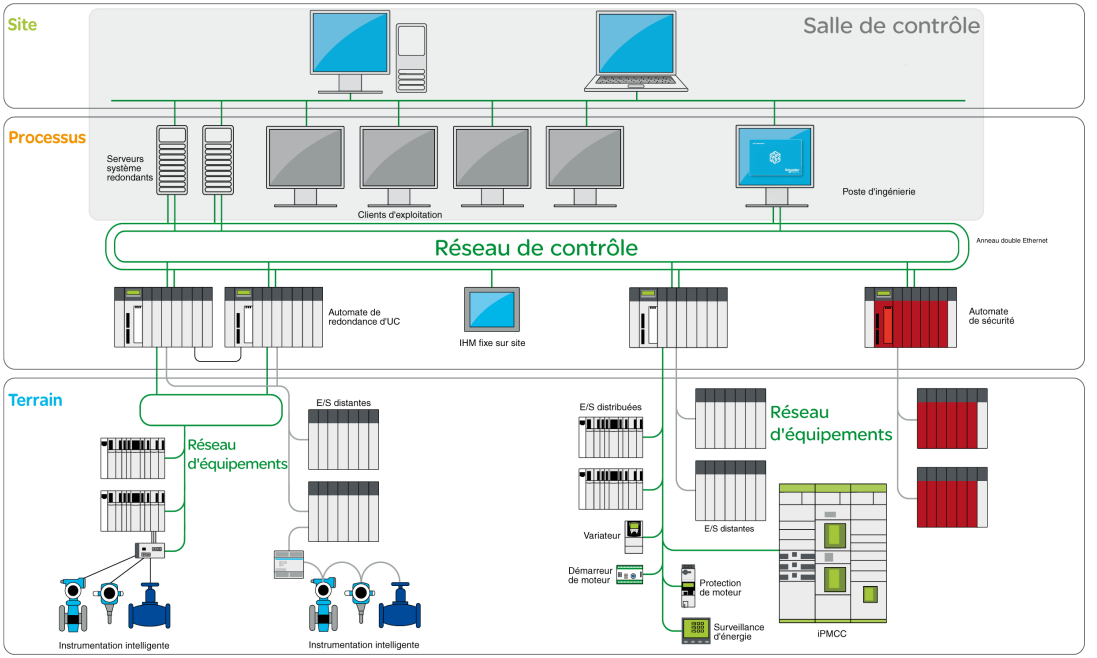
Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Présentation du système

Architecture du système

L'architecture PlantStruxure suivante souligne la nécessité d'une architecture multicouche (avec un réseau de contrôle et un réseau d'équipements) sécurisable. Une architecture plate (avec tous les équipements connectés au même réseau) n'est pas sécurisable.



Communication sécurisée

Les équipements situés dans la salle de commande sont plus exposés aux attaques que ceux qui sont connectés au réseau d'équipements. Donc implémentez une communication sécurisée entre la salle de contrôle d'une part et le PAC et 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 de système ci-dessous, la zone de la salle de contrôle est grisée pour la distinguer du PAC et des équipements.

Accès sécurisé aux ports USB

L'accès physique aux ports USB de l'UC doit être contrôlé.

NOTE : La sécurisation des ports USB de l'UC ne peut s'effectuer que par des moyens physiques (par exemple, armoire ou clé physique).

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

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

Sécurisation renforcée du PC

Introduction

Les PC situés dans la salle de contrôle sont très vulnérables aux attaques. La sécurité de ceux qui prennent en charge Control Expert ou OFS doit être renforcée.

Sécurisation renforcée des postes de travail d'ingénierie

Les clients ont le choix entre différents PC commerciaux pour leurs postes de travail d'ingénierie. Les principales techniques de sécurisation renforcée sont les suivantes :

- Gestion des mots de passe forts
- Gestion des comptes utilisateur
- Méthodes du droit minimum appliqué aux applications et comptes utilisateur
- Suppression ou désactivation des services superflus
- Suppression des droits de gestion à distance
- Gestion systématique des correctifs

Désactivation des cartes d'interface réseau inutilisées

Vérifiez que les cartes d'interface réseau non requises par l'application sont désactivées. 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 7, procédez comme suit :

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

Configuration de la connexion au réseau local

Différents paramètres réseau de Windows renforcent la sécurité en la mettant au niveau de l'approche de défense en profondeur recommandée par Schneider Electric.

Dans les systèmes Windows 7, 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).** .

La liste suivante présente un exemple des modifications de configuration que vous pouvez apporter à votre système dans 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**, décochez les cases **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, des masques de sous-réseau et des passerelles IPv4 statiques.
- N'utilisez pas DHCP ou DNS dans la salle de contrôle.

Désactivation du protocole RDP (bureau à distance)

Les recommandations de Schneider Electric relatives au renforcement de la protection incluent la désactivation du protocole de connexion de bureau à distance (RDP) sauf si votre application requiert le protocole RDP. La procédure ci-dessous décrit comment désactiver ce protocole :

Etape	Action
1	Dans Windows 2008R2 ou Windows 7, désactivez le protocole RDP en sélectionnant **Ordinateur → Propriétés système → Paramètres système avancés**.
2	Dans l'onglet **Utilisation à distance**, désactivez la case à cocher **Autoriser les connexions d'assistance à distance vers cet ordinateur**.
3	Sélectionnez l'option **Ne pas autoriser les connexions à cet ordinateur**.

Mise à jour des stratégies de sécurité

Mettez à jour les stratégies de sécurité sur les ordinateurs de votre système en utilisant `gpupdate` dans une fenêtre de commande. Pour plus d'informations, consultez la documentation Microsoft relative à `gpupdate`.

Désactivation de LANMAN et de NTLM

Le protocole Microsoft LAN Manager (LANMAN ou LM) et son successeur NT LAN Manager (NTLM) présentent des vulnérabilités. Leur utilisation est donc déconseillée dans les applications de contrôle.

La procédure ci-dessous indique comment désactiver LM et NTLM sur un système Windows 7 ou Windows 2008R2 :

Etape	Action
1	Dans une fenêtre de commande, exécutez `secpol.msc` pour ouvrir la fenêtre **Stratégie de sécurité locale**.
2	Ouvrez **Paramètres de sécurité → Stratégies locales → Options de sécurité**.
3	Sélectionnez **Envoyer uniquement les réponses NTLMv2. Refuser LM et NTLM** dans le champ **Sécurité réseau : niveau d'authentification LAN Manager**.
4	Cochez la case **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 `gpupdate` pour valider la stratégie de sécurité modifiée.

Gestion des mises à jour

Avant le déploiement, mettez-à jour tous les systèmes d'exploitation de PC à l'aide des utilitaires proposés dans la page Web **Windows Update** de Microsoft. Pour accéder à cet outil dans Windows 2008R2 ou Windows 7, sélectionnez **Démarrer → Tous les programmes → Windows Update**.

Désactivation des services de communication intégrés inutilisés

Services de communication intégrés

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

Description

Pour réduire le spectre des attaques possibles et fermer des portes de communication potentielles, désactivez tout service intégré inutilisé.

Désactivation de services Ethernet dans Control Expert

Vous pouvez activer/désactiver les services Ethernet Ethernet dans les onglets de control Expert. Les onglets sont décrits pour chacune des plates-formes suivantes :

- Modicon M340 *(voir page 64)*
- Modicon M580 *(voir page 65)*
- Modicon Quantum *(voir page 66)*
- Modicon X80 modules *(voir page 68)*
- Modicon Premium/Atrium *(voir page 69)*

Définissez les paramètres des onglets Ethernet avant de télécharger l'application dans l'UC (CPU).

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` *(voir EcoStruxure™ Control Expert, Communication, Bibliothèque de blocs)* permet de désactiver un service après sa configuration dans l'application Control Expert. Le service peut être réactivé à l'aide du même bloc fonction.

Restriction du flux de données provenant du réseau de contrôle (contrôle d'accès)

Flux de données provenant du réseau de contrôle

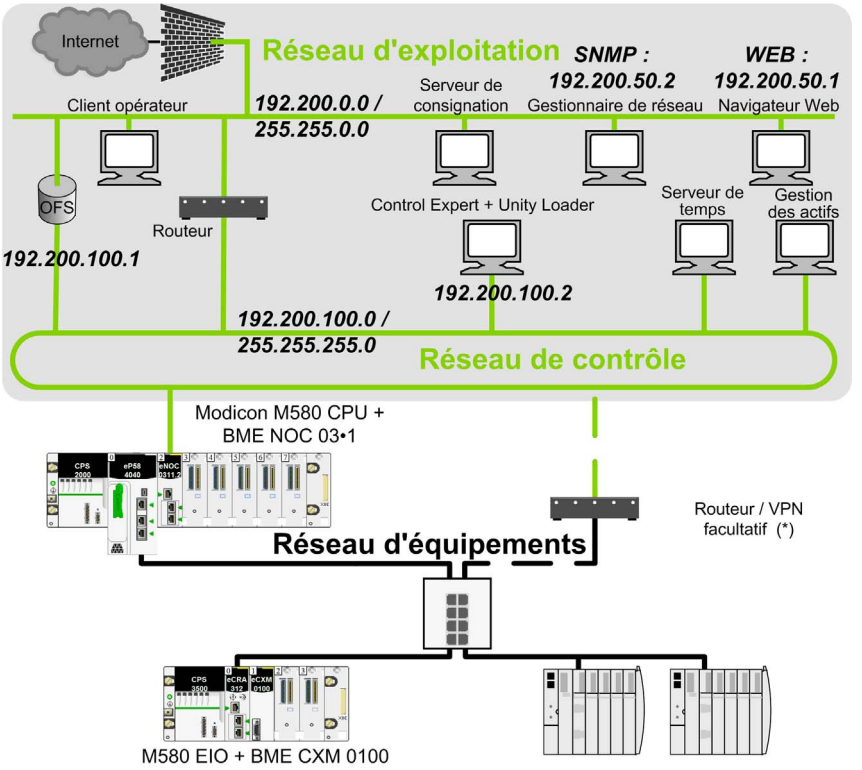
Ce flux de données IP émane du réseau de contrôle.

Description

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

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 provenant des équipements qui communiquent sur les réseaux d'exploitation et de contrôle (situés dans la zone grisée).



(*) Certains services requièrent un accès au réseau d'équipements (par exemple : mise à jour du micrologiciel, horodatage de la source). Dans ces cas, c'est un routeur/VPN qui gère l'accès sécurisé.

Configuration des adresses autorisées dans l'exemple d'architecture

Objectifs du contrôle d'accès :

- Tout équipement connecté au réseau d'exploitation (adresse IP = 192.200.x.x) a accès au serveur Web de l'UC.
- Tout équipement connecté au réseau de contrôle (adresse IP = 192.200.100.x) peut communiquer avec l'UC selon le protocole Modbus TCP et accéder au serveur Web de l'UC.

Pour limiter le flux de données dans l'exemple d'architecture ci-dessus, les adresses et services autorisés sont définis comme suit dans ce tableau de contrôle d'accès Control Expert :

Source	Adresse IP	Sous-réseau	Masque sous-réseau	FTP	TFTP	HTTP	Port502	EIP	SNMP
Gestionnaire de réseau	192.200.50.2	Non	–	–	–	–	–	–	X
Réseau d'exploitation	192.200.0.0	Oui	255.255.0.0	–	–	X	–	–	–
Unity Loader	192.200.100.2	Non	–	X	–	–	–	–	–
Réseau de contrôle	192.200.100.0	Oui	255.255.255.0	–	–	–	X	–	–
X Sélectionné – Non sélectionné ou sans contenu									

Description des réglages

Une adresse autorisée est définie pour les équipements autorisés à communiquer avec l'UC selon le protocole Modbus TCP ou EtherNet/IP.

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

192.200.50.2 (SNMP): configuré pour autoriser l'accès à partir du gestionnaire de réseau avec le protocole SNMP.

192.200.0.0 (HTTP) : sous-réseau du réseau d'exploitation configuré pour autoriser tous les navigateurs Web connectés au réseau d'exploitation à accéder au navigateur Web de l'UC.

192.200.100.2 (FTP): configuré pour autoriser l'accès à partir de Unity Loader avec le protocole FTP.

192.200.100.0 (Port502) : sous-réseau du réseau de contrôle configuré pour autoriser tous les équipements connectés au réseau de contrôle (OFS, Control Expert, Unity Loader) à accéder à l'UC via le Port502 Modbus.

NOTE : l'analyse de la liste d'accès concerne chaque entrée de celle-ci. Si une correspondance (adresse IP + service autorisé) est trouvée, les autres entrées sont ignorées.
Dans l'écran **Sécurité** de Control Expert, saisissez les règles propres à un sous-réseau dédié, avant la règle du sous-réseau. Par exemple, pour octroyer un droit SNMP particulier à l'équipement 192.200.50.2, saisissez la règle avant celle du sous-réseau 192.200.0.0/255.255.0.0 qui autorise un accès HTTP à tous les équipements du sous-réseau.

Configuration de la communication sécurisée

Introduction

La communication sécurisée vise à protéger les voies de communication qui autorisent un accès distant aux ressources critiques du système (telles que l'application PAC intégrée ou le micrologiciel). IPsec (acronyme d'Internet Protocol Security) est un standard ouvert défini par l'IETF, qui assure des communications privées et protégées sur des réseaux IP en combinant des protocoles de sécurité et des mécanismes cryptographiques. Notre implémentation de la protection IPsec inclut l'anti-relecture, la vérification de l'intégrité des messages et l'authentification de l'origine des messages.

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

Description

La fonction IPsec permet de sécuriser :

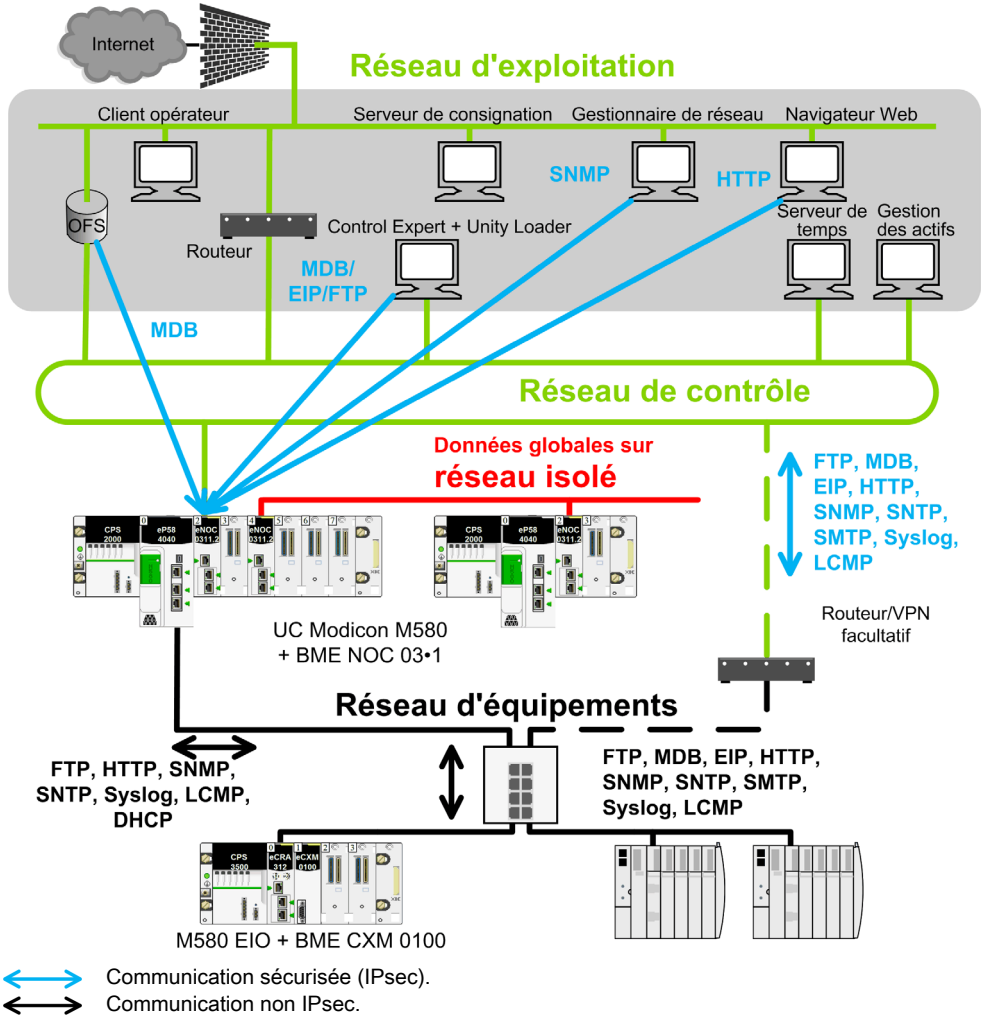
- l'accès Modbus de la salle de contrôle à l'UC PAC via le module BMENOC0301/11 ;
- l'accès de la salle de contrôle aux services de communication exécutés à l'intérieur du module BMENOC0301/11 en mode serveur (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

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

Connexion sans fil : lorsqu'un module sans fil PMXNOW0300 est utilisé pour configurer une connexion sans fil, configurez-le avec le niveau de sécurité maximum disponible (WPA2-PSK).

Exemple d'architecture

La figure suivante montre, au moyen d'un exemple, les différents protocoles ou services mis en œuvre dans une communication sécurisée entre la salle de contrôle et un PAC Modicon M580.



Flux de données avec fonctionnalité de communication sécurisée

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

Service Ethernet	Sécurité des flux de données
Serveur EIP de classe 3	Ces services sont pris en charge à l'aide de connexions sécurisées.
Serveur FTP, serveur TFTP	
HTTP	
ICMP (ping, etc.)	
Serveur Modbus (port 502)	
ARP	Ces services sont pris en charge à l'aide de connexions sécurisées et non sécurisées. **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 le protocole IPSec est activé. **NOTE :** avant que l'homologue (PC) n'initie IKE/IPsec, IPSec ne sécurise pas ce trafic. Une fois le protocole IKE/IPSec actif, IPsec sécurise ce trafic. Le protocole n'est pris en charge que si le destinataire des paquets est un PC sur lequel IPSec est 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 OSI de couche 3. Les protocoles OSI de couche 2 (ARP, RSTP, LLDP, protocole de vérification en boucle) ne sont pas protégés par IPsec.
- IPsec ne peut pas sécuriser le flux de communication **Global data** (à l'aide de modules BMXNGD0100). Utilisez cette configuration sur un réseau isolé.

Limitations

Limitations de IPsec dans l'architecture : BMENOC0301/11 ne prend pas en charge la transmission IP au réseau d'équipements.

Si la transparence est requise entre le réseau de contrôle et le réseau d'équipements, un routeur/parefeu/VPN externe (comme un parefeu) est nécessaire pour sécuriser la communication entre les deux réseaux (comme indiqué dans l'exemple d'architecture précédent *(voir page 27)*).

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

- mise à jour du micrologiciel de l'UC Modicon M580 à partir de Unity Loader via le service FTP ;
- réalisation d'un diagnostic réseau de l'UC Modicon M580 à partir d'un outil de gestion de réseau via le service SNMP ;
- diagnostic d'une UC Modicon M580 à partir d'un DTM via le service EIP ;
- diagnostic d'une UC Modicon M580 à partir d'un navigateur Web via le service HTTP ;
- consignation des événements de cybersécurité d'une UC Modicon M580 dans un serveur syslog via le service syslog ;
- synchronisation de l'heure de l'UC Modicon M580 à partir d'un serveur de temps global via le service NTP.

NOTE : Le BMENOC0301/11 est le seul module à assurer une communication sécurisée entre l'atelier et la salle de contrôle.

Configuration de la communication IPsec dans l'architecture du système

Pour configurer la communication IPsec, procédez comme suit :

- Dans la salle de contrôle, identifiez les applications clientes autorisées qui doivent communiquer avec le PAC à l'aide de Modbus (Control Expert, Unity Loader, OFS, applications clientes telles que SGBackup, ...).
  Configurez IPsec sur chaque PC prenant en charge ces applications autorisées.
- Dans la salle de contrôle, identifiez les applications clientes autorisées qui doivent communiquer avec chaque module BMENOC0301/11 configuré dans le rack local (Control Expert DTM, Unity Loader, gestionnaire SNMP, navigateur Web, concepteur Web pour module FactoryCast BMENOC0301/11).
  Configurez IPsec sur chaque PC prenant en charge ces applications autorisées.
- Intégrez un module BMENOC0301/11 avec fonction IPsec dans l'embase de chaque PAC connecté au réseau de contrôle.
  Pour configurer la fonction IPsec sur un module BMENOC0301/11, procédez en deux étapes :
  - 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 : reposant sur ce secret partagé, IPsec est un élément clé de la stratégie de sécurité gérée par l'administrateur de sécurité. Pour renforcer la sécurité de la clé pré-partagée, nous vous recommandons d'utiliser un outil externe comme KeePass *(voir page 30)* pour générer une chaîne de caractères appropriée.

Le module BMENOC0301/11 est configuré avec Control Expert. Initialement, l'application est téléchargée via le lien USB. Les téléchargements ultérieurs sont effectués par Ethernet avec fonction IPsec si IPsec est activé.

Chaque PC prenant en charge IPsec doit être conforme aux exigences suivantes pour la configuration IPsec :

- Utilisez Microsoft Windows 7 ou Windows 10.
- Détenir les droits d'administrateur permettant de configurer IPsec.
  Une fois IPsec configuré, définissez le compte Windows comme un compte utilisateur normal sans droits d'administrateur.
- **Renforcez la protection du PC en procédant comme indiqué dans la rubrique *Sécurisation renforcée du PC*** *(voir page 20)*.

Pour plus d'informations sur la configuration, consultez la rubrique *Configuration des communications IP sécurisées (voir Modicon M580, BMENOC0301/0311 Ethernet Communications Module, Installation and Configuration Guide)*.

Génération des clés pré-partagées avec une sécurité optimale

La sécurité des communications IPsec repose sur la complexité de la clé pré-partagée. Nous recommandons l'utilisation d'outils spécialisés pour générer des clés pré-partagées d'une sécurité optimale.

Notamment KeePass, que vous pouvez télécharger gratuitement à partir d'Internet. Téléchargez KeePass, installez-le sur votre PC et lancez-le.

Configurez KeePass v2.34 et utilisez-le pour générer des mots de passe utilisables comme clés pré-partagées :

Etape	Action
1	Créez un 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 le dossier.
3	Dans la boîte de dialogue **Create Composite Master Key**, renseignez le champ **Master password**. Saisissez à nouveau le mot de passe dans le champ **Repeat**.
4	Appuyez sur **OK** pour ouvrir l'**étape 2**, puis appuyez à nouveau sur **OK**.
5	Dans la boîte de dialogue de la nouvelle base de données, développez **New Database**.
6	Sélectionnez **Réseau** 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 renseigner les champs **Password** et **Repeat password**.
12	Ouvrez la boîte de dialogue **Password Generation Options** (**Tools → Generate Password**).

Etape	Action
13	Effectuez les sélections suivantes dans **Generate using character set** : ● Upper-case (A, B, C, …) ● Lower-case (a, b, c, …) ● Digits (0, 1, 2, …) ● Minus (-) ● Underline (_) ● Special (!, $, %, &, …) ● Brackets ([,], [, (,), <, >) **NOTE :** Les caractères suivants ne sont pas autorisés dans la clé pré-partagée : ● { ● } ● ; ● #
14	Cliquez sur **OK**.
15	Cliquez avec le bouton droit de la souris sur votre équipement 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 du protocole IPsec.

Diagnostic de la communication IPsec dans l'architecture du système

Pour plus d'informations sur le diagnostic d'IPsec dans l'architecture du système, consultez la rubrique *Configuration des communications IP sécurisées (voir Modicon M580, BMENOC0301/0311 Ethernet Communications Module, Installation and Configuration Guide)*.

Cible de sécurité CSPN

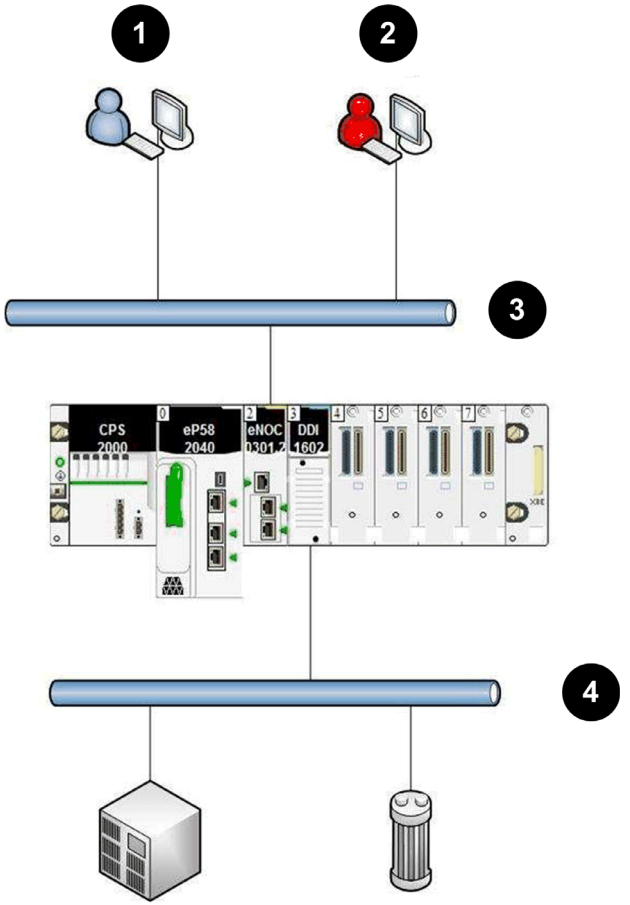
Présentation de la certification CSPN

CSPN (Certification de Sécurité de Premier Niveau) est une certification de cybersécurité actuellement utilisée en France. Un produit doté de la certification CSPN est censé résister à une cyberattaque menée par deux hommes-mois de pirates expérimentés. La plate-forme Modicon M580 est certifiée CSPN. Cette rubrique décrit l'environnement, les configurations d'automate programmable (PAC) et les paramètres qui répondent aux exigences de la certification CSPN pour assurer un niveau optimal de sécurité.

Présentation du PAC M580

Le PAC M580 est conçu pour contrôler et commander continuellement un processus industriel sans intervention humaine. A chaque étape, le PAC traite les données reçues de ses entrées, des capteurs, et envoie des commandes à ses sorties, les actionneurs. Les échanges avec la supervision (HMI, SCADA) sont effectués via un module de communication Ethernet BMENOC0301/0311 situé dans le rack local avec le PAC. Le PAC peut fonctionner dans un environnement hostile et en dépit de l'humidité, de la poussière ou de températures inhabituelles pour des systèmes informatiques et en présence de contraintes mécaniques ou CEM importantes.

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



1 Opérateur utilisant Control Expert
2 Utilisateur malveillant
3 Réseau de supervision
4 Réseau de terrain sans utilisateur malveilllant

Fonctionnalités M580

Le PAC M580 PAC offre les fonctionnalités suivantes :

Fonction	Description
Exécution du programme utilisateur	Un PAC M580 exécute un programme utilisateur qui traite les entrées et met à jour les sorties.
Gestion des entrées/sorties	Un PAC M580 peut lire des entrées locales et écrire des sorties locales. Ces entrées/sorties, qui peuvent être numériques ou analogiques, permettent au PAC M580 de contrôler et commander le processus industriel.
Communication avec la supervision	Un PAC M580 peut communiquer avec un système SCADA pour recevoir des commandes et transmettre des données de processus via le protocole Modbus.
Fonctions administratives	Un PAC M580 intègre des fonctions administratives, fournies dans Control Expert , à des fins de configuration et de programmation.
Journalisation à distance	Un PAC M580 prend en charge la définition d'une stratégie de journalisation 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	Version 2.20 ou ultérieure	Cette UC respecte les règles de sécurité décrites dans les documents de sécurité (voir les hypothèses).
BMENOC0301/0311	Version 2.11 ou ultérieure	Ce module Ethernet gère les communications sécurisées avec la couche supérieure (logiciel de supervision et d'ingénierie Control Expert).

NOTE : Control ExpertLe logiciel de programmation , les PC, les autres modules PAC et les composants de l'embase n'entrent pas dans le cadre de la certification.

Profils utilisateur

Les utilisateurs qui interagissent avec le PAC pour une implémentation sécurisée disposent des profils suivants prédéfinis par l'éditeur de sécurité Control Expert :

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

Implémentation sécurisée

Les éléments suivants contribuent à la mise en place d'un environnement propice à une implémentation sécurisée :

Elément	Critères de sécurité
Documentation sur la sécurité	La documentation du produit (guides d'utilisation, livres blancs, etc.) comprend les instructions pour une utilisation sécurisée. Toutes les recommandations qui y figurent sont appliquées avant l'évaluation.
Administrateurs	Les administrateurs système sont compétents, formés et dignes de confiance.
Locaux	Le PAC réside dans un local sécurisé dont l'accès est restreint aux seules personnes dignes de confiance. En particulier, un utilisateur malveillant n'a pas accès aux ports physiques des PAC. 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 Control Expert avant son chargement dans le PAC.
Journalisation active	La fonction de journalisation 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 PAC via l'interface USB, et le PAC est déconnecté du réseau.
Mise à niveau du micrologiciel	Le micrologiciel est mis à niveau à l'aide de l'interface USB, et le PAC est déconnecté 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 PAC peut être effectuée avec une station d'ingénierie Control Expert connectée de point à point au port Ethernet **ou** au port USB local du PAC.
- Dans les conditions de fonctionnement normal (mode d'exécution, SCADA connecté sur le réseau de contrôle Ethernet), vérifiez que Control Expert est déconnecté.
- Pour toute modification ultérieure de la configuration ou du programme d'application, connectez Control Expert au port USB du PAC.

Paramètres de cybersécurité

Ce tableau décrit les paramètres de cybersécurité :

Paramètre	Rubrique	Guide de l'utilisateur
ACL activée.	Configuration des services de sécurité	Modicon M580 - Module de communication Ethernet BMENOC0301/0311 - Guide de l'utilisateur
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	Modicon M580 - Matériel - Manuel de référence
Protection de la mémoire activée.	Protection mémoire	
Projet totalement sécurisé : ● Application sécurisée avec identifiant et mot de passe. ● Protection de section activée.	Protection d'un projet dans Control Expert	
Aucune information de chargement stockée dans l'UC.	Données intégrées du PAC	EcoStruxure™ Control Expert - Modes de fonctionnement
Modification du mot de passe par défaut du 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 répertorie les équipements critiques par rapport à l'environnement :

Equipement	Description pour une utilisation appropriée
Contrôle-commande du processus industriel	Le PAC contrôle et commande un processus industriel en lisant des entrées et en envoyant des commandes à des actionneurs. La disponibilité de ces actions fait l'objet d'une protection.
Flux du poste de travail d'ingénierie	L'intégrité, la confidentialité et l'authenticité des flux entre le PAC et le poste de travail d'ingénierie sont protégées.

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

Equipement	Disponibilité	Confidentialité	Intégrité	Authenticité
Contrôle-commande du processus industriel	X			
Flux du poste de travail d'ingénierie		X	X	X

PAC : Ce tableau répertorie les équipements critiques des PAC :

Equipement	Description pour une utilisation appropriée
Micrologiciel	L'intégrité et l'authenticité du micrologiciel sont protégées.
Mémoire du PAC	La mémoire du PAC contient la configuration du PAC et 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 PAC sont protégées.
Secrets d'utilisateur	Les utilisateurs concernés ne divulguent pas les mots de passe qu'ils utilisent pour s'authentifier.

Exigences de sécurité pour les équipements critiques du PAC :

Equipement	Disponibilité	Confidentialité	Intégrité	Authenticité
Micrologiciel			X	X
Mémoire du PAC			X	X
Mode d'exécution			X	X
Secrets d'utilisateur		X	X	

Menaces pour la sécurité

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

	Contrôle-commande du processus industriel	Flux du poste de travail d'ingénierie	Micrologiciel	Mémoire du PAC	Mode d'exécution	Secrets d'utilisateur
Refus de service	Di					
Altération du micrologiciel		I, Au				
Altération du mode d'exécution					I, Au	
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 arrive à générer un refus de service sur le PAC en effectuant une action inattendue ou en explorant une vulnérabilité (envoi d'une requête mal formée, utilisation d'un fichier de configuration corrompu...). Ce refus de service affecte l'ensemble du PAC ou seulement certaines de ses fonctions.
Altération du micrologiciel	L'attaquant parvient à injecter et exécuter un micrologiciel corrompu sur le PAC. 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 PAC par des moyens légitimes. Au final, l'attaquant arrive à modifier la version du micrologiciel installée sur le PAC sans en avoir le droit.
Altération du mode d'exécution	L'attaquant parvient à modifier le mode d'exécution du PAC sans y être autorisé (commande stop par exemple).
Altération de la mémoire	L'attaquant parvient à modifier (temporairement ou de façon permanente) le programme utilisateur ou la configuration qui s'exécute dans la mémoire du PAC.
Altération des flux	L'attaquant parvient à altérer les échanges entre le PAC et un composant externe sans être détecté. Il peut effectuer des attaques telles que le vol des informations d'identification, la violation du contrôle d'accès ou la mitigation du contrôle du processus industriel.

	Refus de service permanent	Altération du micro-logiciel	Altération du mode d'exécution	Altération de la mémoire	Altération des flux
Gestion des entrées mal formées	X				
Stockage sécurisé des secrets				X	
Authentification sécurisée sur interface administrative					X
Stratégie de contrôle d'accès					X
Signature de micrologiciel		X			
Intégrité et authenticité de la mémoire du PAC				X	
Intégrité du mode d'exécution du PAC			X		
Communication sécurisée					X

Type de menace	Description
Gestion des entrées mal formées	Le PAC a été développé pour gérer correctement les entrées mal formées, notamment le trafic réseau mal formé.
Gestion sécurisée des secrets	Le PAC a été développé pour gérer correctement les entrées mal formées, notamment le trafic réseau mal formé. ● 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 PAC ● Mots de passe d'autres services (comme FTP)
Authentification sécurisée sur interface administrative	Les jetons de session sont protégés contre le piratage et la relecture ; ils ont une durée de vie brève. L'identité et les droits du compte utilisateur sont vérifiés systématiquement avant toute action nécessitant un privilège. Un mot de passe d'application est défini dans chaque configuration pour éviter toute modification du PAC par un utilisateur non authentique.
Stratégie de contrôle d'accès	La stratégie de contrôle d'accès permet de garantir l'authenticité des opérations nécessitant des privilèges, à savoir les opérations qui peuvent modifier des équipements critiques identifiés. La liste de contrôle d'accès (ACL) est activée dans chaque configuration et seules les adresses IP identifiées peuvent se connecter au PAC.
Signature de 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 PAC	La fonction de protection de la mémoire est activée dans chaque configuration, ce qui permet 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 PAC se charge d'assurer l'intégrité et l'authenticité du programme utilisateur, de sorte que ce dernier ne peut être modifié que par des utilisateurs autorisés. 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 PAC	Le PAC se charge d'assurer que le mode d'exécution ne peut être modifié que par des utilisateurs autorisés et authentifiés. La fonctionnalité RUN/STOP par entrée uniquement est activée, ce qui permet d'éliminer la possibilité de modification d'état RUN/STOP via l'interface Ethernet.
Communication sécurisée	Le PAC prend en charge la communication sécurisée, protégée en termes d'intégrité, de confidentialité et d'authenticité (IPsec crypté avec ESP). Le protocole FTP est désactivé et IPsec garantit une communication Modbus sécurisée via le module BMENOC0301/0311.

Configuration de l'audit de la cybersécurité (consignation des événements)

Introduction

La consignation des événements et l'analyse de cette consignation sont essentielles dans un système sécurisé. 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 en local 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 à l'aide du protocole Syslog ;
- des clients de consignation (points de connexion Ethernet où les événements de cybersécurité sont surveillés : équipement, Control Expert ou DTM).

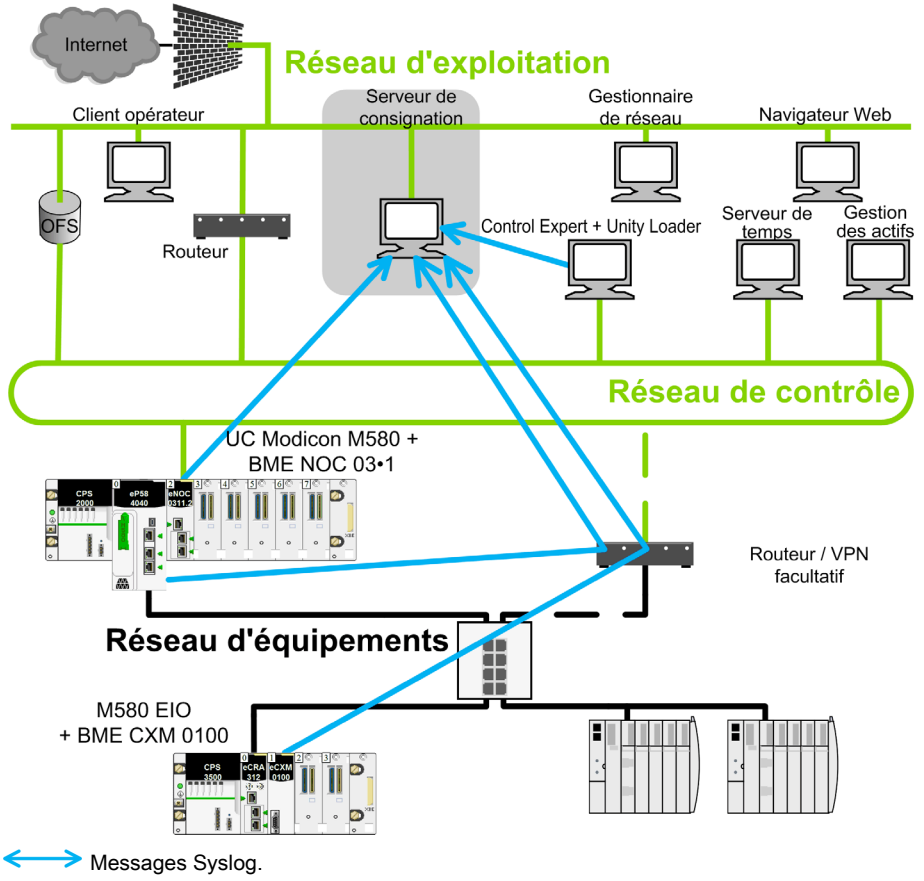
Description du service de consignation des événements

Chaque client de consignation sert à :

- détecter et horodater les événements.
  Une 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 des équipements.

Exemple d'architecture

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



Evénements consignés

Structure d'un message Syslog :

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 est défini par la 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 et font partie du champ TIMESTAMP. **T** et **Z** doivent figurer en majuscules. **Z** spécifie que l'heure est au format UTC. Description du contenu du champ d'horodatage : **YYY** Année **MM** Mois **DD** Jour **hh** Heure **mm** Mois **ss** Seconde **nnn** Fraction de seconde en milliseconde (0 si non disponible)
HOSTNAME	Identifie la machine ayant envoyé le message Syslog : nom de domaine complet (FQDN) ou adresse IP statique source, si FQDN n'est pas pris en charge.
APP-NAME	Identifie l'application qui crée le message Syslog. Il contient des informations qui permettent d'identifier l'entité émettrice du message (par exemple, un sous-ensemble d'une référence commerciale).
PROCID	Identifie le processus, l'entité ou le composant qui envoie l'événement. Reçoit la valeur NILVALUE s'il n'est pas utilisé.
MSGID	Identifie le type de message auquel l'événement est lié, par exemple HTTP, FTP, Modbus. Reçoit la valeur NILVALUE s'il n'est pas utilisé.
MESSAGE TEXT	Ce champ contient plusieurs informations : ● Adresse de l'émetteur : adresse IP de l'entité qui génère le journal. ● ID de l'homologue : si un homologue est impliqué dans l'opération (par exemple, nom d'utilisateur d'une opération de consignation). Reçoit la valeur Null s'il n'est pas utilisé. ● Adresse de l'homologue : si un homologue est impliqué dans l'opération. Reçoit la valeur Null s'il n'est pas utilisé. ● Type : numéro unique attribué à un message (description fournie dans les tableaux suivants). ● Commentaire : chaîne décrivant le message (description fournie dans les tableaux suivants).

Le tableau suivant présente des événements liés à un PAC, qui peuvent être consignés dans un serveur syslog :

Description de l'événement	Catégorie	Gravité (1)	Type	Commentaire
Connexion établie à partir de ou depuis un outil ou un équipement : ● Connexion établie. Par exemple : stockage de données via FTP, mot de passe de Control Expert via Modbus, chargement de micrologiciel via FTP, FDR... ● Connexion établie de l'utilisateur à un outil. Par exemple : éditeur de sécurité de Control Expert. ● Connexion TCP établie (aucun utilisateur). Par exemple : message explicite TCP/IP Modbus Port502 pour l'UC M580.	10	Informational	1	`Successful login` ou `successful connection`.
Echec de connexion à partir d'un outil ou d'un équipement : ● Echec de connexion suite à une vérification erronée de la liste de contrôle d'accès (ACL) (adresse IP source ou filtrage de port TCP). ● Echec de connexion (avec vérification correcte de l'ACL). Par exemple : stockage de données via FTP, application Control Expert via Modbus, serveur FDR via FTP... ● Echec de connexion de l'utilisateur à un outil logiciel. Par exemple : Control Expert. ● Echec de connexion TCP (aucun utilisateur). Par exemple : message explicite TCP/IP Modbus Port502 pour l'UC M580.	10	Warning	2	`Failed login`, `failed connection` ou `connection denied from`.
Déconnexion déclenchée en local ou par un homologue : ● En cas de requête de déconnexion (FTP).	10	Informational	5	`Disconnection`.
Déconnexion automatique (par exemple, timeout d'inactivité).	10	Informational	6	`Auto logout`.
Modifications majeures dans le système : ● Chargement du micrologiciel.	13	Informational	10	`XXXX upload`. Par exemple : `firmware upload`, `web pages upload`.
(1) REMARQUE : les termes gravité, Emergency, Alert, Critical, Error, Warning, Notice, Informational et Debug sont utilisés dans ce tableau comme des attributs des messages d'événement syslog et définis dans la spécification RFC 5424 de l'Internet Engineering Task Force (IETF).				

Description de l'événement	Catégorie	Gravité (1)	Type	Commentaire
Modification de l'exécution des paramètres de communication hors de la configuration : ● Services de communication activés ou désactivés (FTP, TFTP, HTTP, bloc fonction dans l'équipement PAC M580).	10	Warning	18	`Major communication parameter update: XXXX YYYY` (`XXXX` = ID du paramètre de communication, `YYYY` = valeur). Par exemple : `major communication parameter update: FTP enable`.
Modification de l'état du port de commutation intégré : ● Liaison du port opérationnelle, liaison du port inopérante, ...	10	Warning	19	`ETHXX YYYY` (`XX` = numéro du port, `YYYY` = état du port). Par exemple : `ETH3 link down` (après une déconnexion du câble sur le port 3).
Modifications topologiques détectées : ● A partir de RSTP : modification du rôle du port ou modification de la racine.	10	Warning	20	`topology change detected`.
Erreur de vérification de l'intégrité : ● Erreur de signature numérique. ● Erreur d'intégrité uniquement (hachage).	10	Error	84	`XXXX integrity error` (`XXXX` identifie l'objet avec une erreur détectée). Par exemple : `firmware integrity error`.
Modifications majeures dans le système : ● Modification du mode d'exploitation du programme (`run`, `stop` ...).	13	Notice	85	`XXXX state update: YYYY` (`XXXX` identifie l'objet modifié, `YYYY` identifie le nouvel état). Par exemple : `PLC state update: RUN`.
Modifications majeures dans le système : ● Redémarrer après `RESET`	13	Warning	14	`Restart`
Modifications majeures dans le système : ● Modification du mode d'exploitation du programme : `PLC INIT`	13	Notice	85	`PLC INIT`
(1) REMARQUE : les termes gravité, Emergency, Alert, Critical, Error, Warning, Notice, Informational et Debug sont utilisés dans ce tableau comme des attributs des messages d'événement syslog et définis dans la spécification RFC 5424 de l'Internet Engineering Task Force (IETF).				

Description de l'événement	Catégorie	Gravité (1)	Type	Commentaire
Modifications majeures dans le système : ● Modification matérielle (insertion de carte SD, remplacement du module, ...).	13	Informational	26	`XXXX hardware update: YYYY` (`XXXX` identifie le matériel modifié, `YYYY` identifie la mise à jour). Par exemple : `PLC hardware update: SD card insertion`.
(1) REMARQUE : les termes gravité, Emergency, Alert, Critical, Error, Warning, Notice, Informational et Debug sont utilisés dans ce tableau comme des attributs des messages d'événement syslog et définis dans la spécification RFC 5424 de l'Internet Engineering Task Force (IETF).				

NOTE : les événements spécifiques de Control Expert non décrits dans le tableau précédent sont définis dans la colonne du profil utilisateur *(voir EcoStruxure™ Control Expert, Modes de fonctionnement)* **Editeur de sécurité** et envoyés via syslog.

Valeurs de catégorie de message Syslog, conformément à la spécification RFC 5424 associée au type d'événement :

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.
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 sécurité de message Syslog, conformément à la spécification RFC 5424 associée au type d'événement :

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

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

De nombreux serveurs syslog sont disponibles pour différents systèmes d'exploitation. Exemples de fournisseurs de services syslog :

WinSyslog : pour le système d'exploitation Windows.
Lien : *www.winsyslog.com/en/*.

Kiwi Syslog pour le système d'exploitation Windows.
Lien : *www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx*.

Splunk pour les systèmes d'exploitation Windows et Unix.
Lien : *www.splunk.com/*.

Rsyslog pour le système d'exploitation Unix.
Lien : *www.rsyslog.com/*.

Syslog-ng version Open Source du système d'exploitation Unix.
Lien : *www.balabit.com/network-security/syslog-ng/opensource-logging-system*.

Syslog Server version Open Source du 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, DTM et Control Expert.

La fonction de consignation des événements, l'adresse du serveur et le numéro de port sont configurés dans Control Expert comme ci-dessous, 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 → Diagnostic automate**.
3	Cochez la case **Consignation des événements** (décochée par défaut). **NOTE :** un projet avec cette case cochée ne peut être ouvert que dans Unity Pro (Control Expert) 10.0 ou version ultérieure.
4	Renseignez les champs **Adresse du serveur SYSLOG** et **Numéro du port du serveur SYSLOG**.
5	Sélectionnez **Générer** après avoir configuré ce paramètre (sélection de la commande **Analyser le projet** non obligatoire).

Diagnostic de la consignation des événements

Le tableau suivant indique le type de diagnostic de consignation des événements, disponible pour différents équipements :

Equipements	Informations de diagnostic
Control Expert	Si une erreur de communication avec le serveur syslog survient, elle est enregistrée dans le visualiseur d'événements. Pour activer le visualiseur d'événements dans Control Expert, cochez la case **Audit** dans l'onglet **Règles** de l'Editeur de sécurité *(voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.
DDT d'équipement BMENOC0301/11 (paramètre `SERVICE_STATUS2`)	Deux informations de diagnostic sont disponibles : **EVENT_LOG_STATUS :** valeur = 1 si le service de consignation des événements est opérationnel ou désactivé. 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 l'acquittement des messages TCP de la part du serveur syslog. valeur = 0 si l'acquittement est reçu.
DDT d'équipement de l'UC Modicon M580	
DDT d'équipement BMECXM	

Identification et authentification

Gestion des comptes

Schneider Electric recommande de suivre les consignes suivantes concernant la gestion des comptes :

- 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 d'administrateur pour installer des applications.

Gestion des commandes de compte utilisateur (UAC) (Windows 7)

Pour prévenir toute tentative non autorisée de modification du système, Windows 7 octroie aux applications les autorisations d'un utilisateur normal, sans droits d'administration. A ce niveau, les applications ne sont pas autorisées à modifier le système. L'UAC invite l'utilisateur à octroyer ou révoquer des droits supplémentaires à une application. Configurez l'UAC au niveau maximum. Au niveau maximum, l'UAC affiche un message demandant à l'utilisateur d'autoriser une application à effectuer des modifications exigeant des droits d'administration.

Pour accéder aux paramètres d'UAC dans Windows 7, sélectionnez **Panneau de configuration → Comptes et protection des utilisateurs → Comptes d'utilisateur → Modifier les paramètres du contrôle de compte d'utilisateur** ou saisissez **UAC** dans le champ de recherche du **menu Démarrer** de Windows 7.

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. Schneider Electric recommande de suivre les consignes suivantes :

- Activez l'authentification par mot de passe sur tous les serveurs Web et de messagerie, les CPU et les modules d'interface Ethernet.
- **Changez tous les mots de passe par défaut immédiatement après l'installation**, y compris ceux des éléments suivants :
  - comptes d'utilisateur et d'application sous 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 n'interfère pas avec la capacité d'un opérateur à répondre à un événement, tel qu'un arrêt d'urgence.
- Ne communiquez pas les mots de passe par e-mail ou par toute autre méthode non sécurisée sur Internet.

Gestion du protocole HTTP

Hypertext Transfer Protocol (HTTP) est le protocole qui est utilisé par le Web. Il est utilisé sur les systèmes de contrôle pour prendre en charge les serveurs Web intégrés aux produits de contrôle. Les serveurs Web Schneider Electric utilisent les communications HTTP pour afficher des données et envoyer des commandes via des pages Web.

Si le serveur HTTP n'est pas requis, désactivez-le. Sinon, utilisez le protocole HTTPS (*Hypertext Transfer Protocol Secure*), qui combine HTTP et un protocole cryptographique, au lieu de HTTP. 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.

Gestion du protocole SNMP

Le protocole *Simple Network Management Protocol* (SNMP) 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 PAC. Ce protocole est constitué de 3 parties :

- Gestionnaire : application qui gère les agents SNMP sur un réseau, par l'envoi de requêtes, la réception des réponses et l'écoute et le traitement des interruptions envoyées 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 être de tout type : routeurs, serveurs d'accès, commutateurs, ponts, hubs, PAC, lecteurs.
- Système de gestion du réseau (NMS) : terminal via lequel les administrateurs peuvent réaliser des tâches d'administration

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

Souvent, le protocole SNMP est automatiquement installé avec la propriété de lecture **publique** et la propriété d'écriture **privée**. Ce type d'installation permet à un utilisateur malveillant de s'authentifier sur un système et de créer un refus de service.

Pour réduire le risque d'attaque via SNMP, procédez comme suit :

- Si possible, désactivez SNMP v1 et v2, et utilisez SNMP v3 qui chiffre les mots de passe et les messages.
- Si SNMP v1 ou v2 est requis, utilisez les paramètres d'accès pour limiter les équipements (adresses IP) ayant accès au commutateur. Attribuez différents mots de passe de lecture et de lecture/écriture aux équipements.
- Modifiez les mots de passe par défaut de tous les équipements prenant en charge SNMP.
- Bloquez tout le trafic entrant et sortant SNMP à la périphérie du réseau de l'entreprise et du réseau des opérations de la salle de commande.
- Filtrez les commandes SNMP v1 et v2 entre le réseau de contrôle et le réseau des opérations d'une part, et certains hôtes d'autre part, ou envoyez-les via un autre réseau de gestion sécurisé.
- Contrôlez l'accès en identifiant l'adresse IP autorisée à interroger un équipement SNMP.

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

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

- **Application**
  La protection de l'application de l'UC et d'Control Expert par un mot de passe empêche tout téléchargement, modification ou ouverture indésirable de l'application (fichiers .STU et .STA). Pour plus d'informations, consultez la rubrique *Protection de l'application (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.
- **Section**
  La fonction de protection de sections est accessible dans l'écran **Propriétés** du projet en mode local. Elle permet de protéger les sections du programme. Pour plus d'informations, consultez la rubrique *Protection de sections et de 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.
- **Stockage de données**
  La protection du stockage de données par un mot de passe empêche toute intrusion dans la zone réservée au stockage des données dans la carte SD (si une carte valide est insérée dans l'UC). 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 mot de passe empêche tout téléchargement d'un micrologiciel malveillant dans l'UC. Pour plus d'informations, consultez la rubrique *Protection du micrologiciel (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.

Autorisations de contrôle

Editeur de sécurité Control Expert

Un outil de configuration de la sécurité permet de définir les utilisateurs du logiciel ainsi que leurs autorisations respectives. La sécurité d'accès Control Expert concerne le terminal sur lequel le logiciel est installé et non pas le projet, qui bénéficie d'un système de protection spécifique.

Pour plus d'informations sur l'éditeur de sécurité, consultez la section *Gestion de la sécurité d'accès (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.

Recommandation : définissez un mot de passe de super-utilisateur et limitez les autorisations des autres utilisateurs avec un profil restrictif.

Mode de programmation et de surveillance

Deux modes sont disponibles pour accéder à l'UC en mode **En ligne** :

- Mode **Programmation** : le programme de l'UC est modifiable. Lorsqu'un terminal est connecté à l'UC pour la première fois, l'UC est réservée ce qui empêche toute connexion à un autre terminal.
- Mode **Surveillance** : le programme de l'UC n'est pas modifiable, mais les variables le sont. Le mode de surveillance ne réserve pas l'UC. Une UC déjà réservée est accessible en mode de surveillance.

Pour choisir un mode dans 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)*.

Recommandation : réglez le mode d'accès à l'UC **En ligne** sur **Utiliser le mode de suivi**, si possible.

Protection des sections de programme

La fonction de protection des sections est accessible dans l'écran **Propriétés** du projet en mode local. Elle permet de protéger les sections du programme. Pour plus d'informations, consultez la rubrique *Protection de sections et de 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.

Recommandation : activez la protection des sections.

Protection de la mémoire de l'UC

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

NOTE : la protection de la mémoire n'est pas configurable sur les UC à redondance d'UC. Dans ces cas, utilisez la communication sécurisée IPsec.

La protection de la mémoire est activée comme suit :

- UC Modicon M340 : bit d'entrée. Pour plus d'informations, consultez la section *Configuration des processeurs Modicon M340 (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.
- UC Modicon M580 : bit d'entrée. Pour plus d'informations, consultez la section *Gestion de l'entrée Run/Stop (voir Modicon M580, Hardware, Reference Manual)*.
- UC Modicon Quantum : commutateur physique sur le module d'UC, qu'il soit d'entrée de gamme *(voir Quantum using EcoStruxure™ Control Expert, Hardware, Reference Manual)* ou haut de gamme *(voir Quantum using EcoStruxure™ Control Expert, Hardware, Reference Manual)*.
- UC Modicon Premium : bit d'entrée. Pour plus d'informations, consultez la section *Configuration des processeurs Premium (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.
- UC Modicon MC80 : bit d'entrée. Pour plus d'informations, consultez le manuel sur l'UC Modicon MC80.

Recommandation : activez la protection de la mémoire de l'UC, si possible.

Gestion de l'accès à distance aux modes Run/Stop

NOTE : Les UC à redondance d'UC n'autorisent pas l'accès à distance au mode Run/Stop. Dans ces cas, utilisez la communication IPsec sécurisée.

La gestion de l'accès à distance aux modes Run/Stop définit comment démarrer ou arrêter une UC à distance. Elle dépend de la plate-forme :

Modicon M580 : L'accès à distance aux modes Run/Stop de l'UC permet l'une des actions suivantes :

- Arrêt ou démarrage de l'UC à distance via une requête.
- Arrêt de l'UC à distance via une requête. Refus de démarrage de l'UC à distance via une requête (seule l'exécution contrôlée par l'entrée est possible si une entrée valide est configurée).
- Refus de démarrage ou d'arrêt de l'UC à distance via une requête.

Pour les options de configuration de l'UC qui permettent d'empêcher des commandes distantes d'accéder aux modes Run/Stop, consultez la section *Gestion de l'entrée Run/Stop (voir Modicon M580, Hardware, Reference Manual)*.

Modicon M340 : L'accès à distance aux modes Run/Stop de l'UC permet l'une des actions suivantes :
- ❍ Arrêt ou démarrage de l'UC à distance via une requête.
- ❍ Arrêt de l'UC à distance via une requête. Refus de démarrage de l'UC à distance via une requête (seule l'exécution contrôlée par l'entrée est possible si une entrée valide est configurée).

Reportez-vous à la section *Configuration des processeurs Modicon M340 (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.

Modicon Premium : L'accès à distance aux modes Run/Stop de l'UC permet l'une des actions suivantes :
- ❍ Arrêt ou démarrage de l'UC à distance via une requête.
- ❍ Arrêt de l'UC à distance via une requête. Refus de démarrage de l'UC à distance via une requête (seule l'exécution contrôlée par l'entrée est possible si une entrée valide est configurée).

Reportez-vous à la section *Configuration des processeurs Premium/Atrium (voir EcoStruxure™ Control Expert, Modes de fonctionnement)*.

Modicon Quantum : L'accès à distance aux modes Run/Stop de l'UC permet les actions suivantes :
- ❍ Arrêter ou lancer l'UC à distance via une requête.

Modicon MC80 : L'accès à distance aux modes Run/Stop de l'UC permet l'une des actions suivantes :
- ❍ Arrêt ou démarrage de l'UC à distance via une requête.
- ❍ Arrêt de l'UC à distance via une requête. Refus de démarrage de l'UC à distance via une requête (seule l'exécution contrôlée par l'entrée est possible si une entrée valide est configurée).
- ❍ Refus de démarrage ou d'arrêt de l'UC à distance via une requête.

Consultez la section *Configuration des processeurs Modicon MC80* dans le manuel utilisateur du MC80.

Recommandation : désactivez le démarrage ou l'arrêt de l'UC à distance à la demande.

Accès aux variables d'UC

Recommandation : pour protéger les données de l'UC contre les accès non autorisés en lecture ou en écriture, procédez comme suit :
- Utilisez des données non localisées.
- Configurez Control Expert pour qu'il ne stocke que les variables IHM en sélectionnant **Outils → Options du projet... → Données intégrées de l'automate → Dictionnaire de données → Variables HMI seulement**.
  Variables HMI seulement ne peut être sélectionné que si **Dictionnaire de données** est sélectionné.
- Déclarez comme *HMI* les variables accessibles à partir de la HMI 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.

Gestion des vérifications de l'intégrité des données

Introduction

Vous pouvez utiliser une fonctionnalité de vérification d'intégrité dans Control Expert sur un PC autorisé pour éviter toute modification des fichiers et logiciels Control Expert par un virus ou un logiciel malveillant provenant d'Internet.

Exécution d'une vérification d'intégrité

Control Expert n'effectue une vérification d'intégrité **que** lors de la première exécution de Control Expert. La vérification d'intégrité du micrologiciel PAC s'effectue automatiquement après le chargement d'un nouveau micrologiciel ou le redémarrage du PAC. Pour effectuer une vérification d'intégrité manuelle dans Control Expert, procédez comme suit :

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'effectue en arrière-plan, sans nuire aux performances de votre application. Control Expert crée un journal des connexions réussies et infructueuses aux composants. Ce fichier indique l'adresse IP, la date et l'heure, ainsi que le résultat de la connexion. **NOTE :** si une vérification d'intégrité indique une tentative infructueuse de connexion à un composant, le **Visualiseur d'événement** affiche un message. Cliquez sur **OK**. Corrigez manuellement les éléments dans le journal.

Gestion de la carte SD

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

La signature de la carte SD est gérée par les fonctions `SIG_WRITE` *(voir EcoStruxure™ Control Expert, Système, Bibliothèque de blocs)* et `SIG_CHECK` *(voir EcoStruxure™ Control Expert, Système, Bibliothèque de blocs)*.

Chapitre 3
Services de cybersécurité par plate-forme

Introduction

Ce chapitre répertorie les principaux services de cybersécurité disponibles par plate-forme et indique où trouver des informations détaillées dans l'aide de Control Expert.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Services de cybersécurité

Présentation

Le logiciel, le DTM et les équipements fournissent des services de cybersécurité à un système global. Les services de cybersécurité disponibles sont répertoriés pour les éléments suivants :

- Logiciel Control Expert *(voir page 58)*
- UC Modicon M340 *(voir page 59)*
- UC Modicon M580 *(voir page 60)*
- Modicon Momentum (services de cybersécurité non implémentés)
- UC Modicon Quantum et modules de communication *(voir page 61)*
- Modules Modicon X80 *(voir page 61)*
- UC Modicon Premium/Atrium *(voir page 63)*

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

- Désactivation des services inutilisés *(voir page 23)*
- Contrôle d'accès *(voir page 24)*
- Communication sécurisée *(voir page 26)*
- Consignation des événements *(voir page 41)*
- Authentification *(voir page 49)*
- Autorisations *(voir page 53)*
- Vérifications d'intégrité *(voir page 56)*

Services de cybersécurité dans les logiciels Unity Pro/Control Expert

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

Services de cybersécurité disponibles dans les logiciels Control Expert :

Logiciel	Services de cybersécurité							
Référence	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	Communication sécurisée avec confidentialité	Consignation des événements	Authentification	Autorisations	Vérifications d'intégrité
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

X Disponible, au moins un service implémenté.
– Non disponible
N.A. Non applicable

Services de cybersécurité sur l'UC Modicon M340

Version minimale du micrologiciel et services de cybersécurité disponibles sur l'UC Modicon M340 :

UC		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	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 implémenté.
– Non disponible

Services de cybersécurité sur l'UC Modicon M580 :

Version minimale du micrologiciel et services de cybersécurité disponibles sur l'UC Modicon M580 :

UC		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	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
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 implémenté.
– Non disponible

Services de cybersécurité sur l'UC et les modules Modicon Quantum

Version minimale du micrologiciel et services de cybersécurité disponibles sur l'UC Modicon Quantum :

UC		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	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	–
140CPU67861	3.20	X	X	–	–	X	X	–
X Disponible, au moins un service implémenté. **–** Non disponible								

Modules Modicon Quantum prenant en charge les services de cybersécurité :

Module		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	Consignation des événements	Authentification	Autorisations	Vérifications 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 implémenté. **–** Non disponible								

Services de cybersécurité sur les modules Modicon X80

Modules Modicon X80 prenant en charge les services de cybersécurité :

Module		Services de cybersécurité							
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	Communication sécurisée 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 implémenté.
– Non disponible

Services de cybersécurité sur l'UC et les modules Modicon Premium/Atrium

Version minimale du micrologiciel et services de cybersécurité disponibles sur l'UC Modicon Premium/Atrium :

UC		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	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	–
TSXP571634M TSXP572634M TSXP573634M (via le 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 implémenté. **–** Non disponible								

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

Module		Services de cybersécurité						
Référence	Version min. micrologiciel	Désactivation des services inutilisés	Contrôle d'accès	Communication sécurisée	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 implémenté. **–** Non disponible								

Services de sécurité Modicon M340

Présentation

Les paramètres des services de sécurité de communication sont fournis pour l'UC Modicon M340 dans différents manuels et décrits dans la rubrique suivante.

UC Modicon M340 avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Paramètres de configuration de la messagerie (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Services de sécurité Modicon M580

UC Modicon M580

Les paramètres de communication liés à la cybersécurité sont décrits dans la rubrique *Onglet Sécurité (voir Modicon M580, Hardware, Reference Manual)*.

Services de sécurité Modicon Quantum

Présentation

Les paramètres des services de sécurité de l'UC Modicon Quantum et des modules Ethernet sont fournis dans différents manuels et décrits dans les rubriques suivantes.

UC Modicon Quantum avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (activation/désactivation de HTTP, FTP et TFTP) (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Contrôle d'accès : Consultez la section *Configuration de la messagerie de l'automate Ethernet Modicon Quantum avec Control Expert (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Module 140 NOC 771 0x

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (activation/désactivation de HTTP, FTP et TFTP) (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Contrôle d'accès : Consultez la section *Configuration du contrôle d'accès (voir Quantum sous 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 dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Quantum EIO, Réseau de contrôle, Guide d'installation et de configuration)*.

Contrôle d'accès : Consultez la section *Configuration du contrôle d'accès (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 dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Quantum EIO, Réseau de contrôle, Guide d'installation et de configuration)*.

Contrôle d'accès : Consultez la section *Configuration du contrôle d'accès (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 dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (activation/désactivation de HTTP, FTP et TFTP) (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*, la section *Sécurité (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)* et la section *Définition des mots de passe HTTP et d'écriture (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Module 140 NWM 100 00

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (activation/désactivation de HTTP, FTP et TFTP) (voir Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Services de sécurité Modicon X80

Présentation

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

Module BMECXM0100

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

Module BMENOC0301/11

Les paramètres de communication liés à la cybersécurité sont décrits dans la section *Configuration des services de sécurité (voir Modicon M580, BMENOC0301/0311 Ethernet Communications Module, Installation and Configuration Guide)*.

Module BMX NOC 0401.2

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Configuration du contrôle d'accès (voir Modicon M340, Module de communication Ethernet BMX NOC 0401, Manuel de l'utilisateur)*.

Module BMX NOE 0100.2 et BMX NOE 0110.2

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Paramètres de configuration de la messagerie (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Module BMX PRA 0100

Le BMX PRA 0100 est configuré en tant qu'UC Modicon M340. Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Paramètres de configuration de la messagerie (voir Modicon M340 pour Ethernet, Processeurs et modules de communication, Manuel utilisateur)*.

Services de sécurité Modicon Premium/Atrium

Présentation

Les paramètres des services de sécurité de l'UC Modicon Premium/Atrium et des modules Ethernet sont fournis dans différents manuels et décrits dans les rubriques suivantes.

UC Modicon Premium/Atrium avec ports Ethernet intégrés

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Paramètres de configuration du service de sécurité (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Configuration de la messagerie TCP/IP (TSX P57 6634/5634/4634) (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

UC Modicon Premium/Atrium via les ports ETY

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Paramètres de configuration du service de sécurité (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Configuration de la messagerie TCP/IP (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

Module TSX ETC 101.2

Les paramètres de communication liés à la cybersécurité sont décrits dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Sécurité (voir Premium sous EcoStruxure™ Control Expert, Module de communication Ethernet TSX ETC 101 , Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Configuration du contrôle d'accès (voir Premium sous 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 dans les rubriques ci-dessous :

Communication Ethernet : Consultez la section *Paramètres de configuration du service de sécurité (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

Contrôle d'accès : Consultez la section *Configuration de la messagerie TCP/IP (voir Premium et Atrium sous EcoStruxure™ Control Expert, Modules réseau Ethernet, Manuel utilisateur)*.

Glossaire

!

%I

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

%IW

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

%M

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

%MW

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

%Q

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

%QW

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

%SW

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

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.

Adresse IP

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.

Anneau principal

Anneau principal d'un réseau EthernetRIO. Cet anneau contient des modules RIO et un rack local (contenant une UC (CPU) avec un service de scrutation Ethernet) ainsi qu'un module d'alimentation.

Anneau secondaire

Réseau Ethernet comportant une boucle reliée à un anneau principal, par l'intermédiaire 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 d'E/S distantes (RIO) ou distribués.

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. En voici la syntaxe : `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 réponse de l'application). Temps de réaction d'une application CPU à une entrée donnée. Le temps ART est mesuré à partir de l'activation sur l'automate CPU 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 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.

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 topographie se compose d'un rack local (contenant une UC (CPU) avec un service de scrutation d'E/S distantes (Ethernet) et une ou 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.

Commutateur

Equipement 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

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.

connexion de classe 1

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

connexion de classe 3

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

Connexion optimisée du rack

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.

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 un processus, par opposition aux systèmes de contrôle de 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.

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.

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 réglée sur 1 lorsque la valeur en cours est égale à la valeur de présélection.

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.

Equipement d'E/S Ethernet M580

Equipement Ethernet qui assure la récupération automatique du réseau et des performances RIO déterministes. Le délai nécessaire pour résoudre 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 communication. Les équipements d'E/S M580Ethernet sont les suivants :

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

Equipement 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

Equipement Ethernet (appareil Schneider Electric, PC, serveur et autre équipement tiers) qui prend en charge l'échange avec une CPU ou un autre service de scrutation d'E/S Ethernet.

équipement prêt

Equipement 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 Schneider ElectricEtherNet/IP qui permet à un scrutateur de prendre le rôle d'un adaptateur. L'esclave local permet au module de publier des données par le biais de connexions de messagerie implicite. Un esclave local s'utilise généralement pour des échanges poste à poste entre des PAC.

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.

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.

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*IEC 61131-3 (langage à blocs fonction). Langage de programmation graphique qui fonctionne comme un diagramme de flux. Par l'ajout de blocs logiques simples (`AND`, `OR`, etc.), chaque fonction ou bloc fonction du programme est représenté(e) sous cette forme graphique. 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*. 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 le standard générique pour l'accès aux données entre systèmes hôtes et instruments de terrain intelligents. Un hôte peut être une application logicielle exécutée sur l'ordinateur portable ou le terminal portatif d'un technicien ou sur le système de contrôle de processus ou de gestion d'actifs d'un site industriel, ou encore sur tout système utilisant une plateforme de contrôle quelconque.

Horodatage applicatif

La solution d'horodatage applicatif permet d'accéder au buffer des événements horodatés à l'aide d'un système SCADA qui ne prend pas en charge l'interface OPC DA. Dans ce cas, les blocs fonction dans l'application PLC Control Expert lisent les événements dans le buffer et les formatent pour les envoyer au système SCADA.

Horodatage système

xxx

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

IGMP

Acronyme de *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 puissance 15) à (2 puissance 15) - 1.

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

IODDT

(*type de données dérivé d'E/S*) Type de données structuré représentant un module, ou le canal d'une CPU. Chaque module expert possède ses propres IODDT.

IPsec

(abréviation de *Internet Protocol security*, sécurité IP). Ensemble de protocoles standards libres, qui permettent de protéger la sécurité et la confidentialité des sessions de communication IP du trafic entre modules utilisant IPsec. Ces protocoles ont été développés par le groupe IETF (Internet Engineering Task Force). 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.

L

Langage en blocs fonctionnels

Voir FBD.

LD

Acronyme de *Ladder Diagram*IEC 61131-3 (schéma à contacts). Langage de programmation représentant les instructions à exécuter sous forme de schémas graphiques très proches d'un schéma électrique (contacts, bits de sortie, 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.

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 Etendu

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.

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.schneider-electric.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.

NTP

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

Nuage DIO

Groupe d'équipements distribués qui ne sont pas requis pour prendre en charge le protocole RSTP. DIOLes nuages nécessitent uniquement une connexion en fil de cuivre (sans anneau). Ils peuvent être connectés à des ports cuivre sur des commutateurs double anneau (DRS) ou directement à l'UC (CPU) ou aux modules de communication Ethernetdu rack local . Les nuages DIOne peuvent **pas** être connectés à des *sous-anneaux*.

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 de 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 Service

Port Ethernet dédié sur les modules M580RIO. 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 connecter l'IHM/Control Expert/ConneXview à l'UC (CPU)
- 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

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.

R

rack local

Rack M580 contenant l'CPU et un module d'alimentation. Un rack local se compose d'un ou de deux racks : le rack principal et le rack étendu qui appartient à la même famille que le rack principal. Le rack étendu est facultatif.

Redondance d'UC

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

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.

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 distribuées. Les équipements connectés à ce réseau suivent des règles spécifiques pour permettre le déterminisme des E/S distantes.

réseau d'équipements

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

Réseau d'exploitation

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

Réseau de contrôle

Réseau Ethernet contenant des automates (PAC), des systèmes SCADA, un serveur NTP, des ordinateurs (PC), des systèmes AMS, des commutateurs, etc. Deux types de topologies sont pris en charge :

- à plat : tous les modules et équipements du réseau appartiennent au même sous-réseau.
- à 2 niveaux : le réseau est divisé en un réseau d'exploitation et un réseau intercontrôleurs. Ces deux réseaux peuvent être indépendants physiquement, mais ils sont généralement liés par un équipement de routage.

Réseau DIO

Réseau contenant des équipements distribués dans lequel la scrutation d'E/S est effectuée par une UC CPU dotée d'un service de scrutation des E/S distribuées DIO sur le rack local. Dans un réseau DIO, le trafic réseau est traité après le trafic RIO, qui est prioritaire dans un réseau RIO.

Réseau DIO isolé

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

Réseau EIO

Abréviation de *Ethernet I/O* (E/S Ethernet). Réseau Ethernet contenant 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) ConneXium étendu

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

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

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

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.

Scrutateur d'E/S

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).

Service de scrutation d'E/S Ethernet

Service de scrutation d'E/S Ethernet intégré aux CPU M580 qui gère les équipements distribués et les stations RIO sur un réseau d'équipements M580.

Service de scrutation DIO Ethernet

Service de scrutation DIO intégré aux CPU M580 qui gère les équipements distribués sur 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, de manière structurée, le fonctionnement d'un automate (CPU) séquentiel. Cette description graphique du fonctionnement séquentiel du processeur et des différentes situations qui en découlent est réalisée 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*. Processus de détermination de l'ordre des événements dans un système industriel et corrélation de ces événements à une horloge en temps réel.

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.

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.

Station 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.

T

T->O

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

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.

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.

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

Acronyme de *time of day*. Le type `TOD`, 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 déclaré sous la forme suivante : xxxxxxxx:
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`.

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.

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.

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 préféré aux autres protocoles 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.

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 de mémoire de type `BOOL`, `WORD`, `DWORD`, etc. 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

D

E

H

L

M

N

P

Q

R

S

T

U

V

X