Masterpact MTZ

Guide de cybersécurité

06/2017

DOCA0122FR-01

www.schneider-electric.com

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.

AVIS CONCERNANT LA CYBERSÉCURITÉ

⚠ AVERTISSEMENT

RISQUES POUVANT AFFECTER LA DISPONIBILITÉ, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DU SYSTÈME

- Modifiez le mot de passe par défaut afin d'empêcher tout accès non autorisé aux paramètres et aux informations du dispositif.
- Désactivez les ports et services inutilisés, ainsi que les comptes par défaut, pour réduire le risque d'attaques malveillantes.
- Protégez les appareils en réseau par plusieurs niveaux de cyberdéfense (pare-feu, segmentation du réseau, détection des intrusions et protection du réseau).
- Respectez les bonnes pratiques de cybersécurité (par exemple : moindre privilège, séparation des tâches) pour réduire les risques d'intrusion, la perte ou l'altération des données et journaux, ou l'interruption des services.

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

A propos de ce manuel

Présentation

Objectif du document

Ce guide fournit des informations sur la cybersécurité des disjoncteurs Masterpact™ MTZ avec unités de contrôle Micrologic™ X, pour aider les concepteurs et les utilisateurs de système à mettre en place un environnement sécurisé d'exploitation du produit.

Ce guide n'aborde pas la question générique de la sécurisation de votre réseau de contrôle industriel ou de votre réseau Ethernet d'entreprise. Pour une présentation générale des menaces de cybersécurité et des moyens de protection disponibles, consultez le document *How Can I Reduce Vulnerability to Cyber Attacks?*.

NOTE : dans ce guide, le terme **sécurité** fait référence à la cybersécurité.

Champ d'application

Les informations fournies dans ce guide concernent les disjoncteurs Masterpact MTZ avec unités de contrôle Micrologic X.

Documents connexes

Titre du document	Référence
Unité de contrôle Micrologic X - Guide utilisateur	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note

Vous pouvez télécharger ces publications ainsi que d'autres informations techniques sur notre site Web : *http://www.schneider-electric.com/en/download*.

Marques commerciales

Toutes les marques appartiennent à Schneider Electric Industries SAS ou à ses filiales.

Chapitre 1
Introduction à la cybersécurité

Présentation

Ce chapitre fournit des informations générales sur la stratégie de cybersécurité de Schneider Electric et explique l'intérêt de la cybersécurité pour les disjoncteurs Masterpact MTZ avec unité de contrôle Micrologic X.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Introduction à la cybersécurité

Présentation

La cybersécurité vise à protéger votre réseau de communication et tous les équipements qui y sont connectés, contre les attaques susceptibles de perturber les opérations (disponibilité), de modifier des informations (intégrité) ou de divulguer des informations confidentielles (confidentialité). Son objectif consiste à augmenter les niveaux de protection des informations et des actifs physiques contre le vol, la corruption, l'utilisation abusive ou les accidents, tout en maintenant l'accès pour les utilisateurs cibles. La cybersécurité revêt de nombreux aspects, comme la conception de systèmes sécurisés, la restriction de l'accès à l'aide d'outils physiques et numériques, l'identification des utilisateurs, ainsi que la mise en œuvre de procédures de sécurité et de bonnes pratiques.

Consignes de Schneider Electric

Outre les recommandations fournies dans ce guide et qui sont propres aux disjoncteurs Masterpact MTZ, vous devez adopter l'approche de défense en profondeur de Schneider Electric concernant la cybersécurité. Cette approche est décrite dans la note technique suivante :

- *How Can I Reduce Vulnerability to Cyber Attacks?*

De plus, de nombreuses ressources et informations à jour sur la cybersécurité sont disponibles sur une page dédiée du site Web global de *Schneider Electric*.

Intérêt de la cybersécurité pour les disjoncteurs Masterpact MTZ

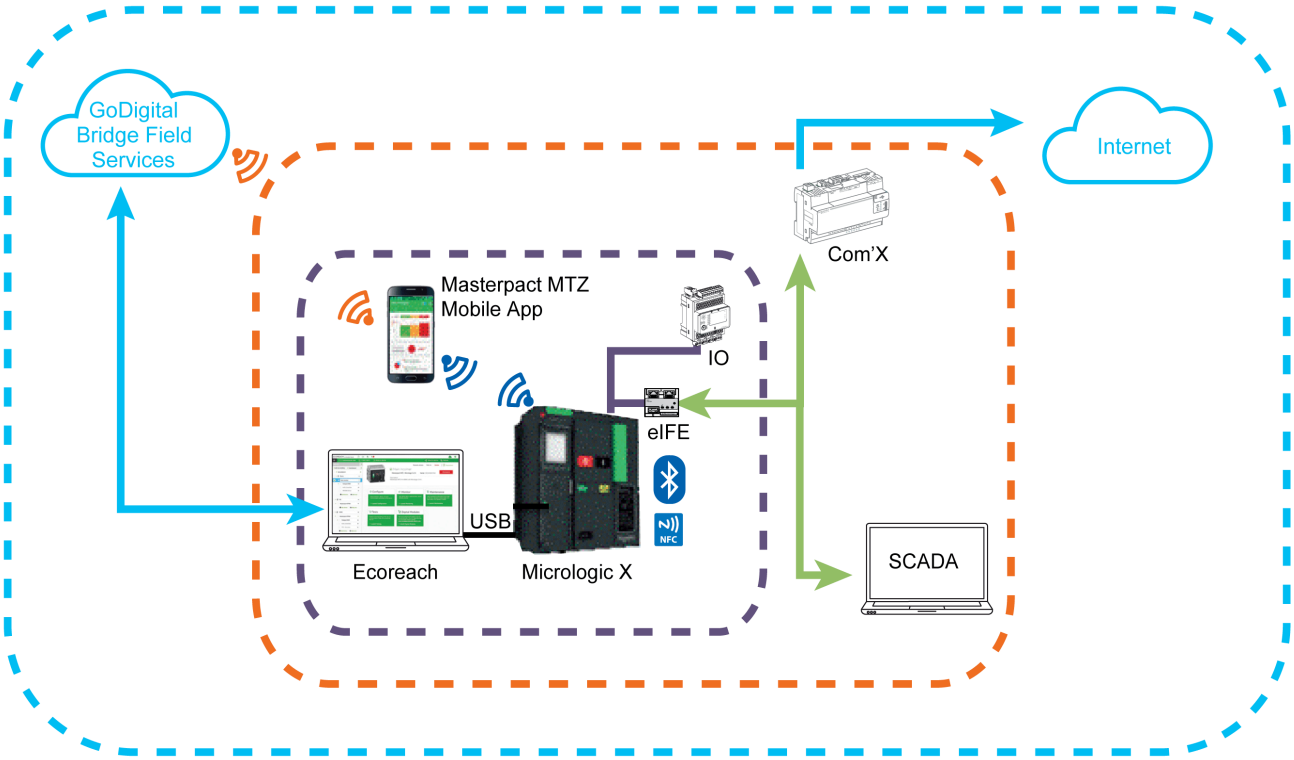
Présentation

Le disjoncteur Masterpact MTZ est un élément clé d'une usine ou d'un équipement, car il contrôle l'alimentation du système, assure la protection électrique et fournit des informations sensibles.

Les disjoncteurs Masterpact MTZ dotés de fonctions de communication assurent également un accès continu aux fonctions de contrôle en temps réel et aux données de surveillance. Ces fonctionnalités permettent de gérer votre système avec une efficacité et une flexibilité accrues. Toutefois, elles vous exposent potentiellement aux cyberattaques.

Disjoncteur Masterpact MTZ et environnement d'exploitation

La figure suivante montre les différents mots de communication avec l'unité de contrôle Micrologic X qui assure l'interface avec le disjoncteur Masterpact MTZ.



L'unité fonctionnelle intelligente (IMU) Masterpact MTZ englobe le disjoncteur, l'unité de contrôle Micrologic X, ainsi que les modules ULP, l'interface de communication et le module IO associés.

Pour communiquer avec le disjoncteur Masterpact MTZ via son unité de contrôle Micrologic X, les voies suivantes sont disponibles :

- Interface homme-machine (IHM) Micrologic X
- Connexion NFC sans fil à partir d'un smartphone
- Connexion Bluetooth Low Energy (BLE) sans fil à partir d'un smartphone
- Connexion au port USB mini-B de l'unité de contrôle Micrologic X depuis :
  - Un PC exécutant le logiciel Ecoreach
  - Un smartphone exécutant l'application mobile Masterpact MTZ
- Connexion Ethernet via le réseau de contrôle industriel (IC) lorsque l'interface de communication est présente
- Connexion Modbus-SL via le réseau de contrôle industriel (IC) lorsque l'interface IFM est présente

Vulnérabilité du système aux cyberattaques

Chacune des voies de communication indiquées ci-dessus représente une vulnérabilité potentielle dans votre système. Ce guide fournit des consignes pour sécuriser ces voies et éviter les attaques intentionnelles ou une mauvaise utilisation accidentelle.

Chapitre 2
Recommandations de cybersécurité pour la conception, la planification et l'installation de système

Présentation du chapitre

Ce chapitre fournit des informations importantes à prendre en compte lors des phases de conception, de planification et d'installation d'un réseau de contrôle industriel (IC) comprenant l'unité fonctionnelle intelligente (IMU) Masterpact MTZ. Les recommandations et consignes dans ce chapitre visent à mettre en place un environnement d'exploitation sécurisé.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Identification et protection des informations et opérations sensibles

Présentation

Lors de la planification et de la conception d'un réseau de contrôle industriel, il est important d'identifier les informations essentielles à vos opérations. Une fois identifiées, ces informations sensibles doivent être protégées.

En général, les informations sensibles incluent :
- les informations permettant d'accéder à votre installation et à votre réseau de contrôle industriel ;
- les informations concernant les opérations, accessibles via l'IMU Masterpact MTZ.

Il vous revient de déterminer comment analyser et utiliser ces informations au mieux des intérêts de votre organisation.

Informations sur le réseau de communication de l'entreprise

Les informations sensibles utilisées pour accéder à votre installation et à votre réseau de contrôle incluent :
- l'architecture de votre système ;
- les adresses IP ou MAC des équipements de communication connectés ;
- les numéros de port utilisés pour la communication Ethernet ;
- les ID et mots de passe des utilisateurs.

Cette liste n'est pas exhaustive et il est important de prendre en compte toutes les informations de votre entreprise qui peuvent faciliter l'accès aux systèmes critiques.

Contrôle d'accès

Une partie importante de la cybersécurité consiste à concevoir une stratégie de contrôle d'accès efficace. Le contrôle d'accès vise à identifier des employés ou des groupes d'utilisateurs au sein de votre entreprise, et à déterminer le type d'accès dont ils ont besoin pour effectuer leurs tâches efficacement.

Récapitulatif des informations et opérations accessibles via chaque chemin d'accès

Selon l'interface ou le chemin de communication utilisé pour accéder à l'unité fonctionnelle intelligente (IMU) Masterpact MTZ, les opérations d'information et de contrôle disponibles varient. Le tableau suivant récapitule l'accès aux opérations d'information et de contrôle :

Opérations d'information et de contrôle	Accès local				Accès distant
	IHM Micrologic X	NFC	Bluetooth low energy	USB	Ethernet / Modbus-SL
Surveillance des données	Lecture	Lecture	Lecture	Lecture	Lecture
Paramètres de protection	Lecture/Ecriture	Lecture	Lecture/Ecriture	Lecture/Ecriture	Lecture/Ecriture
Autres paramètres	Lecture/Ecriture	Lecture	Lecture/Ecriture	Lecture/Ecriture	Lecture/Ecriture
Ouverture/Fermeture/Réinitialisation	Non	Non	Oui	Oui	Oui

Pour plus d'informations sur la protection de chaque interface de communication et de chaque chemin d'accès, consultez les recommandations pour l'accès local *(voir page 19)* ou l'accès distant *(voir page 27)* selon le cas.

Conception d'une stratégie de mot de passe

Présentation

Une stratégie de mot de passe bien conçue constitue votre première ligne de défense contre les cyberattaques.

Dans les installations comprenant le disjoncteur Masterpact MTZ avec unité de contrôle Micrologic X, les mots de passe sont requis pour :

- exécuter certaines tâches sur l'unité de contrôle Micrologic X, quel que soit le mode d'accès (Ethernet/Modbus-SL, connexion USB ou Bluetooth) ;
- se connecter au PC qui exécute le logiciel Ecoreach ;
- se connecter aux pages Web IFE et EIFE.

Mot de passe pour les paramètres et contrôles critiques de Micrologic X

Lorsque vous accédez à l'unité de contrôle Micrologic X, les commandes qui modifient le comportement du disjoncteur Masterpact MTZ requièrent un mot de passe. Par exemple, pour modifier les paramètres de protection ou déclencher le disjoncteur, vous devez avoir le mot de passe de l'unité de contrôle Micrologic X.

Quatre mots de passe sont définis, chacun correspondant à un niveau.

Chaque niveau est attribué à un rôle :

- Les niveaux 1, 2 et 3 sont utilisés pour les rôles généraux, par exemple un rôle opérateur.
- Le niveau 4 est le niveau administrateur. Le niveau administrateur est requis pour écrire des paramètres dans les unités de contrôle Micrologic X à l'aide du logiciel Ecoreach.

En cas de connexion via l'application Masterpact MTZ Mobile App ou le logiciel Ecoreach, l'utilisateur est invité à entrer l'un de ces mots de passe.

En cas de connexion à partir d'une interface de contrôle et de surveillance à distance, le mot de passe doit faire partie de la demande de communication.

Le mot de passe est constitué de quatre caractères ASCII. Il est sensible à la casse et autorise les caractères suivants :

- les chiffres compris entre 0 et 9 ;
- les lettres minuscules de a à z ;
- les lettres majuscules de A à Z.

Ces mots de passe doivent être modifiés régulièrement après la première installation du disjoncteur Masterpact MTZ, à l'aide du logiciel Ecoreach. Ils ne doivent être communiqués qu'à un nombre limité d'utilisateurs approuvés. Le cas échéant, respectez les recommandations suivantes de la stratégie de mot de passe.

ID utilisateur et mots de passe pour PC en réseau

Les PC qui exécutent le logiciel Ecoreach ou qui accèdent à l'unité de contrôle Micrologic X par d'autres moyens (pages Web IFE ou EIFE, ou bien SCADA par exemple) doivent demander un identifiant et un mot de passe aux utilisateurs. Vous devez vérifier que les utilisateurs définissent des mots de passe forts et qu'ils les modifient régulièrement. De plus, vous devez définir un temporisateur pour verrouiller l'écran du PC automatiquement après une période d'inactivité.

Un mot de passe fort comprend des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, lorsqu'ils sont disponibles. Il doit compter au minimum 10 caractères.

Consultez les recommandations suivantes concernant la stratégie de mot de passe.

Mots de passe pour les pages Web IFE et EIFE

Les utilisateurs utilisent un identifiant et un mot de passe pour se connecter aux pages Web IFE et EIFE. Ils doivent modifier leur mot de passe après leur première connexion aux pages Web IFE et EIFE.

Vous devez identifier les utilisateurs qui, au sein de votre organisation, ont besoin de se connecter aux pages Web IFE et EIFE, et respecter les recommandations suivantes de la stratégie de mot de passe.

Recommandations de cybersécurité concernant la stratégie de mot de passe

La stratégie de mot de passe est l'un des piliers de la stratégie de cybersécurité. Une bonne stratégie de mot de passe :

- utilise des mots de passe forts ;
- implique une modification régulière des mots de passe ;
- interdit la réutilisation d'anciens mots de passe ;
- rappelle régulièrement aux utilisateurs les bonnes pratiques concernant les mots de passe.

Pour protéger votre PC et tous les logiciels qui s'exécutent dessus, vous devez au minimum :

- utiliser des mots de passe forts ;
- définir une longueur minimale de 10 caractères pour les mots de passe ;
- régler la période de validité des mots de passe entre 3 et 180 jours ;
- conserver l'historique des huit derniers mots de passe et interdire leur réutilisation.

Tous les utilisateurs doivent connaître les bonnes pratiques concernant les mots de passe, à savoir :

- Ne partagez pas les mots de passe personnels.
- N'affichez pas les mots de passe lors de leur saisie.
- Ne communiquez pas les mots de passe par e-mail ou par d'autres moyens.
- N'enregistrez pas les mots de passe sur les PC ou d'autres équipements.

Formation

Présentation

La formation et l'implication des employés constituent des éléments clés d'une stratégie de cybersécurité. Vous devez vérifier que tous les utilisateurs autorisés à accéder au réseau de contrôle de votre installation connaissent la stratégie de protection des informations de l'entreprise. Vous devez également vous assurer qu'ils ont suivi la formation adéquate pour effectuer leurs tâches conformément à cette stratégie.

En particulier, les utilisateurs doivent connaître les bonnes pratiques suivantes (et faire l'objet de rappels réguliers sur ce sujet) :

- Ne divulguez pas d'informations confidentielles ou sensibles, comme les mots de passe ou les codes d'accès des équipements ou des locaux sous clé.
- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Vérifiez que les smartphones utilisés pour accéder au système ne quittent jamais les utilisateurs et ne sont pas piratables sur Bluetooth ou sur Internet.
- Ne contournez pas les stratégies de sécurité pour des raisons de commodité.

Pour plus d'informations sur la conception et la mise en œuvre d'une bonne stratégie de formation, consultez le document *How Can I Reduce Vulnerability to Cyber Attacks?*.

Chapitre 3
Recommandations de cybersécurité pour l'accès local

Présentation du chapitre

Ce chapitre répertorie les chemins d'accès local au disjoncteur Masterpact MTZ. Il fournit également des recommandations pour sécuriser ces chemins d'accès. Ces éléments importants sont à prendre en compte pour l'exploitation.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Restriction de l'accès local au disjoncteur Masterpact MTZ

Présentation

L'unité fonctionnelle intelligente (IMU) Masterpact MTZ offre des possibilités d'accès local et distant. Vous devez vérifier que seuls les utilisateurs autorisés bénéficient de droits d'accès.

Accès local au disjoncteur Masterpact MTZ

L'accès local à l'unité fonctionnelle intelligente Masterpact MTZ offre plusieurs possibilités d'accès aux informations concernant le système et de contrôle de ce dernier.

Il est donc important de restreindre l'accès local au disjoncteur Masterpact MTZ en l'installant dans un local sous clé pour éviter :

- tout accès non autorisé à l'IHM Micrologic X, avec le risque de modification de paramètres à partir de l'IHM ;
- tout accès non autorisé à la communication Bluetooth sans fil, avec le risque de modification de paramètres à partir de l'application Masterpact MTZ Mobile App ;
- tout accès non autorisé à la communication NFC sans fil, avec le risque de divulgation de données ;
- toute connexion non autorisée par le mini-port USB de l'unité de contrôle Micrologic X, avec le risque de modification de paramètres à partir du logiciel Ecoreach ou d'un smartphone avec Masterpact MTZ Mobile App ;
- tout accès non autorisé au module IO, avec le risque de modification des paramètres de commutation de l'application prédéfinie utilisée.

Il est également important de mettre en œuvre des règles d'accès au local verrouillé. En particulier, vous devez vérifier que :

- le local est maintenu sous clé à tout moment ;
- le local est équipé d'un système d'authentification et d'autorisation ;
- seul le personnel autorisé dispose d'une clé ou du code d'accès ;
- les câbles du réseau de communication qui entrent dans le local et les ports de connexion sur les équipements de communication hors de la salle sont protégés ;
- tous les équipements (PC, smartphones et tablettes) qui ont accès à l'unité de contrôle Micrologic X bénéficient d'une protection renforcée conformément aux dernières consignes en date du fournisseur.

Lorsque le disjoncteur Masterpact MTZ est installé dans un local verrouillé, vous devez mettre en place une procédure d'ouverture d'urgence. Par exemple :

- équipez ce local d'au moins un bouton d'arrêt d'urgence accessible depuis l'extérieur ;
- équipez le disjoncteur d'un déclencheur voltmétrique à manque de tension MN (système à sécurité positive).

Recommandations pour protéger l'accès local à l'IHM Micrologic X

Fonctions accessibles à partir de l'IHM

Toute personne ayant accès à l'armoire hébergeant le disjoncteur Masterpact MTZ a accès à l'IHM sur l'unité de contrôle Micrologic X.

Certaines fonctions critiques, comme les paramètres de protection de l'équipement, sont configurables à l'aide de l'IHM Micrologic X..

Recommandations pour protéger l'accès par l'IHM Micrologic X

L'IHM Micrologic X n'est pas protégée par mot de passe et n'offre aucune protection physique empêchant l'accès à l'afficheur. Par conséquent, pour protéger l'accès à l'IHM, vous devez effectuer les opérations suivantes :

- Installez le disjoncteur Masterpact MTZ dans un local verrouillé.
- Maintenez ce local verrouillé à tout moment.
- Ne donnez la clé ou le code d'accès qu'aux personnes autorisées.

Pour plus d'informations sur la protection de l'accès au disjoncteur Masterpact MTZ, consultez la section Mise en œuvre d'une stratégie d'accès restreint *(voir page 20)*.

Verrouillage des paramètres de protection

Vous pouvez verrouiller les paramètres de protection du disjoncteur Masterpact MTZ pour empêcher leur modification locale sur l'IHM. Par défaut, la modification des paramètres de protection à partir de l'IHM est autorisée.

Il est recommandé de désactiver la modification locale des paramètres de protection sur l'IHM, si vous n'utilisez pas cette fonction. Pour plus d'informations, consultez le document *Unité de contrôle Micrologic X - Guide utilisateur*.

Recommandations pour protéger l'accès par NFC

Fonctions accessibles par NFC

Le protocole NFC (Near Field Communication) sans fil permet de télécharger des données depuis l'unité de contrôle Micrologic X sur un smartphone, même lorsque celle-ci est hors tension. Il n'est pas possible de modifier des paramètres sur l'unité de contrôle, ni d'ouvrir, de fermer ou de réinitialiser le disjoncteur Masterpact MTZ.

Conditions requises pour établir une connexion NFC

Pour établir une connexion NFC sans fil à l'unité de contrôle Micrologic X, les conditions requises sont les suivantes :

- Vous devez avoir physiquement accès au local hébergeant le disjoncteur Masterpact MTZ.
- Vous devez avoir l'application Masterpact MTZ Mobile App installée sur votre smartphone.
- Le smartphone doit prendre en charge le protocole NFC.

Toute personne qui remplit ces conditions peut télécharger des données potentiellement confidentielles sur votre fonctionnement. L'unité de contrôle Micrologic X ne garde aucune trace des connexions établies par NFC.

Pour une procédure détaillée sur l'établissement d'une connexion NFC, consultez le document *Unité de contrôle Micrologic X - Guide utilisateur*.

Recommandations générales pour protéger l'accès par NFC

Pour protéger l'accès aux données accessibles par NFC sans fil, il est recommandé d'effectuer les opérations suivantes :

- Installez le disjoncteur Masterpact MTZ dans un local verrouillé, afin qu'aucune personne non autorisée ne puisse accéder à l'unité de contrôle Micrologic X.
- Maintenez ce local verrouillé à tout moment.
- Ne donnez la clé ou le code d'accès qu'aux personnes autorisées.

Pour plus d'informations, consultez les recommandations pour restreindre l'accès local au disjoncteur Masterpact MTZ *(voir page 20)*.

Recommandations pour la communication NFC

Pour protéger l'accès aux fonctions accessibles par NFC sans fil, il est recommandé d'effectuer les opérations suivantes :

- Déconnectez le smartphone d'Internet (par exemple, en activant le mode avion) en cas de connexion NFC à l'unité de contrôle Micrologic X.
- Désactivez la communication Bluetooth sur le smartphone.
- N'entrez aucun code d'appariement si vous y êtes invité, car il n'est pas requis pour une connexion NFC.

Recommandations pour utiliser Masterpact MTZ Mobile App

Pour restreindre l'accès à l'unité de contrôle Micrologic X à partir d'un smartphone exécutant Masterpact MTZ Mobile App, il est recommandé de n'utiliser que l'application Masterpact MTZ Mobile App officielle de Schneider Electric afin de se connecter au disjoncteur Masterpact MTZ.

Recommandations pour utiliser des smartphones

Pour restreindre l'accès à l'unité de contrôle Micrologic X à partir d'un smartphone, il est recommandé d'effectuer les opérations suivantes :

- Vérifiez que les smartphones dotés de Masterpact MTZ Mobile App sont protégés par un mot de passe et utilisés uniquement dans le cadre professionnel.
- Renforcez les smartphones équipés de l'application Masterpact MTZ Mobile App en mettant en œuvre toutes les fonctionnalités de sécurité recommandées par le fournisseur ou le fabricant du smartphone.
- Mettez à jour les applications antivirus pour smartphones.
- Ne communiquez aucune information sur le smartphone (numéro de téléphone, adresse MAC), sauf en cas de nécessité.
- Déconnectez le smartphone d'Internet (par exemple, en activant le mode avion) pendant une connexion NFC à l'unité de contrôle Micrologic X.
- Ne stockez aucune information confidentielle ou sensible sur votre smartphone.

Recommandations pour protéger l'accès par Bluetooth

Fonctions accessibles par Bluetooth

AVIS

RISQUE DE FONCTIONNEMENT IMPREVU

- L'appareil doit être configuré par du personnel qualifié et à l'aide des résultats de l'analyse du système de protection de l'installation.
- Lors de la mise en service de l'installation et après toute modification, vérifiez que la configuration de Micrologic X et les paramètres des fonctions de protection sont cohérents avec les résultats de cette analyse.
- Les fonctions de protection de Micrologic X sont définies par défaut sur la valeur minimale, excepté pour la fonction de protection long retard qui est définie par défaut sur la valeur maximale.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Grâce aux communications Bluetooth low energy (BLE) sans fil, vous pouvez accéder à l'unité de contrôle Micrologic X depuis un smartphone exécutant Masterpact MTZ Mobile App. Cette application offre une interface orientée tâches avec l'unité de contrôle. Les données transférées par Bluetooth sont chiffrées selon le chiffrement AES 128 bits.

Conditions requises pour établir une connexion Bluetooth

Pour établir une connexion Bluetooth sans fil à l'unité de contrôle Micrologic X, les conditions requises sont les suivantes :

- L'unité de contrôle Micrologic X doit être sous tension.
- La fonction Bluetooth doit être activée sur l'unité de contrôle Micrologic X.
- Un seul smartphone à la fois peut être connecté à une unité de contrôle.
- Vous devez disposer d'un smartphone équipé de l'application Masterpact MTZ Mobile App.
- Le smartphone doit prendre en charge Bluetooth low energy 4.0 ou version ultérieure.
- Vous devez avoir accès à l'unité de contrôle Micrologic X pour activer le bouton-poussoir Bluetooth, et rester physiquement à portée (généralement 20 à 30 mètres) durant toute la connexion.

Toute personne qui remplit ces conditions et établit une connexion a accès à des fonctions qui peuvent avoir un impact sur votre installation.

Pour savoir comment établir une connexion Bluetooth, consultez le document *Unité de contrôle Micrologic X - Guide utilisateur*.

Recommandations générales pour protéger l'accès par Bluetooth

Pour protéger l'accès aux fonctions accessibles par Bluetooth sans fil, il est recommandé d'effectuer les opérations suivantes :

- Installez le disjoncteur Masterpact MTZ dans un local verrouillé, afin qu'aucune personne non autorisée ne puisse accéder à l'unité de contrôle Micrologic X.
- Maintenez ce local verrouillé à tout moment.
- Ne donnez la clé ou le code d'accès qu'aux personnes autorisées.

Pour plus d'informations sur la protection de l'accès au disjoncteur Masterpact MTZ, consultez la section Mise en œuvre d'une stratégie d'accès restreint *(voir page 20)*.

Recommandations pour utiliser Bluetooth

Pour protéger l'accès aux fonctions accessibles par Bluetooth sans fil, il est recommandé d'effectuer les opérations suivantes :

- Désactivez la fonction Bluetooth sur l'unité de contrôle Micrologic X, comme indiqué dans *Unité de contrôle Micrologic X - Guide utilisateur*, et ne l'activez que lorsque vous êtes prêt à établir la connexion.
- Configurez le temporisateur de déconnexion Bluetooth sur 5 minutes.
- Sauf si vous démarrez une connexion Bluetooth, Bluetooth ne doit pas être activée à partir du bouton-poussoir situé sur la face avant de l'unité de contrôle Micrologic X. Bluetooth doit rester désactivée si elle n'est pas utilisée.
- Appuyez sur le bouton-poussoir Bluetooth pour mettre fin à la communication lorsque vous en avez terminé.
- L'appariement doit s'effectuer aussi rarement que possible et dans un local sécurisé, afin qu'aucun intrus ne puisse voir le code saisi.
- N'entrez pas un code d'appariement si le système ne vous y invite pas.
- Pendant l'appariement Bluetooth, conservez le smartphone aussi proche que possible de l'unité de contrôle Micrologic X.

Recommandations pour utiliser Masterpact MTZ Mobile App

Pour restreindre l'accès à l'unité de contrôle Micrologic X à partir d'un smartphone exécutant Masterpact MTZ Mobile App, il est recommandé de n'utiliser que l'application Masterpact MTZ Mobile App officielle de Schneider Electric afin de se connecter au disjoncteur Masterpact MTZ.

Recommandations pour utiliser des smartphones

Pour restreindre l'accès à l'unité de contrôle Micrologic X à partir d'un smartphone, il est recommandé d'effectuer les opérations suivantes :

- Vérifiez que les smartphones dotés de Masterpact MTZ Mobile App sont protégés par un mot de passe et utilisés uniquement dans le cadre professionnel.
- Renforcez les smartphones équipés de l'application Masterpact MTZ Mobile App en mettant en œuvre toutes les fonctionnalités de sécurité recommandées par le fournisseur ou le fabricant du smartphone.
- Mettez à jour les applications antivirus pour smartphones.
- Ne communiquez aucune information sur le smartphone (numéro de téléphone, adresse MAC), sauf en cas de nécessité.
- Déconnectez le smartphone d'Internet lors d'une connexion Bluetooth avec l'unité de contrôle Micrologic X.
- Ne stockez aucune information confidentielle ou sensible sur votre smartphone.

Recommandations pour protéger l'accès à l'unité de contrôle Micrologic X par le port mini-USB

Fonctions accessibles par le port mini-USB

Il est possible d'accéder à toutes les fonctions de l'unité de contrôle Micrologic X en :

- connectant un PC qui exécute le logiciel Ecoreach au mini-port USB de l'unité de contrôle ;
- connectant un smartphone qui exécute Masterpact MTZ Mobile App au mini-port USB de l'unité de contrôle à l'aide d'un adaptateur USB OTG.

Sachez que l'unité de contrôle ne dispose pas d'une fonction de stockage de masse. Il n'est donc pas possible d'attaquer le système en téléchargeant un logiciel malveillant à partir d'une clé USB ou d'un autre périphérique de stockage de masse.

Conditions requises pour établir une connexion USB ou USB OTG

Pour établir une connexion USB à l'unité de contrôle Micrologic X, les conditions requises sont les suivantes :

- Vous devez avoir physiquement accès à la salle hébergeant le disjoncteur Masterpact MTZ.
- Pour une connexion à partir d'un PC :
  - Vous devez avoir un câble USB avec un connecteur mini-USB pour raccorder votre PC au port mini-USB de l'unité de contrôle Micrologic X.
  - Vous devez avoir un PC qui exécute le logiciel Ecoreach.
- Pour une connexion à partir d'un smartphone :
  - Vous devez avoir un adaptateur OTG et un câble USB avec un mini-connecteur USB pour raccorder votre smartphone au mini-port USB de l'unité de contrôle Micrologic X.
  - Vous devez avoir un smartphone qui exécute Masterpact MTZ Mobile App.

Recommandations générales pour protéger l'accès par port mini-USB

Pour protéger l'accès aux fonctions accessibles par le port mini-USB de l'unité de contrôle Micrologic X, il est recommandé d'effectuer les opérations suivantes :

- Installez le disjoncteur Masterpact MTZ dans un local verrouillé, afin qu'aucune personne non autorisée ne puisse accéder à l'unité de contrôle Micrologic X.
- Maintenez ce local verrouillé à tout moment.
- Ne donnez la clé ou le code d'accès qu'aux personnes autorisées.

Pour plus d'informations, consultez les recommandations pour restreindre l'accès local au disjoncteur Masterpact MTZ *(voir page 20)*.

Recommandations pour les PC exécutant le logiciel Ecoreach

Pour protéger l'accès à l'unité de contrôle Micrologic X à partir d'un PC connecté en local au port mini-USB situé sur la face avant de l'unité de contrôle, il est recommandé d'effectuer les opérations suivantes :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Vérifiez que les PC qui exécutent le logiciel Ecoreach requièrent un ID utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts *(voir page 16)*.
- Vérifiez que les mots de passe utilisateur sont changés régulièrement.
- Interdisez la réutilisation d'anciens mots de passe.
- Réglez un temporisateur pour verrouiller l'écran du PC après une période d'inactivité.
- Renforcez les PC conformément aux consignes les plus récentes du fournisseur du système d'exploitation exécuté sur votre PC.
- Limitez le nombre d'utilisateurs autorisés à utiliser le logiciel Ecoreach.
- Mettez à jour les applications antivirus pour PC.

Recommandations pour les smartphones qui exécutent Masterpact MTZ Mobile App

Pour protéger l'accès à l'unité de contrôle Micrologic X à partir d'un smartphone connecté en local au mini-port USB situé sur la face avant de l'unité de contrôle, il est recommandé d'effectuer les opérations suivantes :

- Vérifiez que les smartphones exécutant Masterpact MTZ Mobile App sont protégés par un mot de passe et utilisés uniquement à titre professionnel.
- Renforcez les smartphones exécutant Masterpact MTZ Mobile App en mettant en œuvre toutes les fonctionnalités de sécurité recommandées par le fournisseur ou le fabricant du smartphone.
- Mettez à jour les applications antivirus pour smartphones.
- Ne communiquez aucune information sur le smartphone (numéro de téléphone, adresse MAC), sauf en cas de nécessité.
- Déconnectez le smartphone d'Internet en cas de connexion USB OTG à l'unité de contrôle Micrologic X.
- Ne stockez aucune information confidentielle ou sensible sur votre smartphone.

Chapitre 4
Recommandations de cybersécurité pour l'accès distant

Présentation du chapitre

Ce chapitre répertorie les chemins d'accès distant au disjoncteur Masterpact MTZ. Il fournit également des recommandations pour sécuriser ces chemins d'accès. Ces éléments importants sont à prendre en compte pour l'exploitation.

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Restriction de l'accès distant au disjoncteur Masterpact MTZ

Présentation

L'unité fonctionnelle intelligente (IMU) Masterpact MTZ offre des possibilités d'accès local et distant. Vous devez vérifier que seuls les utilisateurs autorisés bénéficient de droits d'accès.

Accès distant au disjoncteur Masterpact MTZ

Selon l'architecture de votre système, il existe probablement plusieurs voies d'accès distant au disjoncteur Masterpact MTZ. En particulier, l'accès distant par Ethernet ou Modbus-SL peut fournir un contrôle total sur votre installation. Il est donc extrêmement important de contrôler l'accès distant à votre système.

Vous devez notamment prendre en compte :

- les modes d'accès au système à l'aide des différents chemins de communication disponibles *(voir page 11)* ;
- les informations et contrôles disponibles par chaque chemin d'accès *(voir page 14)*.

Activation et désactivation du contrôle à distance du disjoncteur Masterpact MTZ

Le contrôle à distance du disjoncteur Masterpact MTZ désigne les opérations suivantes :

- Ouverture, fermeture et réinitialisation du disjoncteur
- Modification des paramètres du disjoncteur

Si le contrôle à distance du disjoncteur Masterpact MTZ n'est pas une obligation, il est vivement recommandé de le désactiver dans l'interface IFE, EIFE ou IFM. Par défaut, le contrôle à distance est activé.

Sur l'interface IFE, utilisez le bouton de verrouillage sur le panneau avant pour activer ou désactiver les contrôles à distance envoyés sur le réseau Ethernet.

Sur l'interface EIFE, connectez un PC exécutant le logiciel Ecoreach au port mini-USB situé sur la face avant de l'unité de contrôle Micrologic X pour activer ou désactiver le contrôle à distance du disjoncteur Masterpact MTZ via le réseau Ethernet.

Sur l'interface IFM , utilisez le bouton de verrouillage sur le panneau avant pour activer ou désactiver les contrôles à distance envoyés sur le réseau Modbus-SL.

Verrouillage des paramètres de protection

Vous pouvez verrouiller les paramètres de protection du disjoncteur Masterpact MTZ pour empêcher leur modification à distance. Par défaut, la modification des paramètres de protection à distance est autorisée.

Il est recommandé de désactiver la modification à distance des paramètres de protection, si vous n'utilisez pas cette fonction. Pour plus d'informations, consultez le document *Unité de contrôle Micrologic X - Guide utilisateur*.

Mise en place d'une séparation entre le réseau de contrôle industriel et le réseau d'entreprise

Présentation

Lors de la conception et de la mise en œuvre de votre réseau de contrôle industriel, vous devez utiliser des mécanismes de séparation pour le séparer de votre réseau d'entreprise. Cela contribue à restreindre l'accès à l'unité fonctionnelle intelligente Masterpact MTZ.

Vous devez notamment envisager :

- l'utilisation de pare-feu ;
- la création de zones démilitarisées ;
- l'utilisation de systèmes de détection d'intrusion (IDS) et/ou de prévention d'intrusion (IPS) ;
- la mise en place de stratégies de sécurité et de programmes de formation ;
- la définition de mécanismes de réponse aux incidents.

Des organismes spécialisés (par exemple, NIST) et de normalisation (par exemple, ISO et CEI/IEEE) fournissent et mettent à jour des consignes pour la conception d'un réseau de contrôle industriel et à sa séparation de l'intranet d'entreprise. Pour plus d'informations sur ces différents points, consultez ces publications.

Recommandations pour protéger l'accès distant à l'unité de contrôle Micrologic X par Ethernet

Fonctions accessibles par Ethernet

Lorsqu'un PC exécutant le logiciel Ecoreach est connecté au réseau Ethernet, toutes les fonctions de l'unité de contrôle Micrologic X sont accessibles dans les cas suivants :

- Le disjoncteur Masterpact MTZ est connecté à une interface IFE.
- Le disjoncteur Masterpact MTZ inclut l'interface EIFE.
- Le disjoncteur Masterpact MTZ est connecté à une interface IFM hébergée sur un serveur IFE.

Conditions requises pour établir une connexion Ethernet

Pour établir une connexion Ethernet à l'unité de contrôle Micrologic X, les conditions requises sont les suivantes :

- L'unité de contrôle Micrologic X doit être sous tension.
- L'unité de contrôle Micrologic X doit être connectée à un réseau Ethernet via l'une des interfaces suivantes :
  - une interface IFE ;
  - une interface EIFE ;
  - une interface IFM hébergée sur un serveur IFE.
- Vous devez avoir un PC ou un autre équipement (FDM128 ou automate programmable, par exemple) qui exécute le logiciel de contrôle et de surveillance (SCADA, Ecoreach) connecté au réseau Ethernet pour offrir un accès distant.
- Vous devez avoir un ID utilisateur et un mot de passe avec les droits d'accès appropriés pour vous connecter au logiciel Ecoreach.

Recommandations pour les PC connectés à Ethernet

Pour protéger l'accès à l'unité de contrôle Micrologic X à partir d'un PC en réseau, il est recommandé d'effectuer les opérations suivantes :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Vérifiez que le PC qui permet d'accéder à l'unité de contrôle Micrologic X via Ethernet (par exemple, à l'aide des pages Web IFE ou EIFE, ou bien de SCADA) requiert un identifiant utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts *(voir page 15)*.
- Vérifiez que les mots de passe utilisateur sont changés régulièrement.
- Interdisez la réutilisation d'anciens mots de passe.
- Réglez un temporisateur pour verrouiller l'écran du PC après une période d'inactivité.
- Renforcez le PC en suivant les consignes les plus récentes du fournisseur du système d'exploitation de votre PC.
- Limitez le nombre d'utilisateurs autorisés à accéder à l'unité de contrôle Micrologic X à partir d'un PC en réseau.
- Mettez à jour les applications antivirus pour PC.

Outre les précautions ci-dessus, vous devez également suivre les consignes et recommandations générales concernant la protection de votre installation, indiquées dans le document *How Can I Reduce Vulnerability to Cyber Attacks?*.

Recommandations pour protéger l'accès distant à l'unité de contrôle Micrologic X par Modbus-SL

Fonctions accessibles par Modbus-SL

Lorsqu'un PC exécutant le logiciel Ecoreach est connecté au réseau Modbus-SL, toutes les fonctions de l'unité de contrôle Micrologic X sont accessibles si le disjoncteur Masterpact MTZ est connecté à une interface IFM.

Conditions requises pour établir une connexion Modbus-SL

Pour établir une connexion Modbus-SL à l'unité de contrôle Micrologic X, les conditions requises sont les suivantes :

- L'unité de contrôle Micrologic X doit être sous tension.
- L'unité de contrôle Micrologic X doit être connectée à une interface IFM.
- Vous devez avoir un PC ou un autre équipement (un automate programmable, par exemple) qui exécute le logiciel de contrôle et de surveillance (SCADA, Ecoreach) connecté au réseau Modbus-SL qui fournit l'accès distant.
- Vous devez avoir un ID utilisateur et un mot de passe avec les droits d'accès appropriés pour vous connecter au logiciel Ecoreach.

Recommandations pour les PC connectés à Modbus-SL

Pour protéger l'accès à l'unité de contrôle Micrologic X à partir d'un PC en réseau, il est recommandé d'effectuer les opérations suivantes :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Vérifiez que le PC qui fournit l'accès à l'unité de contrôle Micrologic X en Modbus-SL (par exemple, via SCADA) requiert un identifiant utilisteur et un mot de passe.
- Imposez l'utilisation de mots de passe forts *(voir page 15)*.
- Vérifiez que les mots de passe utilisateur sont changés régulièrement.
- Interdisez la réutilisation d'anciens mots de passe.
- Réglez un temporisateur pour verrouiller l'écran du PC après une période d'inactivité.
- Renforcez le PC en suivant les consignes les plus récentes du fournisseur du système d'exploitation de votre PC.
- Limitez le nombre d'utilisateurs autorisés à accéder à l'unité de contrôle Micrologic X à partir d'un PC en réseau.
- Mettez à jour les applications antivirus pour PC.

Outre les précautions ci-dessus, vous devez également suivre les consignes et recommandations générales concernant la protection de votre installation, indiquées dans le document *How Can I Reduce Vulnerability to Cyber Attacks?*.

Chapitre 5
Recommandations de cybersécurité pour les mises à niveau du firmware et les Digital Modules

Contenu de ce chapitre

Ce chapitre contient les sujets suivants :

Installation des mises à niveau du firmware

Présentation

La distribution de logiciels altérés ou illégaux pouvant contenir des applications modifiées ou supplémentaires est une cyberattaque de plus en plus prisée. Ces applications peuvent compromettre l'intégrité du logiciel d'origine ou son utilisation.

Pour garantir l'intégrité et l'authenticité de tous les composants de l'IMU Masterpact MTZ, c'est-à-dire de l'unité de contrôle Micrologic X, de l'interface IFE, EIFE ou IFM , et du module IO, toutes les mises à niveau du firmware d'origine Schneider Electric sont signées numériquement.

Mettez à niveau le firmware à l'aide du logiciel Ecoreach. Vous devez avoir la dernière version en date du logiciel Ecoreach. Utilisez le logiciel Ecoreach pour mettre à niveau le firmware à l'aide du menu Firmware. La documentation Ecoreach est disponible en téléchargement sur le site Schneider Electric (*https://www.schneider-electric.com/en/download/*).

Recommandations de cybersécurité concernant les mises à niveau du firmware

Il est essentiel d'installer le firmware le plus récent.

Lors de l'installation de mises à niveau du firmware sur les composants de l'IMU Masterpact MTZ, il est recommandé d'effectuer les opérations suivantes :

- Installez les mises à niveau selon les pratiques de technologie opérationnelle en vigueur, comme leur test sur un système de non-production avant leur installation et leur déploiement dans votre environnement de production.
- N'utilisez que la version la plus récente du logiciel Ecoreach pour télécharger et installer les mises à niveau du firmware.
- Renforcez le PC qui exécute le logiciel Ecoreach, en respectant les dernières consignes en date du fournisseur du système d'exploitation.

Firmware signé

Tous les firmwares conçus pour l'IMU Masterpact MTZ sont signés à l'aide de l'infrastructure de clé publique Schneider Electric. Les signatures numériques sont authentifiées à l'aide du certificat public présent dans le logiciel Ecoreach.

Lorsqu'un firmware est téléchargé dans l'IMU Masterpact MTZ via le logiciel Ecoreach, l'unité de contrôle Micrologic X en vérifie automatiquement la signature numérique. Cette vérification s'effectue à l'aide du certificat public stocké dans l'unité de contrôle.

Pour des raisons de sécurité, les certificats sont passibles de modifications. Il est donc essentiel (et cela relève de votre responsabilité) de vérifier que la version du logiciel Ecoreach que vous utilisez pour télécharger et installer des mises à niveau du firmware est la dernière en date. Dans la dernière version du logiciel Ecoreach, les certificats publics utilisés pour signer le firmware sont à jour.

Les certificats qui ne sont plus valides sont publiés dans une liste de certificats révoqués (CRL). Cette liste est disponible sur le site Web officiel de Schneider Electric.

Avantages d'utiliser le logiciel Ecoreach pour les mises à niveau du firmware

Le logiciel Ecoreach joue un rôle important dans l'intégrité de votre réseau de contrôle industriel pendant les mises à niveau du firmware. N'utilisez que la version la plus récente du logiciel Ecoreach pour télécharger et installer des mises à niveau du firmware, car c'est la seule à vous apporter les avantages suivants :

- Lorsque vous téléchargez des mises à niveau du firmware à partir du centre de téléchargement officiel de Schneider Electric à l'aide du logiciel Ecoreach, leur signature numérique est automatiquement vérifiée.
- Lorsque vous téléchargez un firmware dans l'unité de contrôle Micrologic X (à l'aide du logiciel Ecoreach via une connexion USB), sa signature numérique est automatiquement vérifiée.

Le logiciel Ecoreach effectue des vérifications automatiques en fonction de la validité du certificat public utilisé.

Pour en savoir plus sur le téléchargement et l'installation de mises à niveau du firmware, consultez l'aide en ligne d'Ecoreach.

⚠ AVERTISSEMENT

RISQUE DE FONCTIONNEMENT IMPREVU

- Mettez à jour votre logiciel Ecoreach dès que possible lorsque vous recevez une notification indiquant qu'une mise à jour est disponible.
- Utilisez cette dernière version du logiciel Ecoreach pour mettre à niveau le micrologiciel de tous vos produits.
- Consultez régulièrement la liste des certificats révoqués sur le site Web officiel de Schneider Electric. Si un certificat est révoqué pour l'un de vos produits, n'installez pas de micrologiciel antérieur à la date de la révocation.

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

Vérification de la liste des certificats révoqués

À intervalles réguliers et au minimum tous les trois mois, vous devez consulter la liste des certificats révoqués (CRL) publiée par Schneider Electric, pour vérifier qu'elle n'inclut pas les certificats utilisés par vos équipements.

Pour consulter la liste CRL, procédez comme suit :

Étape	Action
1	Affichez la liste CRL publiée sur le site Web de Schneider Electric *(voir page 38)*.
2	Si la liste est vide, cela signifie que vos certificats actuels sont valides. Vous n'avez rien à faire. Si elle n'est pas vide, passez à l'étape 3.
3	Vérifiez que vous utilisez la dernière version en date du logiciel Ecoreach. Si tel n'est pas le cas, mettez à jour votre logiciel Ecoreach.
4	Mettez à niveau votre firmware.

Achat et installation de Digital Modules

Présentation

Les Digital Modules sont des modules optionnels qui étendent les fonctions disponibles à la gamme d'unités de contrôle Micrologic X. Vous pouvez les acheter en même temps que le disjoncteur Masterpact MTZ dans la commande initiale ou ultérieurement sur le site GoDigital en ligne de Schneider Electric.

Tous les Digital Modules conçus pour l'unité de contrôle Micrologic X sont signés numériquement pour une sécurité accrue avec l'infrastructure de clé publique (PKI) de Schneider Electric. Celle-ci garantit l'authenticité et l'intégrité de ces téléchargements. Les Digital Modules doivent être installés à l'aide du logiciel Ecoreach.

Recommandations de cybersécurité pour acheter des Digital Modules

Pour acheter des Digital Modules pour l'unité de contrôle Micrologic X, n'utilisez que le site GoDigital du centre de téléchargement officiel de Schneider Electric.

Lors de l'installation des Digital Modules pour des composants de l'IMU Masterpact MTZ, il est recommandé d'effectuer les opérations suivantes :

- Installez les Digital Modules selon les pratiques de technologie opérationnelle en vigueur, comme leur test sur un système de non-production avant leur installation et leur déploiement dans votre environnement de production.
- N'utilisez que la version la plus récente du logiciel Ecoreach pour télécharger et installer les Digital Modules.
- Renforcez les PC utilisés pour télécharger les Digital Modules et les installer selon les dernières consignes du fournisseur du système d'exploitation.

Recommandations de cybersécurité pour installer des Digital Modules

N'utilisez que le logiciel Ecoreach pour installer les Digital Modules de l'unité de contrôle Micrologic X.

Le logiciel Ecoreach joue un rôle important dans l'intégrité de votre réseau de contrôle industriel. N'utilisez que la version la plus récente du logiciel Ecoreach pour télécharger et installer les Digital Modules, car c'est la seule à vous apporter les avantages suivants :

- Lorsque vous mettez à niveau le firmware d'un équipement de l'IMU à l'aide du logiciel Ecoreach via une connexion USB, la signature numérique de la mise à niveau est automatiquement vérifiée.
- Lorsque vous téléchargez un Digital Module dans l'unité de contrôle Micrologic X à l'aide du logiciel Ecoreach via une connexion USB, la signature numérique du Digital Module est automatiquement vérifiée.

Le logiciel Ecoreach effectue des vérifications automatiques en fonction de la validité du certificat public utilisé.

Pour en savoir plus sur le téléchargement et l'installation de Ecoreach, consultez l'aide en ligne de Digital Modules.

⚠ AVERTISSEMENT

RISQUE DE FONCTIONNEMENT IMPREVU

- Mettez à jour votre logiciel Ecoreach dès que possible lorsque vous recevez une notification indiquant qu'une mise à jour est disponible.
- Utilisez cette dernière version du logiciel Ecoreach pour mettre à niveau le micrologiciel de tous vos produits.
- Consultez régulièrement la liste des certificats révoqués sur le site Web officiel de Schneider Electric. Si un certificat est révoqué pour l'un de vos produits, n'installez pas de micrologiciel antérieur à la date de la révocation.

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

Vérification de la liste des certificats révoqués

À intervalles réguliers et au minimum tous les trois mois, vous devez consulter la liste des certificats révoqués (CRL) publiée par Schneider Electric, pour vérifier qu'elle n'inclut pas les certificats utilisés par vos équipements.

Pour consulter la liste CRL, procédez comme suit :

Étape	Action
1	Affichez la liste CRL publiée sur le site Web de Schneider Electric *(voir page 38)*.
2	Si la liste est vide, cela signifie que vos certificats actuels sont valides. Vous n'avez rien à faire. Si elle n'est pas vide, passez à l'étape 3.
3	Vérifiez que vous utilisez la dernière version en date du logiciel Ecoreach. Si tel n'est pas le cas, mettez à jour votre logiciel Ecoreach.
4	Mettez à niveau votre module numérique.

Portail de cybersécurité de Schneider Electric

Présentation

Le portail de cybersécurité de Schneider Electric décrit la politique de gestion des vulnérabilités de Schneider Electric.

L'objectif de la politique de gestion des vulnérabilités de Schneider Electric est de gérer les vulnérabilités qui ont un impact sur les produits et systèmes Schneider Electric, afin de protéger les solutions installées, les clients et l'environnement.

Schneider Electric travaille avec des chercheurs, des équipes de réponse aux cyberurgences (CERT) et des propriétaires de site pour s'assurer que des informations exactes sont fournies en temps voulu pour protéger correctement leurs installations.

L'équipe CPCERT (Corporate Product CERT) de Schneider Electric est chargée non seulement de gérer les vulnérabilités et les restrictions affectant les produits, mais aussi d'émettre des alertes.

Elle coordonne la communication avec les équipes CERT appropriées, des chercheurs indépendants, des chefs de produit et tous les clients concernés.

Le portail de cybersécurité de Schneider Electric est accessible à l'adresse *http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp*.

Informations disponibles sur le portail de cybersécurité de Schneider Electric

Le portail fournit les informations suivantes :

- Informations sur les vulnérabilités des produits en matière de cybersécurité
- Informations sur les incidents de cybersécurité
- Interface qui permet aux utilisateurs de déclarer des incidents ou des vulnérabilités en matière de cybersécurité
- Accès aux ressources qui fournissent des informations sur la sécurisation de votre environnement système
  Ces environnements sont les suivants :
  - Processus industriels
  - Systèmes de contrôle d'accès et de gestion de bâtiments
  - Centres de données
  - Systèmes de contrôle des infrastructures électriques
- Certificats et listes des certificats révoqués dans l'onglet **Firmware PKI**

Liste des certificats révoqués (CRL) disponible sur le portail de cybersécurité de Schneider Electric

Le tableau suivant fournit la liste des certificats révoqués :

Produit	CRL
Unité de contrôle MTZ	Maître Micrologic du disjoncteur BT
Module IO	Maître Micrologic du disjoncteur BT
IFE	Maître de communication avancée
EIFE	Maître de communication avancée
IFM	Maître Micrologic du disjoncteur BT

Glossaire

B

BLE

Bluetooth low energy.

E

EIFE

Interface Ethernet intégrée, qui est un module optionnel du disjoncteur débrochable Masterpact MTZ. Avec ce module, le disjoncteur est accessible via l'intranet de l'entreprise.

G

GoDigital

Site en ligne Schneider Electric permettant d'acheter des Digital Modules conçus pour l'unité de contrôle Micrologic X.

I

IC

Acronyme d'Industrial Control, signifiant contrôle industriel. Désigne les systèmes matériels et logiciels utilisés pour surveiller et contrôler les processus et équipements de production de l'entreprise.

IFE

Interface Ethernet pouvant être connectée au disjoncteur Masterpact MTZ. Avec ce module, le disjoncteur est accessible via l'intranet de l'entreprise.

IFM

Interface Modbus-SL IFM permettant à une IMU de se connecter à un réseau Modbus à ligne série RS 485 à deux fils. Chaque IMU dispose de sa propre interface IFM et d'une adresse Modbus correspondante.

IHM

Acronyme d'interface homme-machine. Désigne les afficheurs sur la face avant d'un équipement utilisé par un opérateur pour lire des informations ou configurer l'équipement.

IMU

Acronyme d'Intelligent Modular Unit, signifiant unité fonctionnelle intelligente. Dans le cas du disjoncteur Masterpact MTZ, l'IMU désigne le disjoncteur lui-même, l'unité de contrôle Micrologic X, ainsi que les modules ULP, l'interface IFE, EIFE ou IFM et le module IO associés.

IP

Acronyme d'Internet Protocol. Les adresses IP servent à identifier les équipements connectés à l'intranet de l'entreprise ou à Internet.

IT

Acronyme d'Information Technology. Désigne le réseau informatique et les systèmes d'information de l'entreprise, par opposition au réseau de contrôle industriel (IC) ou au réseau de technologie opérationnelle (OT).

L

LAN

Acronyme de Local Area Network, signifiant réseau local. Désigne l'intranet ou le réseau informatique de l'entreprise.

N

NFC

Acronyme de Near Field Communication. Désigne un protocole de communication sans fil.

O

OT

Acronyme d'Operational Technology, signifiant technologie opérationnelle. Désigne les systèmes matériels et logiciels utilisés par l'entreprise pour surveiller et contrôler directement les processus et équipements de production, également appelés réseau de contrôle industriel (IC). L'abréviation OT est souvent utilisée pour désigner le réseau opérationnel de l'entreprise, par opposition à son réseau informatique.

P

PIN

Acronyme de Personal Identication Number, signifiant numéro d'identification personnel.

PKI

Acronyme de Public Key Infrastructure, signifiant infrastructure de clé publique. Définit un ensemble de services utilisés pour générer et authentifier des signatures numériques. Une infrastructure de clé publique est conçue pour garantir la confidentialité, l'intégrité et l'authenticité des informations.

R

RAS

Acronyme de Remote Access Server, signifiant serveur d'accès distant.

S

SCADA

Acronyme de Supervisory Control And Data Acquisition. Désigne les systèmes conçus pour obtenir des données en temps réel sur les processus et équipements de production en vue de les surveiller et de les contrôler à distance.

T

TCP/IP

Acronyme de Transmission Control Protocol/Internet Protocol. Désigne la suite de protocoles utilisés pour les communications sur Internet.

V

VPN

Acronyme de Virtual Private Network, signifiant réseau privé virtuel. Un VPN permet d'établir un « tunnel » sécurisé/privé entre un point d'accès externe authentifié et le réseau d'entreprise sécurisé.

DOCA0122FR-01

Schneider Electric Industries SAS
35, rue Joseph Monier
CS30323
F - 92506 Rueil Malmaison Cedex

http://www.schneider-electric.com

06/2017