
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.

Vous acceptez de ne pas reproduire, excepté pour votre propre usage à titre non commercial, tout ou partie de ce document et sur quelque support que ce soit sans l'accord écrit de Schneider Electric. Vous acceptez également de ne pas créer de liens hypertextes vers ce document ou son contenu. Schneider Electric ne concède aucun droit ni licence pour l'utilisation personnelle et non commerciale du document ou de son contenu, sinon une licence non exclusive pour une consultation « en l'état », à vos propres risques. Tous les autres droits sont réservés.

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.

© 2019 Schneider Electric. Tous droits réservés.



| | | |
|-------------------|---|-----------|
| | Consignes de sécurité | 5 |
| | A propos de ce manuel | 7 |
| Chapitre 1 | Introduction à la cybersécurité | 9 |
| | Introduction à la cybersécurité | 10 |
| | Intérêt de la cybersécurité pour les disjoncteurs MasterPact MTZ | 11 |
| Chapitre 2 | Recommandations de cybersécurité pour la conception, la planification et l'installation de système | 13 |
| | Identification et protection des informations et opérations sensibles et critiques | 14 |
| | Conception d'une stratégie de mot de passe | 15 |
| | Formation | 17 |
| Chapitre 3 | Recommandations de cybersécurité pour l'accès local | 19 |
| | Restriction de l'accès local au disjoncteur MasterPact MTZ | 20 |
| | Recommandations pour protéger l'accès local à l'IHM MicroLogic X | 21 |
| | Recommandations pour protéger l'accès par NFC | 22 |
| | Recommandations pour protéger l'accès par Bluetooth | 23 |
| | Recommandations pour protéger l'accès à l'unité de contrôle MicroLogic X par le port mini-USB | 25 |
| Chapitre 4 | Recommandations de cybersécurité pour l'accès distant | 27 |
| | Restriction de l'accès distant au disjoncteur MasterPact MTZ | 28 |
| | Mise en place d'une séparation entre le réseau de TO et le réseau d'entreprise | 29 |
| | Recommandations pour protéger l'accès distant à l'unité de contrôle MicroLogic X par Ethernet | 30 |
| | Recommandations pour protéger l'accès distant à l'unité de contrôle MicroLogic X par Modbus-SL | 31 |
| Chapitre 5 | Recommandations de cybersécurité pour les mises à niveau du firmware et les Digital Modules | 33 |
| | Installation de mises à niveau du firmware | 34 |
| | Achat et installation de Digital Modules | 36 |
| | Portail d'assistance à la cybersécurité de Schneider Electric | 37 |
| Glossaire | | 39 |

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.

AVERTISSEMENT

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

- Modifiez les mots de passe par défaut à la première utilisation, afin d'empêcher tout accès non autorisé aux réglages, contrôles et informations des appareils.
- 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 cybersécurité (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 technologie opérationnelle 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.

Les informations indiquées dans ce document peuvent être mises à jour à tout moment. Schneider Electric recommande de disposer en permanence de la version la plus récente, disponible sur le site www.schneider-electric.com/docs.

Document(s) à consulter

| Titre de documentation | Référence |
|--|---|
| <i>MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur</i> | DOCA0102FR |
| <i>How Can I Reduce Vulnerability to Cyber Attacks?</i> | Cybersecurity System Technical Note |
| <i>MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note</i> | DOCA0144EN |
| <i>Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker - Release Note</i> | DOCA0146EN |
| <i>Enerlin'X IFE Switchboard Server IFE/EIFE Ethernet Interface - Release Note</i> | DOCA0147EN |
| <i>Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Release Note</i> | DOCA0149EN |
| <i>Enerlin'X FDM128 - Ethernet Display for Eight Devices - Release Note</i> | DOCA0151EN |

Vous pouvez télécharger ces publications et autres informations techniques depuis notre site web à l'adresse : <https://www.se.com/ww/en/download/> .

Marques commerciales

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

