PacT Series

Master**Pact,** Com**PacT,** Power**PacT**

Guide de cybersécurité

PacT Series offre des disjoncteurs et des commutateurs de classe mondiale

DOCA0122FR-07
05/2023

www.se.com

Mentions légales

Table des matières

Consignes de sécurité

Informations importantes

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

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

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

⚠ DANGER

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

⚠ AVERTISSEMENT

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

⚠ ATTENTION

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

AVIS

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

Remarque Importante

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

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

Avis concernant la cybersécurité

⚠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 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.

À propos de ce manuel

Gamme principale PacT Series

Pérennisez votre installation grâce aux PacT Series basse et moyenne tension de Schneider Electric. Fondée sur l'innovation légendaire de Schneider Electric, la PacT Series comprend des disjoncteurs, des interrupteurs, des relais différentiels et des fusibles, adaptés à toutes les applications standard et spécifiques. Bénéficiez de performances fiables avec la PacT Series sur les tableaux de distribution compatibles EcoStruxure, de 16 à 6300 A en basse tension et jusqu'à 40,5 kV en moyenne tension.

Objectif du document

Ce guide fournit des informations sur la cybersécurité des disjoncteurs MasterPact, ComPacT et PowerPacT avec déclencheurs et unités de contrôle MicroLogic en vue d'aider les concepteurs et les utilisateurs de système à mettre en place un environnement sécurisé d'exploitation du produit.

NOTE:

- Les informations relatives à la nouvelle génération de disjoncteurs ComPacT NS et PowerPacT P et R contenues dans ce document s'appliquent également aux gammes existantes de disjoncteurs ComPact NS et PowerPact P et R. Les exceptions sont indiquées le cas échéant.
- Les informations relatives à la nouvelle génération de disjoncteurs ComPacT NSX et PowerPacT H-, J-, and L-Frame contenues dans ce document s'appliquent également aux gammes existantes de disjoncteurs ComPact NSX et PowerPact à châssis H, J et L. Les exceptions sont indiquées le cas échéant.
- Les nouvelles gammes sont basées sur la même architecture technique et dimensionnelle que la gamme existante de disjoncteurs.

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 contenues dans ce guide concernent les disjoncteurs suivants :

- Disjoncteurs MasterPact MTZ avec unités de contrôle MicroLogic
- Disjoncteurs MasterPact NT/NW avec déclencheurs MicroLogic
- Disjoncteurs ComPacT NS avec déclencheurs MicroLogic
- Disjoncteurs PowerPacT à châssis P et R avec déclencheurs MicroLogic
- Disjoncteurs ComPacT NSX avec déclencheurs MicroLogic
- Disjoncteurs PowerPacT à châssis H, J et L avec déclencheurs MicroLogic

NOTE: Les informations contenues dans ce guide concernent également les anciennes gammes ComPact et PowerPact.

Informations en ligne

Les informations indiquées dans ce guide 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.se.com/ww/en/download.

Les caractéristiques techniques des équipements décrits dans ce guide sont également fournies en ligne. Pour accéder aux informations en ligne, accédez à la page d'accueil Schneider Electric à l'adresse www.se.com.

Documents associés aux appareils CEI

Titre de documentation	Référence
MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
ComPacT NSX - Déclencheurs électroniques Micrologic 5/6/7 - Guide utilisateur	DOCA0188EN DOCA0188ES DOCA0188FR DOCA0188ZH
ComPact NSX - Déclencheurs électroniques Micrologic 5/6/7 - Guide utilisateur	DOCA0141EN DOCA0141ES DOCA0141FR DOCA0141ZH
MasterPact NT/NW - Déclencheurs MicroLogic A et E - Guide utilisateur	04443724AA (EN) EAV16735 (ES) 04443723AA (FR)
MasterPact NT/NW - Déclencheurs MicroLogic P - Guide utilisateur	04443726AA (EN) EAV16736 (ES) 04443725AA (FR)
MasterPact NT/NW - Déclencheurs MicroLogic H - Guide utilisateur	04443728AA (EN) EAV16737 (ES) 04443727AA (FR)
ComPacT NS - Déclencheurs MicroLogic A/E - Guide utilisateur	DOCA0218EN DOCA0218ES DOCA0218FR DOCA0218ZH
ComPacT NS - Déclencheurs MicroLogic P - Guide utilisateur	DOCA0219EN DOCA0219ES DOCA0219FR DOCA0219ZH
Enerlin'X EIFE - Interface Ethernet intégrée pour un disjoncteur débrochable Masterpact MTZ - Guide utilisateur	DOCA0106EN DOCA0106ES DOCA0106FR DOCA0106ZH
Enerlin'X IFE - Serveur de tableau Ethernet - Guide utilisateur	DOCA0084EN DOCA0084ES DOCA0084FR DOCA0084ZH
Enerlin'X IFE - Interface Ethernet pour un disjoncteur - Guide utilisateur	DOCA0142EN DOCA0142ES DOCA0142FR DOCA0142ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note
MicroLogic - Déclencheurs et unités de contrôle - Historique du micrologiciel	DOCA0155EN
MasterPact MTZ - MicroLogic X Control Unit - Firmware Release Notes	DOCA0144EN
Enerlin'X IFM - Interface Modbus-SL pour un disjoncteur (TRV00210/ STRV00210) - Notes de publication du micrologiciel	DOCA0145EN
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes	DOCA0146EN
Enerlin'X IFE/EIFE Ethernet Interface - Notes de publication du micrologiciel	DOCA0147EN
Serveur de tableau IFE Enerlin'X - Notes de publication du micrologiciel	DOCA0148EN
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Notes de publication du micrologiciel	DOCA0149EN
Enerlin'X FDM121 - Notes de publication du micrologiciel	DOCA0150EN

Titre de documentation	Référence
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes	DOCA0151EN
BCM ULP - Notes de publication du micrologiciel	DOCA0152EN
ComPacT NSX / PowerPacT à châssis H, J et L - Notes de publication du micrologiciel MicroLogic 5/6	DOCA0153EN
ComPacT NSX - MicroLogic 7 Trip Unit - Firmware Release Notes	DOCA0154EN
EcoStruxure Cybersecurity Admin Expert User Guide	CAE_EN_UM_B4.1

Vous pouvez télécharger ces publications et d'autres informations techniques depuis notre site Web : www.se.com/ww/en/download/.

Documents associés aux appareils UL/ANSI

Titre de documentation	Référence
MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
PowerPacT à châssis H, J et L - Déclencheurs MicroLogic 5 et 6 - Guide utilisateur	48940-312-01 (EN, ES, FR)
MasterPact NT/NW - Déclencheurs MicroLogic A - Guide utilisateur	48049-136-05 (EN, ES, FR)
MasterPact NT/NW - Déclencheurs MicroLogic P - Guide utilisateur	48049-137-05 (EN)
MasterPact NT/NW - Déclencheurs MicroLogic H - Guide utilisateur	48049-330-03 (EN, ES, FR)
Enerlin'X EIFE - Interface Ethernet intégrée pour un disjoncteur débrochable Masterpact MTZ - Guide utilisateur	DOCA0106EN DOCA0106ES DOCA0106FR DOCA0106ZH
Enerlin'X IFE - Serveur de tableau Ethernet - Guide utilisateur	1040IB1401(EN) 1040IB1402(ES) 1040IB1403(FR)
Enerlin'X IFE - Interface Ethernet pour un disjoncteur - Guide utilisateur	0602IB1801EN 0602IB1802ES 0602IB1803FR
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note
MicroLogic - Déclencheurs et unités de contrôle - Historique du micrologiciel	DOCA0155EN
MasterPact MTZ - MicroLogic X Control Unit - Firmware Release Notes	DOCA0144EN
Enerlin'X IFM - Interface Modbus-SL pour un disjoncteur (TRV00210/ STRV00210) - Notes de publication du micrologiciel	DOCA0145EN
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes	DOCA0146EN
Enerlin'X IFE/EIFE Ethernet Interface - Notes de publication du micrologiciel	DOCA0147EN
Serveur de tableau IFE Enerlin'X - Notes de publication du micrologiciel	DOCA0148EN
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Notes de publication du micrologiciel	DOCA0149EN
Enerlin'X FDM121 - Notes de publication du micrologiciel	DOCA0150EN
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes	DOCA0151EN
BCM ULP - Notes de publication du micrologiciel	DOCA0152EN
ComPacT NSX / PowerPacT à châssis H, J et L - Notes de publication du micrologiciel MicroLogic 5/6	DOCA0153EN
EcoStruxure Cybersecurity Admin Expert User Guide	CAE_EN_UM_B4.1

Vous pouvez télécharger ces publications et autres informations techniques depuis notre site Web : www.se.com/us/en/download/.

Introduction à la cybersécurité

Contenu de cette partie

Présentation

Cette section fournit des informations générales sur la stratégie de cybersécurité de Schneider Electric et explique l'intérêt de la cybersécurité pour les disjoncteurs MasterPact, ComPacT et PowerPacT équipés de déclencheurs ou d'unités de contrôle MicroLogic.

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, ComPacT et PowerPacT, vous devez adopter l'approche de défense en profondeur de Schneider Electric concernant la cybersécurité.

Cette approche est décrite dans la note technique *How Can I Reduce Vulnerability to Cyber Attacks?*.

De plus, vous trouverez de nombreuses ressources utiles et des informations actualisées sur le portail d'assistance à la cybersécurité de sur le site web global de Schneider Electric, page 51.

Intérêt de la cybersécurité pour les disjoncteurs MasterPact, ComPacT et PowerPacT

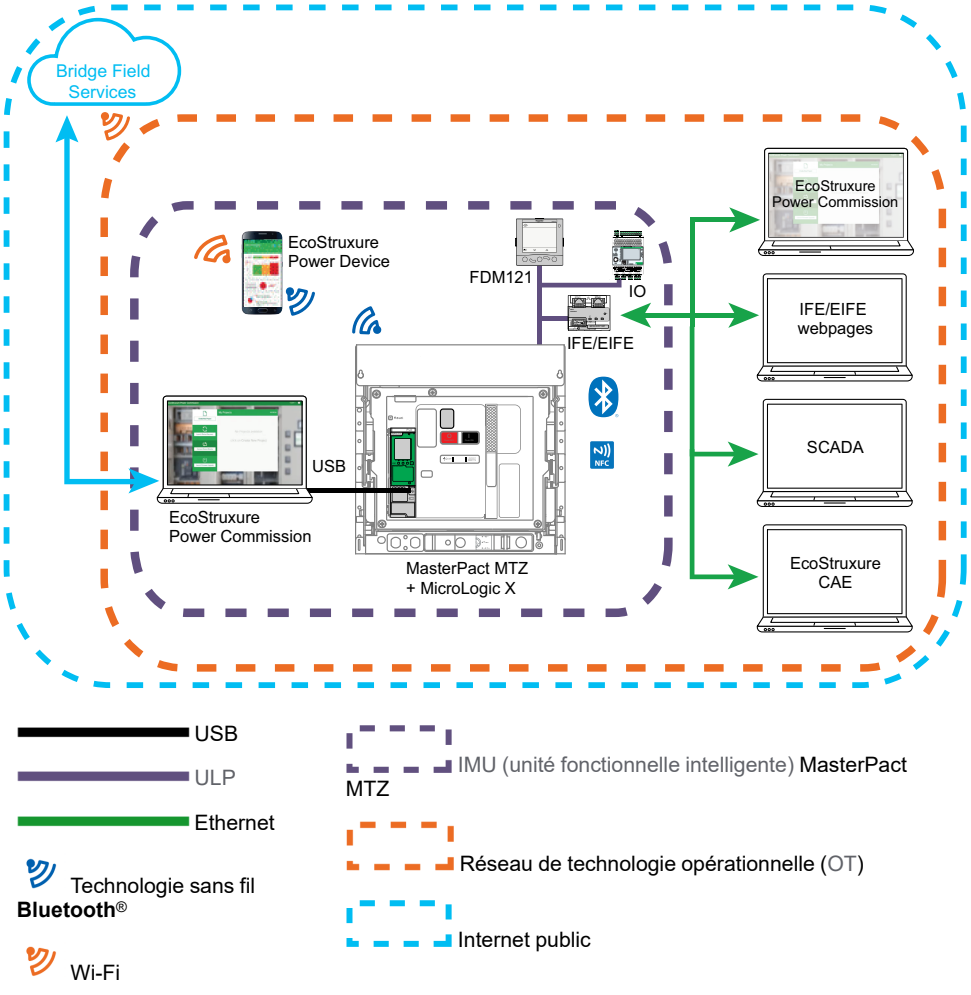
Présentation

Le disjoncteur MasterPact, ComPacT et PowerPacT est un élément clé d'une usine ou d'un équipement, car il contrôle l'alimentation du processus, assure la protection électrique et fournit des informations essentielles.

Les disjoncteurs MasterPact, ComPacT et PowerPacT 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 de distribution électrique avec une efficacité et une flexibilité accrues. Cependant, elles peuvent faire l'objet de cyber-attaques.

Disjoncteur MasterPact MTZ et environnement d'exploitation

La figure suivante montre les différents modes de communication avec l'unité de contrôle MicroLogic X du disjoncteur MasterPact MTZ.



L'unité fonctionnelle intelligente (IMU) MasterPact MTZ englobe le disjoncteur, l'unité de contrôle MicroLogic X et les modules ULP associés, l'interface de communication et les modules IO.

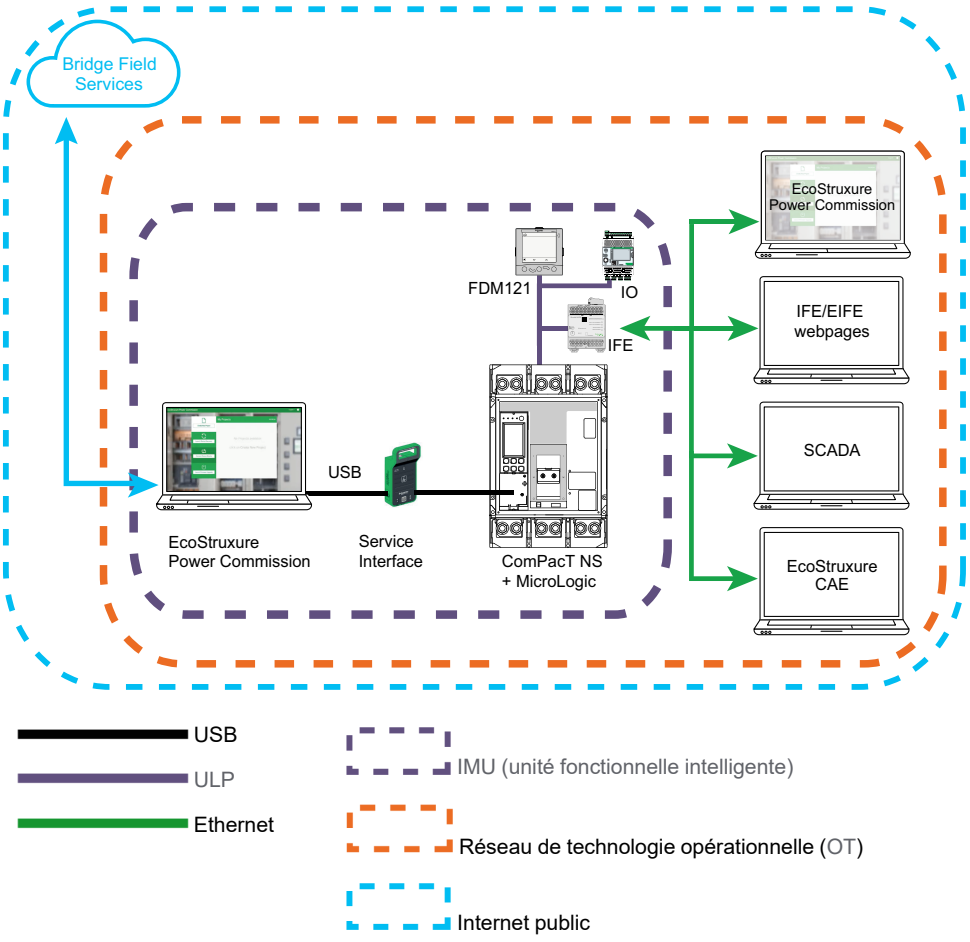
Pour communiquer avec le disjoncteur MasterPact MTZ via son unité de contrôle MicroLogic X, les voies suivantes sont disponibles :

- Interface humain-machine (IHM) MicroLogic X
- Afficheur en face avant FDM121 pour un disjoncteur

- Connexion NFC sans fil à partir d'un smartphone
- Connexion Bluetooth Low Energy 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 EcoStruxure™ Power Commission
  - Un smartphone exécutant Application EcoStruxure Power Device
- Connexion Ethernet (protocoles Modbus TCP/IP ou IEC 61850) via le réseau de technologie opérationnelle (OT) lorsque l'interface IFE ou EIFE est présente
- Connexion Modbus-SL via le réseau de technologie opérationnelle (OT) lorsque l'interface IFM est présente

Disjoncteur MasterPact NT/NW, ComPacT NS et PowerPacT à châssis P et R et environnement d'exploitation

La figure suivante montre les différents modes de communication avec le déclencheur MicroLogic du disjoncteur.



L'IMU englobe le disjoncteur MasterPact NT/NW, ComPacT NS ou PowerPacT à châssis P ou R, le déclencheur MicroLogic ainsi que les modules ULP, l'interface de communication et les modules IO associés.

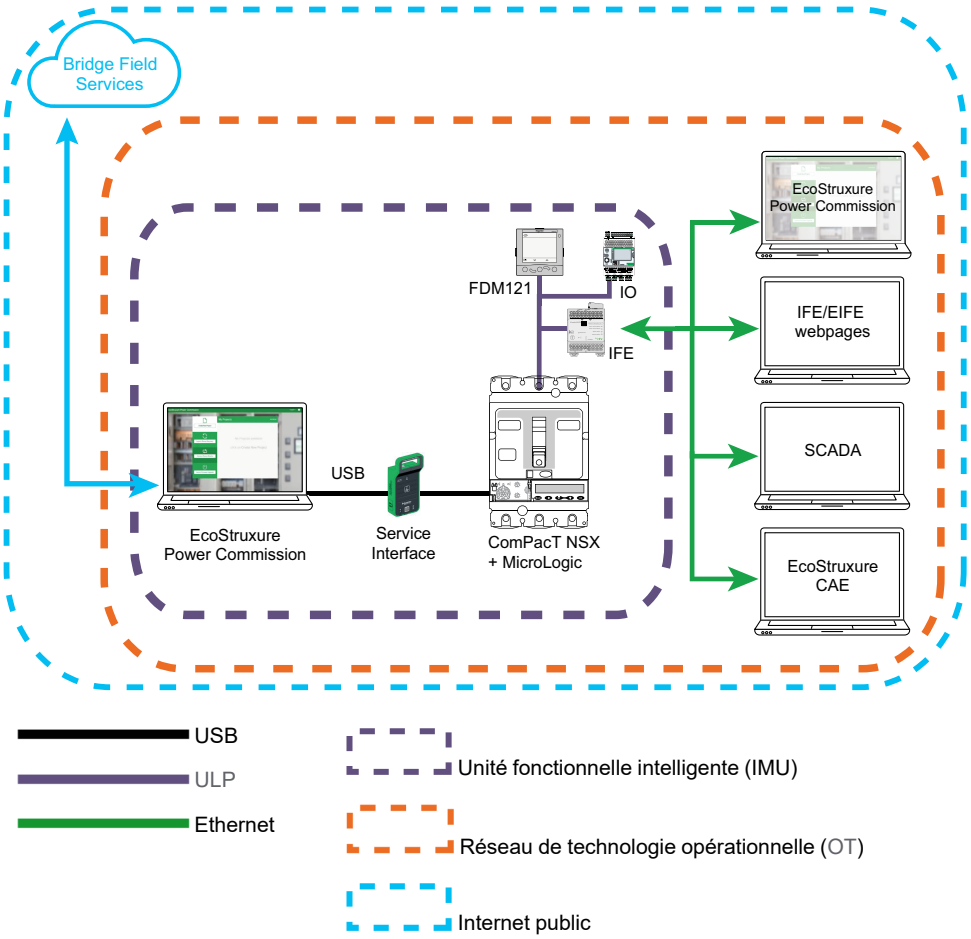
Pour communiquer avec le disjoncteur via son déclencheur MicroLogic, les voies suivantes sont disponibles :

- Interface humain-machine (IHM) MicroLogic
- Afficheur frontal FDM121 pour un disjoncteur
- Connexion au déclencheur MicroLogic à partir d'un PC exécutant le logiciel EcoStruxure Power Commission via l'interface de service
- Connexion Ethernet (protocole Modbus TCP/IP) via le réseau de technologie opérationnelle (OT) lorsque l'interface IFE est présente

- Connexion Modbus-SL via le réseau de technologie opérationnelle (OT) lorsque l'interface IFM est présente

Disjoncteur ComPacT NSX et PowerPacT à châssis H, J et L et environnement fonctionnel

La figure suivante montre les différents modes de communication avec le déclencheur MicroLogic du disjoncteur.



L'IMU englobe le disjoncteur ComPacT NSX ou PowerPacT à châssis H, J ou L, le déclencheur MicroLogic ainsi que les modules ULP, l'interface de communication et les modules IO associés.

Pour communiquer avec le disjoncteur via son déclencheur MicroLogic, les voies suivantes sont disponibles :

- Interface humain-machine (IHM) MicroLogic
- Afficheur frontal FDM121 pour un disjoncteur
- Connexion au déclencheur MicroLogic à partir d'un PC exécutant le logiciel EcoStruxure Power Commission via l'interface de service ou l'interface de maintenance USB
- Connexion Ethernet (protocole Modbus TCP/IP) via le réseau de technologie opérationnelle (OT) lorsque l'interface de communication est présente
- Connexion Modbus-SL via le réseau de technologie opérationnelle (OT) lorsque l'interface IFM est présente

Vulnérabilité du système aux cyberattaques

Chacune des voies de communication ci-dessus représente une vulnérabilité dans votre système, si les mesures de sécurité appropriées ne sont pas mises en

place. Ce guide fournit des consignes pour sécuriser ces voies et éviter les attaques intentionnelles ou une mauvaise utilisation accidentelle.

Les fonctions de sécurité suivantes sont conçues pour atténuer les menaces inhérentes à l'utilisation des interfaces IFE et EIFE et des appareils MasterPact, ComPacT et PowerPacT dans un environnement de technologie opérationnelle (OT).

Fonctionnalités de sécurité fournies

Les fonctionnalités de cybersécurité suivantes sont prises en charge par les IMU MasterPact, ComPacT et PowerPacT :

- Gestion des comptes utilisateur (sur les interfaces IFE et EIFE)
- Protection des codes d'accès
- Paramètres et services de sécurité configurables
- Mécanisme de mise à jour du firmware
- Communication sécurisée de machine à machine via Modbus TCP/TLS (sur les interfaces IFE et EIFE)
- Journaux de sécurité au format Syslog ou CSV (sur les interfaces IFE et EIFE)

Ces fonctionnalités assurent des moyens de sécurité qui contribuent à protéger le produit contre des menaces potentielles qui pourraient :

- perturber le fonctionnement du produit (problème de disponibilité)
- modifier les informations (problème d'intégrité)
- dévoiler des informations confidentielles (problème de confidentialité)

Comparaison des fonctions de sécurité entre l'interface IFE/EIFE et le serveur IFE

Le tableau suivant compare les fonctions de sécurité entre l'interface IFE/EIFE équipée du micrologiciel de version 004 et le serveur IFE équipé du micrologiciel de version 003 :

Fonctions	Interface EIFE (LV851001) Interface IFE (LV434001)	Serveur IFE (LV434002)
HTTP	Oui	Oui
HTTPS	Oui	Non
Serveur FTP	Oui	Oui
Client FTP	Oui	Oui
FTPS	Oui	Non
NTP	Oui	Non
SNTP	Non	Oui
RSTP	Oui	Non
Modbus TCP	Oui	Oui
Modbus Secure	Oui	Non
RBAC	Oui	Non
IEC 61850	Oui	Non
Syslog	Oui	Non
SMTP	Oui	Oui
Prise en charge IPv6 et détection DPWS	Oui	Non

SNMP	Oui	Oui
Temps de mise à niveau du firmware	4 minutes environ	16 minutes environ

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

Contenu de cette partie

Présentation

Cette section fournit des informations importantes à prendre en compte lors des phases de conception, de planification et d'installation d'un réseau de technologie opérationnelle (OT) comprenant l'unité fonctionnelle intelligente (IMU) MasterPact, ComPacT et PowerPacT. Les recommandations et consignes de cette section visent à mettre en place un environnement d'exploitation sécurisé.

Identification et protection des informations et opérations sensibles et critiques

Présentation

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

En règle générale :

- Les informations essentielles incluent des données et des opérations accessibles via l'IMU MasterPact, ComPacT et PowerPacT (par exemple, état du disjoncteur, déclencheur ou commande d'ouverture/fermeture).
- Les informations sensibles incluent toute information permettant d'accéder à votre installation et à votre réseau de technologie opérationnelle (par exemple, mots de passe ou codes d'accès des équipements ou des locaux sous clé).

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 connectés en réseau ;
- 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 et le niveau 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(e) pour accéder à l'unité fonctionnelle intelligente (IMU) MasterPact, ComPacT et PowerPacT, les informations et les opérations de contrôle disponibles varient.

Le tableau ci-après décrit l'accès aux opérations d'information et de contrôle via l'IMU MasterPact MTZ :

Opérations d'information et de contrôle	**Accès local**					**Accès à distance**
	IHM MicroLogic	**afficheur FDM121**	**NFC**	**Bluetooth Low Energy technology**	**USB**	**Ethernet / Modbus-SL**
Surveillance des données	Lecture	Lecture	Lecture	Lecture	Lecture	Lecture
Paramètres de protection	Lecture/ Ecriture	Lecture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture	Lecture/ Ecriture
Autres paramètres	Lecture/ Ecriture	Lecture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture	Lecture/ Ecriture
Ouverture/ Fermeture/ Réinitialisation	Non	Oui	Non	Oui	Oui	Oui

Le tableau suivant décrit l'accès aux opérations d'information et de contrôle via les IMU MasterPact NT/NW, ComPacT NS et PowerPacT à châssis P ou R :

Opérations d'information et de contrôle	**Accès local**			**Accès à distance**
	IHM MicroLogic	**afficheur FDM121**	**Prise de test**	**Ethernet / Modbus-SL**
Surveillance des données	Lecture	Lecture	Lecture	Lecture
Paramètres de protection	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Autres paramètres	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Ouverture/Fermeture/ Réinitialisation	Non	Oui	Oui	Oui

Le tableau suivant décrit l'accès aux opérations d'information et de contrôle via les IMU ComPacT NSX et PowerPacT à châssis H, J ou L :

Opérations d'information et de contrôle	**Accès local**			**Accès à distance**
	MicroLogic IHM	**afficheur FDM121**	**Prise de test**	**Ethernet / Modbus-SL**
Surveillance des données	Lecture	Lecture	Lecture	Lecture
Paramètres de protection	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Autres paramètres	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Ouverture/Fermeture/ Réinitialisation	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, page 26 ou l'accès distant, page 39 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, ComPacT et PowerPacT avec déclencheur ou unité de contrôle MicroLogic, les mots de passe sont requis pour les tâches suivantes :

- Exécution de commandes intrusives sur l'unité de contrôle MicroLogic, quel que soit le mode d'accès (Modbus-TCP/Modbus-SL, connexion USB ou technologie sans fil Bluetooth)
- Exécution de commandes intrusives sur le déclencheur MicroLogic, quel que soit le mode d'accès (Modbus-TCP/Modbus-SL, afficheur FDM121 ou port de test)
- Connexion au PC qui exécute le logiciel EcoStruxure Power Commission
- Connexion aux pages Web des interfaces IFE et EIFE
- Connexion aux pages Web du serveur IFE
- Connexion aux pages Web des interfaces IFE et EIFE via le logiciel d'affichage EcoStruxure Power Commission à partir d'une IMU MasterPact MTZ
- Connexion au serveur FTPS pour la configuration IEC 61850 des interfaces IFE et EIFE à partir d'un MasterPact MTZ

Recommandations de cybersécurité concernant la stratégie de mot de passe

⚠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.

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

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 ;
- gère les mots de passe à l'aide d'un référentiel ;
- interdit la réutilisation d'anciens mots de passe ;
- rappelle régulièrement aux utilisateurs les bonnes pratiques concernant les mots de passe.

Pour protéger votre système, vous devez au minimum :

- utiliser des mots de passe forts ;
- définir une longueur minimale de 10 caractères pour les mots de passe ;
- modifier le mot de passe périodiquement.

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.

Mot de passe pour les paramètres et contrôles critiques de MicroLogic

Lorsque vous accédez au déclencheur ou à l'unité de contrôle MicroLogic par une interface de communication, les commandes intrusives qui modifient le comportement du disjoncteur MasterPact, ComPacT et PowerPacT requièrent un mot de passe. Par exemple, pour modifier les paramètres de protection ou exploiter le disjoncteur, vous devez avoir le mot de passe MicroLogic.

Quatre mots de passe sont définis pour un déclencheur ou une unité de contrôle MicroLogic, un pour chacun des quatre profils d'utilisateur suivants :

- Administrateur
- Services
- Ingénieur
- Opérateur

Pour plus d'informations sur les profils d'utilisateur, consultez les guides utilisateur MicroLogic, page 8.

En cas de connexion via l'application Application EcoStruxure Power Device ou le logiciel EcoStruxure Power Commission, 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 de 0 à 9
- les lettres minuscules de a à z ;
- les lettres majuscules de A à Z.

Les mots de passe par défaut doivent être modifiés lors de l'installation initiale du disjoncteur MasterPact, ComPacT et PowerPacT et régulièrement après, à l'aide du logiciel EcoStruxure Power Commission. Stockez les mots de passe dans un référentiel de mots de passe. Ne communiquez les mots de passe qu'à un nombre limité d'utilisateurs de confiance. Le cas échéant, respectez les recommandations de la stratégie de mot de passe.

Mot de passe pour l'accès à distance à l'unité de contrôle MicroLogic X via l'interface IFE ou EIFE

Dans une IMU MasterPact MTZ, l'accès à l'unité de contrôle MicroLogic X est vérifié par un mécanisme de contrôle d'accès basé sur des rôles (RBAC) lorsque la connexion est établie à l'aide des moyens suivants :

- Logiciel EcoStruxure Power Commission via Ethernet
- Pages Web de l'interface IFE
- Pages Web de l'interface EIFE
- Serveur FTPS pour les interfaces IFE et EIFE.

Pour plus d'informations sur le mécanisme RBAC, reportez-vous à la section *Mots de passe pour les pages Web d'interface IFE ou EIFE et serveur FTPS IFE ou EIFE*, page 23.

Mot de passe d'accès distant aux déclencheurs ComPacT NSX via l'interface IFE

Dans une IMU ComPacT NSX équipée d'un déclencheur MicroLogic 5, 6 ou 7, l'accès au déclencheur MicroLogic est vérifié par un mécanisme de contrôle d'accès basé sur les rôles (RBAC) lorsque la connexion est établie à l'aide des moyens suivants :

- Logiciel EcoStruxure Power Commission via Ethernet
- Pages Web de l'interface IFE
- Serveur FTPS pour les interfaces IFE et EIFE.

Pour plus d'informations sur le mécanisme RBAC, reportez-vous à la section *Mots de passe pour les pages Web d'interface IFE ou EIFE et serveur FTPS IFE ou EIFE*, page 23.

Identifiants utilisateur et mots de passe pour PC en réseau

Les PC qui exécutent le logiciel EcoStruxure Power Commission ou qui accèdent au déclencheur ou à l'unité de contrôle MicroLogic par d'autres moyens (pages Web IFE ou 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.

Le cas échéant, respectez les recommandations de la stratégie de mot de passe.

Mots de passe pour les pages Web de l'interface IFE ou EIFE et le serveur FTPS IFE ou EIFE

L'accès aux pages Web de l'interfaceIFE, aux pages Web de l'interface EIFE et au serveur FTPS pour interfaces IFE et EIFE est vérifié par le mécanisme de contrôle d'accès basé sur les rôles (RBAC).

Le mécanisme RBAC permet d'attribuer aux utilisateurs un rôle qui définit les fonctionnalités auxquelles ils peuvent accéder.

L'administrateur de la sécurité de votre système répertorie les utilisateurs du système et attribue un rôle à chacun d'eux.

L'administrateur de la sécurité peut gérer les utilisateurs de l'interface IFE ou EIFE :

- Sur les pages Web de l'interface IFE ou EIFE
- A l'aide du logiciel EcoStruxure Cybersecurity Admin Expert (CAE)

L'administrateur de sécurité peut utiliser le logiciel CAE pour définir la politique de sécurité du système.

La politique de sécurité s'applique à tous les éléments du système qui sont compatibles avec le logiciel CAE. Pour les systèmes basse tension, elle s'applique aux interfaces IFE et EIFE du système.

L'administrateur de la sécurité peut définir les paramètres suivants de la poligique de sécurité avec le logiciel CAE :

- Période d'inactivité minimum. Après un certain délai d'inactivité de l'utilisateur, les pages Web de l'interface IFE ou EIFE sont verrouillées. L'utilisateur doit entrer le mot de passe à nouveau pour les déverrouiller.
- Nombre maximum de tentatives de connexion.
- Durée de la période de verrouillage.

Pour plus d'informations, consultez le document CAE_EN_UM_B4.1 *EcoStruxure Cybersecurity Admin Expert User Guide*.

Mots de passe pour les pages Web du serveur IFE

Chaque utilisateur des pages Web du serveur IFE a un identifiant utilisateur et un mot de passe personnels pour se connecter à ces pages. Un utilisateur doit modifier le mot de passe après sa connexion initiale aux pages Web.

Vous devez identifier les utilisateurs qui, au sein de votre organisation, ont besoin de se connecter aux pages Web du serveur IFE et respecter les recommandations de la stratégie de mot de passe (le cas échéant).

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 communication OT 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 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 sont protégés contre le piratage via la technologie sans fil Bluetooth ou via Internet.
- Ne contournez pas les stratégies de sécurité pour des raisons de commodité.

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

Recommandations de cybersécurité pour l'accès local

Contenu de cette partie

Présentation

Cette section répertorie les chemins d'accès local au disjoncteur MasterPact, ComPacT et PowerPacT. Elle fournit également des recommandations pour sécuriser ces chemins d'accès. Ces éléments importants sont à prendre en compte pour l'exploitation.

Restriction de l'accès local au disjoncteur MasterPact, ComPacT et PowerPacT

Présentation

L'unité fonctionnelle intelligente (IMU) MasterPact, ComPacT et PowerPacT 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, ComPacT et PowerPacT

L'accès local à l'unité fonctionnelle intelligente MasterPact, ComPacT et PowerPacT 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, ComPacT et PowerPacT en l'installant dans un local sous clé pour éviter :

- tout accès non autorisé à l'IHM MicroLogic, 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 Application EcoStruxure Power Device
- tout accès non autorisé à la communication NFC sans fil, avec le risque de divulgation de données
- toute connexion non autorisée via le port mini USB de l'unité de contrôle MicroLogic, avec le risque de modification de paramètres depuis le logiciel EcoStruxure Power Commission ou un smartphone exécutant Application EcoStruxure Power Device
- toute connexion non autorisée via le port de test du déclencheur MicroLogic, avec le risque de modification de paramètres à partir du logiciel EcoStruxure Power Commission à l'aide de l'interface de service ou de l'interface de maintenance USB
- 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 au déclencheur ou à l'unité de contrôle MicroLogic bénéficient d'une protection renforcée conformément aux dernières consignes en date du fournisseur.

Lorsque le disjoncteur MasterPact, ComPacT et PowerPacT 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

Fonctions accessibles à partir de l'IHM

Toute personne ayant accès à l'armoire qui héberge le disjoncteur a accès à l'IHM MicroLogic.

Certaines fonctions critiques, comme les paramètres de protection de l'équipement, sont configurables à partir de l'IHM MicroLogic.

Recommandations pour protéger l'accès par l'IHM MicroLogic

L'IHM MicroLogic n'est pas protégée par un mot de passe et toutes les IHM MicroLogic ne peuvent pas être verrouillées physiquement pour empêcher l'accès à l'écran d'affichage. Par conséquent, pour protéger l'accès à l'IHM :

- Scellez le capot de protection de l'IHM MicroLogic si cela est possible.
- Installez le disjoncteur 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, consultez la section Mise en œuvre d'une stratégie d'accès restreint, page 27.

Verrouillage des paramètres de protection

Vous pouvez verrouiller les paramètres de protection du disjoncteur 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, reportez-vous aux guides d'utilisation MicroLogic, page 8.

Recommandations pour protéger l'accès via NFC (MasterPact MTZ)

Fonctions accessibles via NFC

La communication sans fil NFC (Near Field Communication) permet de télécharger des données de diagnostic depuis l'unité de contrôle MicroLogic X vers un smartphone, même lorsque l'unité de contrôle 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 suivantes doivent être remplies :

- Vous devez avoir physiquement accès au local hébergeant le disjoncteur MasterPact MTZ, et à l'armoire de l'équipement.
- Vous devez avoir l'application Application EcoStruxure Power Device installée sur votre smartphone.
- Le smartphone doit prendre en charge 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 via NFC.

Vous trouverez la procédure détaillée d'établissement d'une connexion NFC dans le document *MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur*, page 8.

Recommandations générales pour protéger l'accès par NFC

Pour protéger l'accès aux données accessibles par NFC sans fil, il est recommandé de prendre les précautions suivantes :

- Installez le disjoncteur MasterPact MTZ dans un local verrouillé, afin que seule une personne autorisée 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, page 27.

Recommandations pour la communication NFC

Pour protéger l'accès à des fonctions accessibles viaNFC sans fil, il est recommandé d'appliquer les précautions suivantes :

- Déconnectez le smartphone d'Internet (par exemple, en activant le mode avion) pendant une connexion NFC à l'unité de contrôle MicroLogic X.
- N'entrez pas de code d'appariement si vous y êtes invité, car cela n'est pas nécessaire pour une connexion NFC.

Recommandations pour utiliser Application EcoStruxure Power Device

Pour restreindre l'accès à l'unité de contrôle MicroLogic X à partir d'un smartphone exécutant Application EcoStruxure Power Device, il est recommandé

de n'utiliser que l'application Application EcoStruxure Power Device 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 Application EcoStruxure Power Device sont protégés par un mot de passe et utilisés uniquement dans le cadre professionnel.
- Renforcez les smartphones équipés de l'application Application EcoStruxure Power Device 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 sensible sur smartphone.

Recommandations pour protéger l'accès via la technologie sans fil Bluetooth® (MasterPact MTZ)

Fonctions accessibles via la technologie sans fil Bluetooth

AVIS

RISQUE DE FONCTIONNEMENT IMPRÉVU

- 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 MicroLogic X sont définies par défaut sur la valeur minimale, sauf la protection long retard qui est définie par défaut sur la valeur maximale.

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

Grâce à la technologie sans fil Bluetooth Low Energy, vous pouvez accéder à l'unité de contrôle MicroLogic X à partir d'un smartphone exécutant Application EcoStruxure Power Device. Cette application offre une interface orientée tâches avec l'unité de contrôle. Les données transférées via Bluetooth sont chiffrées à l'aide de l'algorithme AES 128 bits.

Conditions requises pour établir une connexion Bluetooth

Pour établir une connexion sans fil Bluetooth à l'unité de contrôle MicroLogic X, les conditions suivantes doivent être remplies :

- 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 se connecter à une unité de contrôle.
- Vous devez disposer d'un smartphone équipé de l'application Application EcoStruxure Power Device.
- Le smartphone doit prendre en charge la technologie sans fil Bluetooth Low Energy (version 4.0 ou supérieure).
- Vous devez avoir accès à l'unité de contrôle MicroLogic X pour activer la fonction Bluetooth en appuyant sur le bouton-poussoir d'activation, et vous devez rester physiquement à portée (généralement 20 à 30 mètres) durant toute la durée de la connexion.
- Vous devez entrer le code d'appariement à 6 chiffres généré aléatoirement par l'unité de contrôle MicroLogic X et affiché sur l'IHM MicroLogic X.

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

Vous trouverez les procédures détaillées d'établissement d'une connexion Bluetooth dans le document *MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur*, page 8.

Recommandations générales pour protéger l'accès via la technologie sans fil Bluetooth

Pour protéger l'accès aux fonctions accessibles via la technologie sans fil Bluetooth, les précautions suivantes sont recommandées :

- Installez le disjoncteur MasterPact MTZ dans un local verrouillé, afin que seule une personne autorisée 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, page 27.

Recommandations pour utiliser la technologie sans fil Bluetooth

La mise en oeuvre de la fonction Bluetooth est conforme à la publication spéciale NIST 800-121 Révision 1. Néanmoins, pour protéger l'accès aux fonctions accessibles via la technologie sans fil Bluetooth, les précautions suivantes sont recommandées :

- Désactivez la fonction Bluetooth sur l'unité de contrôle MicroLogic X et ne l'activez que lorsque vous êtes prêt à établir une connexion.

  Vous trouverez les procédures détaillées pour désactiver la fonction Bluetooth dans le document *MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur*, page 8.
- Configurez le temporisateur de déconnexion de la fonction Bluetooth sur 5 minutes.
- Sauf si vous démarrez une connexion Bluetooth, la fonction Bluetooth ne doit pas être activée à partir du bouton-poussoir situé sur la face avant de l'unité de contrôle MicroLogic X. La fonction Bluetooth doit rester désactivée tant qu'elle n'est pas utilisée.
- Appuyez sur le bouton-poussoir Bluetooth pour mettre fin à la communication lorsque vous avez terminé.
- L'appariement doit être effectué uniquement lorsque cela est nécessaire et dans une zone sécurisée.
- N'entrez pas de code d'appariement si vous y êtes invité de manière inattendue.
- Pendant l'appariement Bluetooth, conservez le smartphone aussi proche que possible de l'unité de contrôle MicroLogic X.

Recommandations pour utiliser Application EcoStruxure Power Device

Pour restreindre l'accès à l'unité de contrôle MicroLogic X à partir d'un smartphone exécutant Application EcoStruxure Power Device, il est recommandé de n'utiliser que l'application Application EcoStruxure Power Device 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 Application EcoStruxure Power Device sont protégés par un mot de passe et utilisés uniquement dans le cadre professionnel.
- Renforcez les smartphones équipés de l'application Application EcoStruxure Power Device 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 pendant une connexion Bluetooth à l'unité de contrôle MicroLogic X.
- Ne stockez aucune information sensible sur smartphone.

Recommandations pour protéger l'accès à l'unité de contrôle MicroLogic X par le port mini-USB (MasterPact MTZ)

Fonctions accessibles par le port mini-USB

Il est possible d'accéder aux fonctions de l'unité de contrôle MicroLogic X en :

- connectant un PC qui exécute le logiciel EcoStruxure Power Commission au mini-port USB de l'unité de contrôle ;
- connectant un smartphone qui exécute Application EcoStruxure Power Device 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 suivantes doivent être remplies :

- 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 EcoStruxure Power Commission.
- 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 Application EcoStruxure Power Device.

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 que seule une personne autorisée 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, page 27.

Recommandations pour les PC exécutant le logiciel EcoStruxure Power Commission

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 EcoStruxure Power Commission requièrent un ID utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts, page 21.
- 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 EcoStruxure Power Commission.
- Mettez à jour les applications antivirus pour PC.

Recommandations pour les smartphones qui exécutent Application EcoStruxure Power Device

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 Application EcoStruxure Power Device sont protégés par un mot de passe et utilisés uniquement à titre professionnel.
- Renforcez les smartphones exécutant Application EcoStruxure Power Device 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 sensible sur smartphone.

Recommandations pour configurer IEC 61850

Utilisez le protocole FTPS pour charger le fichier de configuration IEC 61850 vers l'interface IFE ou EIFE.

Recommandations relatives à la protection de l'accès au déclencheur MicroLogic par le port de test

Fonctions accessibles par le port de test via l'interface de maintenance USB

Il est possible d'accéder aux fonctions du déclencheur MicroLogic en connectant un PC exécutant le logiciel EcoStruxure Power Commission au port de test du déclencheur via l'interface de maintenance USB.

L'interface de maintenance USB permet de raccorder un PC exécutant le logiciel EcoStruxure Power Commission au port de test du déclencheur en vue d'effectuer toute la série de vérifications, tests et réglages du déclencheur MicroLogic.

L'interface de maintenance USB est compatible avec les appareils suivants :

- Disjoncteurs ComPacT NSX
- Disjoncteurs PowerPacT à châssis H, J et L

Fonctions accessibles par le port de test via l'interface de service

Il est possible d'accéder aux fonctions du déclencheur MicroLogic en connectant un PC exécutant le logiciel EcoStruxure Power Commission au port de test du déclencheur via l'interface de service.

L'interface de service permet de raccorder un PC exécutant le logiciel EcoStruxure Power Commission au port de test du déclencheur en vue d'effectuer toute la série de vérifications, tests et réglages du déclencheur MicroLogic.

L'interface de service est compatible avec les appareils suivants :

- Disjoncteurs MasterPact NT/NW
- Disjoncteurs EasyPact™ MVS
- Disjoncteurs ComPacT NS
- Disjoncteurs PowerPacT à châssis P et R
- Disjoncteurs ComPacT NSX
- Disjoncteurs PowerPacT à châssis H, J et L

Recommandations générales pour protéger l'accès par port de test

Pour protéger l'accès aux fonctions disponibles via le port de test sur le déclencheur MicroLogic, les précautions suivantes sont recommandées :

- Installez le disjoncteur MasterPact NT/NW, ComPacT ou PowerPacT dans un local pouvant être verrouillé, afin que seule une personne autorisée puisse accéder au déclencheur MicroLogic.
- 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, ComPacT et PowerPacT, page 27.

Recommandations pour les PC exécutant le logiciel EcoStruxure Power Commission

Pour protéger l'accès au déclencheur MicroLogic à partir d'un PC connecté en local au port de test situé à l'avant du déclencheur, les précautions suivantes sont recommandées :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Vérifiez que les PC qui exécutent le logiciel EcoStruxure Power Commission requièrent un ID utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts, page 21.
- 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 EcoStruxure Power Commission.
- Mettez à jour les applications antivirus pour PC.

Recommandations relatives à la protection de l'accès au déclencheur MicroLogic via l'Afficheur FDM121

Fonctions accessibles via Afficheur FDM121

Il est possible d'accéder aux fonctions du déclencheur MicroLogic à partir de l'afficheur FDM121 connecté à l'IMU.

L'afficheur FDM121 indique les mesures, les alarmes et les données d'assistance à l'exploitation en provenance de l'IMU. L'afficheur FDM121 peut être utilisé pour contrôler :

- Un disjoncteur équipé d'un mécanisme moteur
- L'application prédéfinie exécutée par le module IO.

L'afficheur FDM121 est compatible avec les appareils suivants :

- Disjoncteurs MasterPact MTZ
- Disjoncteurs MasterPact NT/NW
- Disjoncteurs ComPacT NS
- Disjoncteurs PowerPacT à châssis P et R
- Disjoncteurs ComPacT NSX
- Disjoncteurs PowerPacT à châssis H, J et L

Recommandations générales pour protéger l'accès par Afficheur FDM121

Pour protéger l'accès aux fonctions disponibles sur l'afficheur FDM121, les précautions suivantes sont recommandées :

- Installez le disjoncteur MasterPact, ComPacT ou PowerPacT et l'afficheur FDM121 associé dans un local pouvant être verrouillé afin que seules les personnes autorisées puissent accéder à l'afficheur FDM121.
- Maintenez ce local verrouillé à tout moment.
- Ne donnez la clé ou le code d'accès qu'aux personnes autorisées.

Pour plus d'informations, reportez-vous aux recommandations relatives à la restriction de l'accès local au disjoncteur MasterPact, ComPacT ou PowerPacT, page 27.

Recommandations de cybersécurité pour l'accès distant

Contenu de cette partie

Présentation

Cette section répertorie les chemins d'accès distant au disjoncteur MasterPact, ComPacT et PowerPacT. Elle fournit également des recommandations pour sécuriser ces chemins d'accès. Ces éléments importants sont à prendre en compte pour l'exploitation.

Restriction de l'accès distant au disjoncteur MasterPact, ComPacT et PowerPacT

Présentation

L'unité fonctionnelle intelligente (IMU) MasterPact, ComPacT et PowerPacT 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, ComPacT et PowerPacT

Selon l'architecture de votre système, il existe probablement plusieurs voies d'accès distant au disjoncteur MasterPact, ComPacT et PowerPacT.

Il est primordial de contrôler l'accès distant à votre système, car un accès distant par les voies de communication suivantes permet de prendre le contrôle total de votre installation :

- logiciel EcoStruxure Power Commission au moyen d'une connexion Ethernet via une interface IFE, EIFE ou IFM
- logiciel EcoStruxure Power Commission au moyen d'une connexion Modbus-SL via une interface IFM
- pages Web IFE ou EIFE au moyen d'une connexion Ethernet via une interface IFE ou EIFE

Vous devez notamment prendre en compte :

- les modes d'accès au système à l'aide des différents chemins de communication disponibles, page 13 ;
- les informations et contrôles disponibles par chaque chemin d'accès, page 20.

Protocoles pris en charge

Les interfaces IFE et EIFE prennent en charge les protocoles de communication suivants :

- HTTPS pour la configuration via les pages Web intégrées
- Modbus TCP/IP pour la communication avec d'autres équipements OT
- Modbus TCP sur TLS
- DHCP pour l'adressage IP du réseau
- DNS pour la résolution de noms réseau
- SNTP pour la synchronisation horaire
- DPWS pour la distribution réseau
- SMTPS pour l'envoi de messages électroniques
- FTPS pour la configuration IEC 61850 et la notification d'événements
- IEC 61850 pour la communication avec les équipements et systèmes de sous-stations

L'interface IFM prend en charge le protocole de communication Modbus-SL.

Les applications MasterPact MTZ prennent en charge les protocoles de communication suivants :

- Technologie sans fil Bluetooth pour la communication avec Application EcoStruxure Power Device
- NFC pour télécharger des données de diagnostic

Activation et désactivation du contrôle à distance du disjoncteur MasterPact, ComPacT et PowerPacT

Le contrôle à distance du disjoncteur MasterPact, ComPacT et PowerPacT désigne les opérations suivantes :

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

Si le contrôle à distance du disjoncteur MasterPact, ComPacT et PowerPacT n'est pas une nécessité, il est vivement recommandé de le désactiver à l'aide de l'interface IFE ou EIFE, du serveur IFE ou de l'interface IFM. Par défaut, le contrôle à distance est activé.

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

Sur l'interface EIFE, connectez un PC exécutant le logiciel EcoStruxure Power Commission au port mini-USB situé à l'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 commandes de contrôle à distance envoyées sur le réseau Modbus-SL.

Verrouillage des paramètres de protection (MasterPact MTZ)

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 la section *MasterPact MTZ - MicroLogic X Unité de contrôle - Guide utilisateur*, page 8.

Désactivation des services réseau IP inutilisés

Les ports de communication situés sur l'interface IFE ou EIFE peuvent être désactivés depuis les pages Web de l'interface IFE ou EIFE.

Recommandations :

- Désactivez les ports de communication inutilisés de l'interface IFE ou EIFE.
- Accédez aux pages Web de l'interface IFE ou EIFE en utilisant le service HTTPS au lieu du service HTTP.
- Accédez au logiciel EPC en utilisant la mise en service sécurisée (disponible dans les pages Web de l'interface IFE ou EIFE) pour les unités de contrôle MicroLogic MasterPact MTZ et les déclencheurs MicroLogic 5, 6 ou 7 ComPacT NSX.

Utilisation de la liste de contrôle d'accès (ACL)

Lorsque le contrôle à distance est nécessaire, il est recommandé d'utiliser la fonctionnalité de filtrage IP des interfaces IFE et EIFE pour dresser la liste des adresses IP des applications (SCADA par exemple) qui sont autorisées à communiquer avec l'IMU). Cette liste est appelée liste de contrôle d'accès (ACL).

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

Présentation

Lors de la conception et de la mise en œuvre de votre réseau de technologie opérationnelle, 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, ComPacT et PowerPacT.

Vous devez notamment prendre en compte :

- l'utilisation de pare-feu ;
- la création de zones démilitarisées ;
- l'utilisation de solutions 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 procédures de réponse aux incidents.

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

Outre les précautions ci-dessus, vous devez également respecter les directives et recommandations générales concernant la séparation de vos réseaux (voir *How Can I Reduce Vulnerability to Cyber Attacks?*).

Recommandations pour protéger l'accès distant au déclencheur ou à l'unité de contrôle MicroLogic via Ethernet

Fonctions accessibles via Ethernet

Lorsqu'un PC exécutant le logiciel de surveillance et de contrôle (SCADA , logiciel EcoStruxure Power Commission) est connecté au réseau Ethernet (Modbus/TCP), les fonctions du déclencheur ou de l'unité de contrôle MicroLogic sont accessibles dans les cas suivants :

- Le disjoncteur MasterPact, ComPacT et PowerPacTest connecté via une interface IFE ou un serveur IFE.
- Le disjoncteur MasterPact MTZ est connecté via l'interface EIFE.
- Le disjoncteur MasterPact, ComPacT et PowerPacT est connecté via une interface IFM hébergée sur un serveur IFE.

Conditions requises pour établir une connexion Ethernet

Pour établir une connexion Ethernet au déclencheur ou à l'unité de contrôle MicroLogic, les conditions suivantes doivent être remplies :

- Le déclencheur ou l'unité de contrôle MicroLogic doit être sous tension.
- Le déclencheur ou l'unité de contrôle MicroLogic doit être connectée à un réseau Ethernet via l'une des interfaces suivantes :
  - Une interface IFE ou EIFE
  - Un serveur IFE
  - Une interface IFM hébergée sur un serveur IFE
- Vous devez avoir un PC ou un autre équipement (afficheur FDM128 ou automate programmable, par exemple) exécutant le logiciel de surveillance et de contrôle (SCADA, EcoStruxure Power Commission) connecté au réseau Ethernet pour permettre l'accès à distance
- Vous devez avoir un PC qui exécute un navigateur Web connecté au réseau Ethernet, pour accéder aux pages Web de l'interface IFE ou EIFE.
- Vous devez avoir un ID utilisateur et un mot de passe avec les droits d'accès appropriés pour vous connecter aux :
  - pages Web des interfaces IFE et EIFE
  - pages Web du serveur IFE
  - serveur FTPS pour les interfaces IFE et EIFE
  - logiciel EcoStruxure Power Commission connecté via une interface IFE ou EIFE
- Vous devez avoir un ID utilisateur et un mot de passe avec les droits d'accès appropriés pour vous connecter au logiciel EcoStruxure Power Commission.

Recommandations concernant les PC connectés à Ethernet

Pour protéger l'accès au déclencheur ou à l'unité de contrôle MicroLogic à partir d'un PC en réseau, les précautions suivantes sont recommandées :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Assurez-vous que le PC qui fournit l'accès au déclencheur ou à l'unité de contrôle MicroLogic via Ethernet (par exemple, à l'aide des pages Web de l'interface IFE ou EIFE, des pages Web du serveur IFE ou du SCADA) exige un ID utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts, page 23.

- Utilisez la fonction de filtrage IP des interfaces IFE et EIFE et du serveur IFE pour autoriser la communication uniquement avec les adresses IP distantes sélectionnées.
- Assurez-vous 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 au déclencheur ou à l'unité de contrôle MicroLogic à partir d'un PC en réseau.
- Mettez à jour les applications antivirus pour PC.

Outre les précautions ci-dessus, vous devez également respecter les consignes et recommandations générales concernant la protection de votre installation (voir) *How Can I Reduce Vulnerability to Cyber Attacks?*.

Recommandations concernant la communication de machine à machine

Pour les systèmes prenant en charge Modbus TCP sur TLS, activez le mode de sécurité de connexion TLS dans les pages Web de l'interface IFE ou EIFE.

La communication sécurisée de machine à machine nécessite des composants qui se connectent à l'interface IFE ou EIFE pour prendre en charge la communication Modbus sécurisée.

Recommandations concernant les journaux de sécurité

Pour vous assurer que les journaux de sécurité sont téléchargés régulièrement, utilisez :

- La fonction d'exportation automatique des journaux via le service Syslog à partir de l'interface IFE ou EIFE.
- L'exportation manuelle des journaux au format CSV à partir de l'interface IFE ou EIFE.

Recommandations pour protéger l'accès distant au déclencheur ou à l'unité de contrôle MicroLogic via Modbus-SL

Fonctions accessibles via Modbus-SL

Lorsqu'un PC exécutant le logiciel de surveillance et de contrôle (SCADA) est connecté au réseau Modbus-SL, les fonctions du déclencheur ou de l'unité de contrôle MicroLogic sont accessibles quand le disjoncteur MasterPact, ComPacT et PowerPacT est connecté à une interface IFM.

Conditions requises pour établir une connexion Modbus-SL

Pour établir une connexion Modbus-SL au déclencheur ou à l'unité de contrôle MicroLogic, les conditions suivantes doivent être remplies :

- Le déclencheur ou l'unité de contrôle MicroLogic doit être sous tension.
- Le déclencheur ou l'unité de contrôle MicroLogic doit être connecté(e) à une interface IFM.
- Vous devez avoir un PC ou un autre équipement (automate programmable, par exemple) exécutant le logiciel de contrôle et de surveillance (SCADA) connecté au réseau Modbus-SL pour permettre l'accès à distance.
- Vous devez avoir un ID utilisateur et un mot de passe avec les droits d'accès appropriés pour vous connecter au logiciel EcoStruxure Power Commission.

Recommandations pour les PC connectés à Modbus-SL

Pour protéger l'accès au déclencheur ou à l'unité de contrôle MicroLogic à partir d'un PC en réseau, les précautions suivantes sont recommandées :

- Conservez les PC sous clé lorsqu'ils sont inutilisés.
- Assurez-vous que le PC qui fournit l'accès au déclencheur ou à l'unité de contrôle MicroLogic à l'aide de Modbus-SL (par exemple, via SCADA) requiert un identifiant utilisateur et un mot de passe.
- Imposez l'utilisation de mots de passe forts, page 23.
- 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 au déclencheur ou à l'unité de contrôle MicroLogic à partir d'un PC en réseau.
- Mettez à jour les applications antivirus pour PC.

Outre les précautions ci-dessus, vous devez également respecter les consignes et recommandations générales concernant la protection de votre installation (voir *How Can I Reduce Vulnerability to Cyber Attacks?*).

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

Contenu de cette partie

Installation de 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.

Afin de garantir l'intégrité et l'authenticité des composants de l' IMU MasterPact, ComPacT et PowerPacT, à savoir l'unité de contrôle MicroLogic X, le serveur IFE, l'interface IFE ou EIFE, l'interface IFM, le module IO et le module afficheur FDM121, le firmware Schneider Electric d'origine est signé numériquement.

Mettez à niveau le firmware à l'aide du logiciel EcoStruxure Power Commission. Vous devez avoir la dernière version en date du logiciel EcoStruxure Power Commission. Utilisez le logiciel EcoStruxure Power Commission pour mettre à niveau le firmware à l'aide du menu Firmware.

Recommandations de cybersécurité concernant les mises à niveau du firmware

⚠AVERTISSEMENT

RISQUE DE FONCTIONNEMENT IMPRÉVU

- Mettez à jour votre logiciel EcoStruxure Power Commission dès que possible lorsque vous recevez une notification indiquant qu'une mise à jour est disponible.
- Utilisez cette dernière version du logiciel EcoStruxure Power Commission pour mettre à jour le firmware 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 firmware antérieur à la date de la révocation.

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

Lors de l'installation de mises à niveau du firmware sur les composants de l' IMU MasterPact, ComPacT et PowerPacT, les recommandations suivantes s'appliquent :

- N'utilisez que la version la plus récente du logiciel EcoStruxure Power Commission pour télécharger et installer les mises à niveau du firmware.
- Renforcez le PC qui exécute le logiciel EcoStruxure Power Commission, en respectant les dernières consignes en date du fournisseur du système d'exploitation.
- Installez les mises à niveau selon les pratiques de technologie opérationnelle (OT) en vigueur, par exemple en les testant sur un environnement hors production (le cas échéant) avant leur installation et leur déploiement dans le système de production.

Consultez la note de publication de firmware, page 8 appropriée pour savoir si la dernière mise à niveau apporte des améliorations en matière de cybersécurité. Si tel est le cas, l'installation de cette version est recommandée.

Firmware signé

Le firmware conçu pour l'unité de contrôle MicroLogic X et les modules ULP est signé à l'aide de l'infrastructure de clé publique (PKI))de Schneider Electric. Les signatures numériques sont authentifiées à l'aide du certificat public présent dans le logiciel EcoStruxure Power Commission.

Lorsque le firmware est chargé sur un appareil via le logiciel EcoStruxure Power Commission, la signature numérique du package de mise à jour est vérifiée automatiquement. Cette vérification utilise le certificat public présent dans chaque appareil.

Pour des raisons de sécurité, les certificats publics sont passibles de modifications. Par conséquent, vous devez vérifier que la version du logiciel EcoStruxure Power Commission que vous utilisez pour télécharger et installer les mises à jour du firmware est la dernière. Dans la dernière version du logiciel EcoStruxure Power Commission, les certificats publics utilisés pour signer le firmware sont à jour.

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

Avantages d'utiliser le logiciel EcoStruxure Power Commission pour les mises à niveau du firmware

Le logiciel EcoStruxure Power Commission joue un rôle important dans l'intégrité de votre réseau de technologie opérationnelle pendant les mises à niveau du firmware. N'utilisez que la version la plus récente du logiciel EcoStruxure Power Commission 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 packages de firmware dans l'unité de contrôle MicroLogic X ou le module ULP à partir du centre de téléchargement officiel de Schneider Electric à l'aide du logiciel EcoStruxure Power Commission, leur signature numérique est automatiquement vérifiée.
- Lorsque vous téléchargez un firmware dans l'unité de contrôle MicroLogic X ou le module ULP (à l'aide du logiciel EcoStruxure Power Commission sur une connexion USB ou Ethernet), sa signature numérique est automatiquement vérifiée.

Le logiciel EcoStruxure Power Commission effectue ces vérifications automatiques en fonction de la validité du certificat public utilisé.

Vous trouverez les procédures détaillées de mise à jour du firmware MicroLogic dans le document *MicroLogic Trip Units and Control Units - Firmware History*, page 8.

Achat et installation de MasterPact MTZDigital 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 en contactant le Customer Care Center (CCC).

Les Digital Modules conçus pour l'unité de contrôle MicroLogic X sont signés numériquement pour une sécurité accrue à l'aide de l'infrastructure de clé publique (PKI) de Schneider Electric. PKI garantit l'authenticité et l'intégrité de ces téléchargements. Les Digital Modules doivent être installés à l'aide du logiciel EcoStruxure Power Commission.

Recommandations de cybersécurité pour installer des Digital Modules

⚠AVERTISSEMENT

RISQUE DE FONCTIONNEMENT IMPRÉVU

- Mettez à jour votre logiciel EcoStruxure Power Commission dès que possible lorsque vous recevez une notification indiquant qu'une mise à jour est disponible.
- Utilisez cette dernière version du logiciel EcoStruxure Power Commission pour mettre à jour le firmware 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 firmware antérieur à la date de la révocation.

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

Lors de l'installation de Digital Modules pour l'unité de contrôle MicroLogic X, les recommandations suivantes s'appliquent :

- Installez les Digital Modules selon les pratiques de technologie opérationnelle (OT) en vigueur, notamment en les testant sur un environnement hors production avant leur installation et leur déploiement dans le système de production.
- N'utilisez que la version la plus récente du logiciel EcoStruxure Power Commission 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.

N'utilisez que le logiciel EcoStruxure Power Commission pour installer les Digital Modules de l'unité de contrôle MicroLogic X.

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

- Lorsque vous mettez à jour le firmware d'un équipement de l'IMU à l'aide du logiciel EcoStruxure Power Commission via une connexion USB ou Ethernet, la signature numérique de la mise à jour est automatiquement vérifiée.
- Lorsque vous téléchargez un Digital Module dans l'unité de contrôle MicroLogic X à l'aide du logiciel EcoStruxure Power Commission via une connexion USB, la signature numérique du Digital Module est automatiquement vérifiée.

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

Pour en savoir plus sur le téléchargement et l'installation des Digital Modules, consultez le document DOCA0144EN*MasterPact MTZ - MicroLogic X Control Unit - Firmware Release Notes*.

Portail d'assistance à la cybersécurité de Schneider Electric

Présentation

Le cybersecurity support portal 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 compétentes, les chercheurs indépendants, les chefs de produit et tous les clients concernés.

Informations disponibles sur le portail d'assistance à la cybersécurité de Schneider Electric

Ce portail fournit les services suivants :

- 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 de cybersécurité

Recommandations de cybersécurité pour la mise au rebut ou la mise hors service

Les interfaces EIFE et IFE et le serveur IFE contiennent des informations confidentielles configurées lors de la mise en service, ainsi que des valeurs de données récentes et des journaux. Ces informations peuvent notamment inclure des mots de passe ou des consommations d'énergie mesurées.

Il est nécessaire d'effectuer une réinitialisation d'usine avant de mettre au rebut l'interface EIFE ou IFE ou le serveur IFE. Pour plus d'informations, reportez-vous au guide utilisateur de votre interface.

Glossaire

B

Bluetooth Low Energy:

Technologie de réseau local sans fil, économe en énergie.

C

Code d'appariement:

Code composé de chiffres qui est utilisé pour vérifier l'identité de l'individu lors de l'établissement d'une connexion Bluetooth.

Connectivité ULP:

ULP est une liaison de communication rapide, dédiée à la surveillance et au contrôle des disjoncteurs. Elle connecte le disjoncteur à une interface Ethernet ou à un module IO. ULP fonctionne à un débit de 1 Mb/s et est Plug-and-Play.

F

FTP - File Transfer Protocol:

Protocole réseau qui permet de transférer des fichiers sur Internet entre deux ordinateurs.

FTPS - Protocole de transfert de fichiers (FTP) sécurisé:

Variante du protocole de transfert standard (FTP) qui ajoute une couche de sécurité sur les données en transit via une connexion par protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security).
.

H

HTTP - Hypertexot Transfer Protocol:

Protocole réseau qui gère la distribution des fichiers et données sur le Web.

HTTPS - Hypertext Transfer Protocol Secure:

Variante du protocole de tranfert web standard (HTTP) qui ajoute une couche de sécurité sur les données en transit via une connexion par protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security).

I

IHM - 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 (Intelligent Modular Unit - unité fonctionnelle intelligente):

Le disjoncteur équipé de ses composants internes de communication (déclencheur ou unité de contrôle MicroLogic) et de modules ULP externes (module IO) connectés à une même interface de communication constituent une unité fonctionnelle intelligente (IMU).

Interface EIFE:

Interface Ethernet intégrée, qui est un module optionnel du disjoncteur débrochable MasterPact MTZ. Avec ce module, le disjoncteur est accessible sur un réseau Ethernet. L'accès aux pages Web de l'interface EIFE et au serveur FTPS EIFE est autorisé selon le mécanisme de contrôle d'accès basé sur les rôles (Role-Based Access Control, RBAC).

Interface IFE:

Interface IFE Ethernet d'un disjoncteur pouvant être connecté au disjoncteur MasterPact MTZ. Avec ce module, le disjoncteur est accessible sur un réseau Ethernet. L'accès aux pages Web de l'interface IFE et au serveur FTPS IFE est autorisé selon le mécanisme de contrôle d'accès basé sur les rôles (Role-Based Access Control, RBAC).

Interface 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.

IP - Internet Protocol:

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

IT - Information Technology, signifiant technologie de l'information:

Désigne le réseau informatique et les systèmes d'information de l'entreprise, par opposition au réseau de technologie opérationnelle (OT).

L

LAN - Local Area Network, signifiant réseau local.:

Désigne l'intranet ou le réseau informatique de l'entreprise.

M

Modbus TCP/IP:

Protocole assurant une communication client/serveur entre des équipements et TCP/IP, qui permet des communications via une connexion Ethernet.

N

NFC - Near field communication:

Désigne un protocole de communication sans fil.

O

OT - 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

PKI - 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.

Protocole IEC 61850 :

Norme qui s'applique aux réseaux et systèmes de communication installés dans des sous-stations. Basée sur le protocole Ethernet, il s'agit d'une méthode de communication standardisée développée pour prendre en charge des systèmes intégrés, composés de dispositifs électroniques intelligents (Intelligent Electronic Device, IED) auto-descriptifs multifournisseurs. Ces systèmes sont interconnectés pour fournir des fonctions de protection, de contrôle, de mesure et de surveillance en temps réel.

R

RBAC - Role-based access control.:

Mode d'attribution des différents niveaux d'accès en fonction des éléments auxquels les rôles définis par l'utilisateur donnent accès.

S

SCADA - 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.

Serveur IFE:

Serveur de tableau électrique IFE Ethernet pouvant être connecté à plusieurs disjoncteurs MasterPact MTZ. Avec ce module, les disjoncteurs sont accessibles sur un réseau Ethernet.

Stratégie de sécurité:

Paramètres de sécurité appliqués à l’ensemble du système sécurisé. En général, une stratégie de sécurité renvoie à l’utilisation de normes. Il permet de définir la configuration de sécurité commune à l’ensemble des équipements.

T

TCP/IP - Transmission control protocol/Internet protocol:

Désigne la suite de protocoles utilisés pour les communications sur Internet.

V

VPN - 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.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

DOCA0122FR-06