PacT Series

TransferPacT Active Automatic (LCD)
TransferPacT Automatic (rotatif)

Guide de cybersécurité

Pact series offre des disjoncteurs et interrupteurs de première qualité.

DOCA0215FR-01
06/2022

www.se.com

Mentions légales

Table des matières

Consignes de sécurité

Informations importantes

AVIS

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'équipement 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 indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ 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, de l'installation et du fonctionnement 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 paramètres, contrôles et informations de l'équipement.
- 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

Objectif du document

Ce guide fournit des informations sur les aspects liés à la cybersécurité des équipement afin d'aider les concepteurs et les opérateurs de systèmes à mettre en place un environnement sécurisé d'exploitation du produit. Ce guide n'aborde pas la question plus vaste 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 la rubrique 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 sont pertinentes pour les commutateurs de transfert TransferPacT Automatic et TransferPact Active Automatic.

Informations en ligne

Le contenu de ce document peut être mis à jour à tout moment. Schneider Electric vous recommande vivement de vous procurer la version la plus récente et la plus à jour disponible sur www.se.com/ww/fr/download.

Les caractéristiques techniques décrites dans le présent document sont également accessibles en ligne. Pour accéder aux informations en ligne, rendez-vous sur la page d'accueil de Schneider Electric www.se.com.

Les caractéristiques techniques présentées dans ce guide doivent être identiques à celles fournies en ligne. Si vous constatez une différence entre les informations contenues dans ce guide et les informations en ligne, utilisez ces dernières.

Pour obtenir des informations sur la conformité du produit aux directives environnementales (RoHS, REACH, PEP et EOLI notamment), accédez à la page *www.se.com/green-premium*.

Document(s) à consulter

Titre du document	Référence
TransferPacT Active Automatic - Commutateur de transfert - Guide de l'utilisateur	DOCA0214FR-01
How Can I Reduce Vulnerability to Cyber Attacks	How Can I Reduce Vulnerability to Cyber Attacks

Introduction à la cybersécurité

Présentation

La cybersécurité protège le réseau de communication et les équipements contre toute interruption d'activité (disponibilité), modification des paramètres (intégrité) ou divulgation d'informations sensibles (confidentialité).

La cybersécurité vise les objectifs suivants :

- Offrir des niveaux accrus de protection des informations et des ressources physiques contre le vol, la corruption, l'utilisation frauduleuse ou les accidents, tout en préservant l'accès des utilisateurs autorisés.
- Concevoir des systèmes sécurisés en restreignant l'accès à l'aide de méthodes physiques et numériques, en identifiant les utilisateurs et en mettant en oeuvre des procédures et des bonnes pratiques liées à la sécurité.

Consignes Schneider Electric

En plus des recommandations fournies dans ce guide pour les appareils, vous devez suivre l'approche de défense en profondeur de Schneider Electric concernant la cybersécurité.

Cette approche est décrite dans la note technique du système 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 offert par le site Web global de Schneider Electric.

Fonctions de l'appareil

Présentation

Le commutateur de transfert automatique (ATSE - Automatic Transfer Switching Equipment) TransferPacT est conçu avec des fonctionnalités de sécurisation qui sont livrées dans un état prédéfini et peuvent être modifiées en fonction des besoins de l'installation. L'appareil doit être configuré et réglé par un personnel qualifié uniquement, car la désactivation ou la modification des paramètres a une incidence sur sa robustesse et celle du réseau de communication en matière de sécurité.

Utilisez ce guide conjointement avec le guide d'utilisation DOCA0214FR-01 pour une configuration détaillée des fonctionnalités et des réglages de l'appareil.

Caractéristiques des communications

La communication avec TransferPacT ATSE s'effectue via les types d'interface suivants :

- Communication câblée via :
  - Modbus-RTU
  - CANopen
- Interaction homme machine (IHM) via :
  - Ecran LCD avec boutons pour l'affichage et l'exploitation.
  - Commutateurs rotatifs et microcommutateurs à LED pour l'exploitation.

Protocoles pris en charge

- Modbus-RTU pour la communication avec les équipements/systèmes de technologie opérationnelle (OT).
- CANopen pour la communication interne entre le contrôleur principal et les accessoires (par exemple module DI/DO, module de communication Modbus).

  NOTE: Modbus-RTU et CANopen sont des protocoles anciens dont les insuffisances intrinsèques en matière de sécurité doivent être compensées par une sécurité physique accrue dans l'application.

Fonctions de sécurité

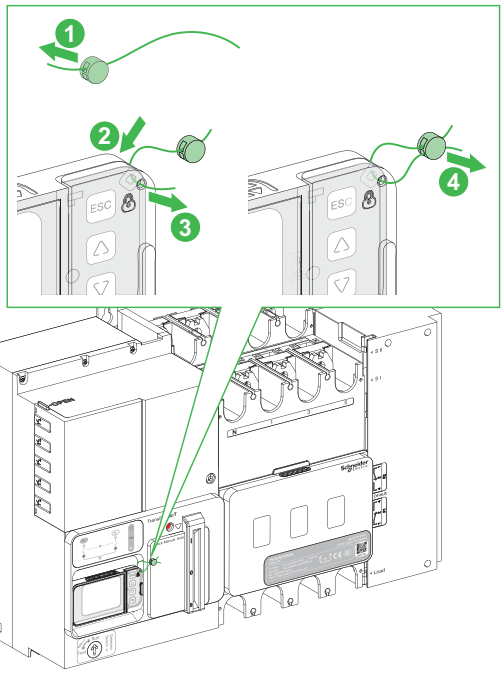
Les fonctions de sécurité suivantes sont prises en charge :

- Le micrologiciel peut être mis à jour en toute sécurité à l'aide des packages signés numériquement par l'infrastructure à clé publique (PKI) de Schneider Electric.
- Vérifie l'intégrité des données stockées dans l'appareil afin d'empêcher toute falsification des configurations, des données d'entreprise et autres.
- Validation rigoureuse des entrées pour empêcher les attaques à distance de Modbus-RTU et/ou CANopen.
- Toute modification de configuration est protégée par un mot de passe.
- Le mot de passe est stocké sous forme de hachage salé et peut être réinitialisé. Pour la réinitialisation du mot de passe, reportez-vous au guide d'utilisation DOCA0214FR-01.
- La fonction de contrôle des communications est désactivée par défaut et ne peut être utilisée qu'après avoir été activée localement. Désactivez-la dès qu'elle n'est pas nécessaire.

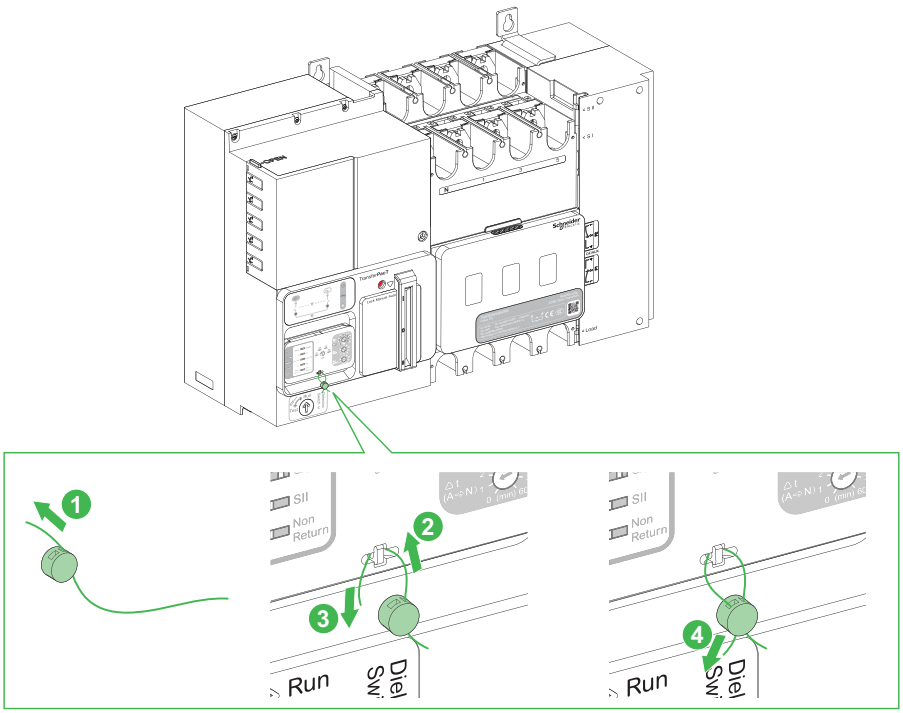
  NOTE: La fonction de contrôle des communications est prise en charge sur TransferPact Active Automatic uniquement. Pour plus d'informations, consultez le guide d'utilisation DOCA0214FR-01.
- L'appareil sera verrouillé pendant 10 minutes après 3 tentatives infructueuses de saisie du mot de passe en vue d'empêcher les attaques de force brute.
- Génère des journaux d'audit pour enregistrer les opérations importantes et les logiques métier aux fins d'analyse et de prévision, de suivi post-événements, d'investigation et de collecte de preuves.

- Couvercle en plastique avec orifice pour permettre aux utilisateurs d'appliquer un plombage afin d'empêcher tout accès physique non autorisé aux boutons (pour TransferPact Active Automatic) ou aux commutateurs rotatifs (pour TransferPact Automatic).

TransferPacT Active Automatic



TransferPacT Automatic



Sécurité de l'appareil

Mise à jour du micrologiciel

Le micrologiciel conçu pour l'appareil est signé par l'infrastructure à clé publique (PKI) de Schneider Electric afin d'en garantir l'intégrité et l'authenticité.

- Inscrivez-vous sur le portail d'assistance à la cybersécurité de Schneider Electric.
- Contactez le support technique de Schneider Electric ou un agent local pour vous aider à mettre à jour le firmware de l'appareil.

Mot de passe

Le mot de passe par défaut est **0000**. Il doit être modifié lors de la première utilisation.

NOTE: Evitez d'utiliser d'anciens mots de passe. En cas de mot de passe oublié ou pour modifier le mot de passe, contactez le service d'assistance sur site ou consultez le guide d'utilisation DOCA0214FR-01.

Date et heure

Des certificats et des signatures numériques sont présents dans l'appareil, ainsi que des journaux d'audit. Pour éviter les erreurs, il est important de synchroniser la date et l'heure. Pour plus d'informations sur la date et l'heure, consultez le guide d'utilisation DOCA0214FR-01.

Journaux d'audit

Générez les journaux d'audit qui enregistrent les événements tels que les tentatives de connexion non valides et la mise à jour du micrologiciel.

Les journaux d'audit ne contiennent aucune information personnelle ou sensible.

Pour détecter des comportements inattendus (tels que des redémarrages fréquents, une mise à jour incorrecte du micrologiciel ou des tentatives de connexion non valides), il est recommandé de surveiller régulièrement les journaux d'audit.

Mise au rebut de l'appareil

L'appareil contient des informations confidentielles configurées pendant la mise en service, ainsi que des valeurs de données récentes et des journaux. Ces informations peuvent notamment inclure un mot de passe, la topologie Modbus, les consommations d'énergie mesurées.

Il est nécessaire d'effectuer une réinitialisation de la configuration et de rétablir le mot de passe par défaut avant de jeter l'appareil. Vous devez avoir accès physiquement à l'appareil tant qu'il est sous tension. Pour connaître la procédure détaillée de rétablissement des réglages d'usine, reportez-vous au guide d'utilisation DOCA0214FR-01.

NOTE: Il est essentiel de planifier la mise hors service pendant le fonctionnement et avant la mise au rebut de l'appareil.

NOTE: Veillez à exporter les derniers journaux d'événements avant la mise hors service de l'appareil.

Sécurité physique de l'appareil

Voici les points de sécurité physique essentiels à prendre en compte lors de l'installation de l'appareil :

- Il est conseillé de déployer et d'utiliser le commutateur conformément à une approche de défense en profondeur recommandée par Schneider Electric pour réduire les risques d'attaque.
- Installez l'ATSE dans une armoire protégée de manière appropriée, par exemple à l'aide d'un cadenas ou d'une clé, afin d'éviter tout risque pendant l'installation et d'empêcher tout accès physique non autorisé.
- Les accessoires d'E/S (le cas échéant) doivent être déployés de manière sécurisée pour empêcher tout accès non autorisé et limiter ainsi le risque d'altération des réglages du commutateur pour l'application prédéfinie utilisée.
- Pour les accessoires Modbus-RTU (le cas échéant) qui sont reconnus comme présentant un risque pour la sécurité dans l'industrie, des mesures physiques de sécurité (telles que des tuyaux dédiés) sont recommandées pour protéger les câbles de communication contre les accès non autorisés, les baisses de communication, les fuites de données ou leur manipulation frauduleuse, etc.
- Pour l'IHM (le cas échéant), un plombage doit être utilisé pour empêcher tout accès non autorisé aux boutons ou aux commutateurs rotatifs.
- Pour l'IHM indépendante (le cas échéant), il est vivement recommandé de la déployer dans la même armoire que l'ATSE pour garantir la sécurité des communications CANopen ou pour protéger les câbles de communication par des mesures physiques de sécurité (telles que des tuyaux dédiés).

Opérations de maintenance recommandées

Des opérations de maintenance régulières sont recommandées tout au long de la durée de vie de l'équipement :

- Assurez-vous que le micrologiciel le plus récent est installé.
- Examinez les journaux d'audit pour identifier d'éventuels comportements inattendus (tentatives de connexion non valides ou redélarrages fréquents, par exemple).
- Modifiez régulièrement le mot de passe de l'administrateur.
- Vérifiez régulièrement les câbles d'E/S pour vous assurer qu'ils sont correctement raccordés et qu'aucun accès non autorisé n'est possible.
- Vérifiez régulièrement les câbles de communication Modbus-RTU et CANopen pour vous assurer qu'aucun d'accès non autorisé n'est possible.
- Désactivez la fonction de contrôle des communications lorsqu'elle n'est pas nécessaire. Pour plus d'informations, consultez le guide d'utilisation DOCA0214FR-01.

Portail d'assistance à la cybersécurité de Schneider Electric

Présentation

Le portail d'assistance à la cybersécurité de Schneider Electric présente la politique de gestion des vulnérabilités de Schneider Electric.

L'objectif de la politique de gestion des vulnérabilités de Schneider Electric est de remédier aux vulnérabilités des produits et systèmes Schneider Electric en matière de cybersécurité, de protéger les solutions installées, les clients et l'environnement.

Schneider Electric travaille en collaboration avec des chercheurs, des équipes d'intervention en cas de cyberurgence (CERT) et des propriétaires de site afin de garantir la fourniture d'informations exactes en temps voulu en vue de protéger les installations de manière adéquate.

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

Elle coordonne la communication avec les équipes CERT appropriées, des chercheurs indépendants, des 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 informations suivantes :

- Informations sur les vulnérabilités des produits en matière de cybersécurité
- Informations sur les incidents de cybersécurité
- Interface permettant aux utilisateurs de déclarer des incidents ou des vulnérabilités en matière de cybersécurité

Signalement et gestion des vulnérabilités

Les incidents liés à la cybersécurité et les vulnérabilités potentielles peuvent être signalés via le site Web de Schneider Electric, sur la page Report a Vulnerability (Signaler une vulnérabilité).

Schneider Electric
35, rue Joseph Monier
92500 Rueil-Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0215FR-01