

PacT Series

TransferPacT Active Automatic (LCD)
TransferPacT Automatic (Rotary)

Cybersecurity Guide

Pact series offers world-class breakers and switches.

DOCA0215EN-01
06/2022



Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

Table of Contents

Safety Information	5
About the Book	7
An Introduction to Cybersecurity	8
Device Features	9
Device Security	12
Physical Security of the Device	13
Recommended Maintenance Operations	14
Schneider Electric Cybersecurity Support Portal	15

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.





The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

 DANGER
DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

 WARNING
WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

 CAUTION
CAUTION indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

CYBERSECURITY SAFETY NOTICE

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About the Book

Document Scope

This guide provides information on the cybersecurity aspects for devices to help system designers and operators promote a secure operating environment for the product. This guide does not address the more general topic of how to secure your operational technology network, or your company ethernet network. For a general introduction to cybersecurity threats and how to address them, refer to [How Can I Reduce Vulnerability to Cyber Attacks](#)

NOTE: In this guide, the term security is used to refer to cybersecurity.

Validity Note

The information in this guide is relevant for devices relevant for TransferPacT Automatic and TransferPacT Active Automatic Transfer Switches.

Online Information

The information contained in this document is likely to be updated at any time. Schneider Electric strongly recommends that you have the most recent and up-to-date version available on www.se.com/ww/en/download.

The technical characteristics of the devices described in the present document also appear online. To access the information online, go to the Schneider Electric home page www.se.com.

The technical characteristics presented in this guide should be the same as those that appear online. If you see a difference between the information contained in this guide and online information, use the online information.

For product compliance with environmental directives such as RoHS, REACH, PEP, and EOL, go to www.se.com/green-premium.

Related Documentation

Document title	Document number
<i>TransferPacT Active Automatic Transfer Switching Equipment (ATSE) User Guide</i>	DOCA0214EN-01
<i>How Can I reduce Vulnerability to Cyber Attacks</i>	How Can I Reduce Vulnerability to Cyber Attacks

An Introduction to Cybersecurity

Introduction

Cybersecurity protects the communication network and the devices against any disrupt operations (availability), modification of settings (integrity), or disclosure of any sensitive information (confidentiality).

The objective of cybersecurity are:

- To provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.
- To design secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practices.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to devices, you should follow the Schneider Electric defense-in-depth approach to cybersecurity.

This approach is described in the system technical note [How Can I Reduce Vulnerability to Cyber Attacks](#) .

In addition, you will find many useful resources and up-to-date information on the Cybersecurity Support Portal on the Schneider Electric global website.

Device Features

Overview

The TransferPacT ATSE (Automatic Transfer Switching Equipment) is designed with security-enabling features, and these features are in a preset state and can be modified to meet your installation needs. The device must only be configured and set by qualified personnel, because disabling or changing settings will affect the overall security robustness of the device and communication network.

Use this guide in conjunction with the user guide DOCA0214EN-01 for detailed configuration of features and settings of the device.

Communication Characteristics

The communication with TransferPacT ATSE is through the following interface types:

- Wired communication through:
 - Modbus-RTU
 - CANopen
- Human Machine Interaction (HMI) through:
 - LCD screen with buttons for display and operating.
 - Rotary and dip switches with LED for operating.

Supported Protocols

- Modbus-RTU for communication with the Operational Technology (OT) devices/systems.
- CANopen for internal communication between the main controller and accessories (e.g. DI/DO module, Modbus communication module)

NOTE: The Modbus-RTU and CANopen are legacy protocols, which have inherent deficiencies in security and need to be compensated with additional physical security in your application.

Security Features

The following security features are supported:

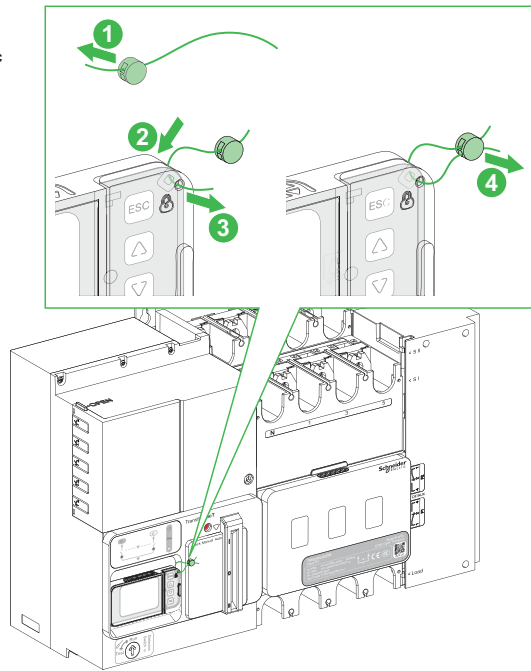
- Firmware can be securely updated through the firmware which is digitally signed by Schneider Public Key Infrastructure (PKI).
- Verifies the integrity of the data stored in the device to prevent configurations, business data and any other data from being tampered.
- Robust input validation to prevent against remote attacks from Modbus-RTU and/or CANopen.
- Any configuration modification is password-protected.
- The password is stored as a salted hash and can be reset. For password reset, refer to user guide DOCA0214EN-01.
- The communication control feature is disabled by default and can only be used after it's enabled locally. Disable it in time when it's not needed.

NOTE: The communication control feature is supported on TransferPact Active Automatic only. For more information, refer to user guide DOCA0214EN-01.

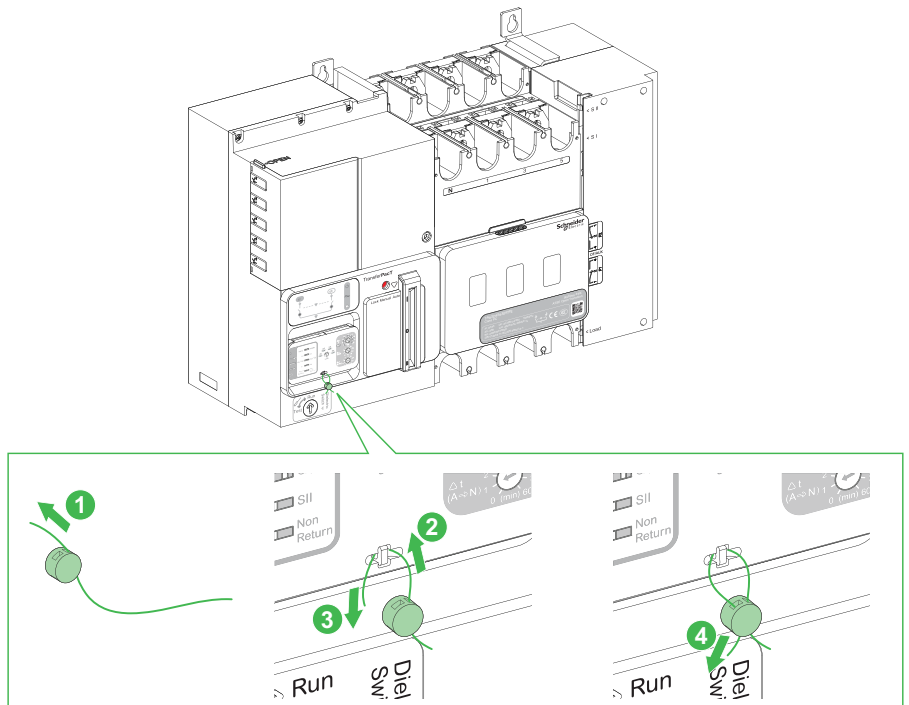
- The device will be locked for 10 minutes after 3 failed password attempts, which used to prevent brute force attacks.
- Generates audit logs to record important operations and business logics for analysis and prediction, post-event tracking, investigation and evidence collection.

- Plastic cover with hole to support users to put on lead sealing to prevent unauthorized physical access to the buttons (for TransferPacT Active Automatic) or rotary switches (for TransferPacT Automatic).

TransferPacT Active Automatic



TransferPacT Automatic



Device Security

Firmware Update

Firmware designed for the device is signed by the Schneider Electric Public Key Infrastructure (PKI) to ensure the integrity and authenticity of the firmware running on the device.

- Register on the Schneider Electric [cybersecurity support portal](#) .
- Contact Schneider Electric technical support or local agent to help you update the device firmware.

Password

The default password is **0000**, it needs to be modified when used for the first time.

NOTE: Avoid using old passwords. For forget password, contact with field service or refer to user guide [DOCA0214EN-01](#).

Date and Time

Certificates and digital signatures are present in the device, as well as audit logs. To avoid errors, it is important to keep the date and time synchronized. For more information about date and time, refer to the user guide [DOCA0214EN-01](#).

Audit Logs

Generate the audit logs that record the events, such as invalid login attempts and firmware update.

The audit logs does not contain any personal and sensitive information.

To detect unexpected behaviors (for example, frequent rebooting, incorrect firmware update, or invalid login attempts), it is recommended to monitor audit logs regularly.

Device Disposal

The device contains confidential information configured during commissioning, recent data values and logs. For example, this information can include password, Modbus device topology, measured power consumptions.

It is required to perform configuration reset and restore the default password before disposing of the device. You must have physical access to the device while it is powered on. For the detailed procedure on how to reset to factory settings, refer to the user guide [DOCA0214EN-01](#).

NOTE: It is critical to plan decommissioning during operation and before the disposal of the device.

NOTE: Make sure the latest event logs are exported before the device is decommissioned.

Physical Security of the Device

The following are the important physical security points to keep in mind for installing the device:

- Recommend to deploy and use the switching equipment in accordance with a **defense-in-depth approach** recommended by Schneider Electronic to reduce the risk of switching equipment being attacked.
- Install the ATSE in a cabinet secured in an appropriate manner, for example with a padlock or a key, to avoid risks during installation or the risk of unauthorized physical access.
- I/O accessories (if any) shall be securely deployed to prevent unauthorized access to mitigate the risk of changing the switch settings for the predefined application in use.
- For Modbus-RTU accessories (if any) which is recognized as a security risk in the industry, physical security measures (such as dedicated pipes) are recommended to protect communication cables from unauthorized access, communication drops, data leakage and tampering, etc.
- For the HMI (if any), a lead seal shall be used to prevent unauthorized access to buttons or rotary switches.
- For the independent HMI (if any), it is highly recommended to deploy it with the ATSE in the same cabinet to ensure CANopen communication security, or to protect the communication cables with physical security measures (such as dedicated pipes).

Recommended Maintenance Operations

Recommended maintenance is required regularly over the lifetime of the device:

- Make sure that the latest firmware is updated.
- Check the audit logs for unexpected behaviors, such as invalid login attempts or frequent rebooting.
- Regularly change the administrator password.
- Regularly check the I/O cables to ensure they are properly connected and there is no unauthorized access.
- Regularly check the Modbus-RTU and CANopen communication cables to ensure there is no unauthorized access.
- Disable the communication control feature in time when it's not needed. For more information, refer to user guide [DOCA0214EN-01](#).

Schneider Electric Cybersecurity Support Portal

Overview

The Schneider Electric Cybersecurity Support Portal outlines the Schneider Electric vulnerability management policy.

The aim of the Schneider Electric vulnerability management policy is to address vulnerabilities in cybersecurity affecting Schneider Electric products and systems, to protect installed solutions, customers, and the environment.

Schneider Electric works with a collaborative approach with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect their installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and issuing alerts on vulnerabilities and mitigations affecting products and solutions.

The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

Information Available on the Schneider Electric Cybersecurity Support Portal

The support portal provides the following:

- Information about cybersecurity vulnerabilities of products.
- Information about cybersecurity incidents.
- An interface that enables users to declare cybersecurity incidents or vulnerabilities.

Vulnerability Reporting and Management

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website [Report a Vulnerability](#).

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.

© 2022 – Schneider Electric. All rights reserved.

DOCA0215EN-01