PacT Series

TransferPacT Active Automatic 转换开关设备 (LCD)
TransferPacT Automatic 转换开关设备（旋转式）

网络安全指南

Pact series 提供出众的断路器和开关。

DOCA0215ZH-01
06/2022

www.se.com

法律声明

施耐德电气品牌以及本指南中涉及的施耐德电气及其附属公司的任何商标均是施耐德电气或其附属公司的财产。所有其他品牌均为其各自所有者的商标。本指南及其内容受适用版权法保护，并且仅供参考使用。未经施耐德电气事先书面许可，不得出于任何目的，以任何形式或方式（电子、机械、影印、录制或其他方式）复制或传播本指南的任何部分。

对于将本指南或其内容用作商业用途的行为，施耐德电气未授予任何权利或许可，但以“原样”为基础进行咨询的非独占个人许可除外。

施耐德电气的产品和设备应由合格人员进行安装、操作、保养和维护。

由于标准、规格和设计会不时更改，因此本指南中包含的信息可能会随时更改，恕不另行通知。

在适用法律允许的范围内，对于本资料信息内容中的任何错误或遗漏，或因使用此处包含的信息而导致或产生的后果，施耐德电气及其附属公司不会承担任何责任或义务。

作为负责任、具有包容性的企业中的一员，我们将更新包含非包容性术语的内容。然而，在我们完成更新流程之前，我们的内容可能仍然包含客户认为不恰当的标准化行业术语。

目录

安全信息

重要信息

声明

在尝试安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特别信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。

在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。

这是提醒注意安全的符号。提醒用户可能存在人身伤害的危险。请遵守所有带此符号的安全注意事项，以避免可能的人身伤害甚至死亡。

DANGER

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

警告

警告表示若不加以避免,可能**会导致**严重人身伤害甚至死亡的危险情况。

小心

小心表示若不加以避免,可能**会导致**轻微或中度人身伤害的危险情况。

注意

注意用于表示与人身伤害无关的危害。

请注意

电气设备的安装、操作、维修和维护工作仅限于有资质的人员执行。Schneider Electric 不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造、安装和操作相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

网络安全注意事项

⚠警告

系统可用性、完整性和保密性的潜在危害

- 首次使用时，更改默认密码，以有助于防止擅自访问设备设置、控件和信息。
- 禁用未使用的端口/服务和默认账户将有助于尽量减少恶意攻击的途径。
- 将联网设备布置在多层网络防御（例如防火墙、网络分段、网络入侵检测和保护）之后。
- 采用网络安全最佳实践（例如，最低权限、责任分离）来帮助阻止非法曝露、丢失、数据和日志修改、或服务中断。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

关于本书

文档范围

本指南中的信息涉及设备的网络安全，旨在帮助系统设计人员和操作人员为产品打造一个安全的运行环境。本指南并不涉及较常见的主题，比如，如何保护您的运营技术网络或企业以太网网络。有关网络安全威胁的简介以及如何应对这些威胁，请参阅 How Can I reduce Vulnerability to Cyber Attacks。

注: 在本指南中，安全一词是指网络安全。

有效性说明

本指南中的信息与 Transfer**PacT** Automatic 和 Transfer**PacT** Active Automatic 转换开关设备相关。

在线信息

本文档中的信息可能在任何时候更新。Schneider Electric 强烈建议您通过 www.se.com/ww/en/download 获得最新版本。

本手册中描述的设备技术特性在网站上也有提供。如要在线访问此信息，请访问 Schneider Electric 主页 www.se.com。

本指南中提供的技术特性应该与在线内容相同。如果发现本指南中包含的信息与在线信息之间存在差异，请以在线信息为准。

有关产品在环境指令（比如 RoHS、REACH、PEP 和 EOLI）方面的合规性，请访问 *www.se.com/green-premium*。

相关的文件

文件名称	文件编号
TransferPacT Active Automatic 转换开关设备 *(ATSE)* 用户指南	DOCA0214ZH-01
如何减少网络攻击漏洞	如何减少网络攻击漏洞

网络安全简介

简介

网络安全可保护通讯网络和设备免受任何中断操作（可用性）、设置修改（完整性）或任何敏感信息泄露（保密性）的影响。

网络安全的目标是：

- 提升信息和物理资产的保护级别，以免遭受盗窃、破坏、滥用或发生事故，同时保证其预期用户的访问和使用。
- 设计安全系统，利用物理和数字方法限制访问，识别用户，以及实施安全程序和最佳实践。

Schneider Electric 指南

除了本指南中针对设备所给的具体建议之外，您还应遵循网络安全的 Schneider Electric 深度防御方法。

系统技术说明 How Can I reduce Vulnerability to Cyber Attacks 中介绍了这种方法.

此外，Schneider Electric 全球网站的 Cybersecurity Support Portal 中也提供了许多有用的资源和最新信息。

设备特性

概述

Tranfer**PacT** ATSE（自动转换开关设备）设计有安全功能，这些功能处于预设状态，可以根据您的安装需求进行修改。设备只能由具备资质的人员配置和设置，因为禁用或更改设置将影响设备和通讯网络的总体安全稳健性。

有关设备功能和设置的详细配置，请结合参阅本指南及用户指南 DOCA0214ZH-01。

通讯特性

与 TransferPacT ATSE 的通讯通过以下接口类型进行：

- 通过以下方式进行的有线通讯：
  - Modbus-RTU
  - CANopen
- 通过以下方式进行的人机交互 (HMI)：
  - LCD 屏幕，带有用于显示和操作的按钮。
  - 旋转和 DIP 开关，带工作指示 LED。

支持的协议

- Modbus-RTU，用于与运营技术 (OT) 设备/系统通讯。
- CANopen，用于主控制器与附件（如 DI/DO 模块、Modbus 通讯模块）之间的内部通讯

  注: Modbus-RTU 和 CANopen 是旧式协议，它们在安全方面存在固有的缺陷，需要通过应用中的额外物理安全来补偿。

安全特性

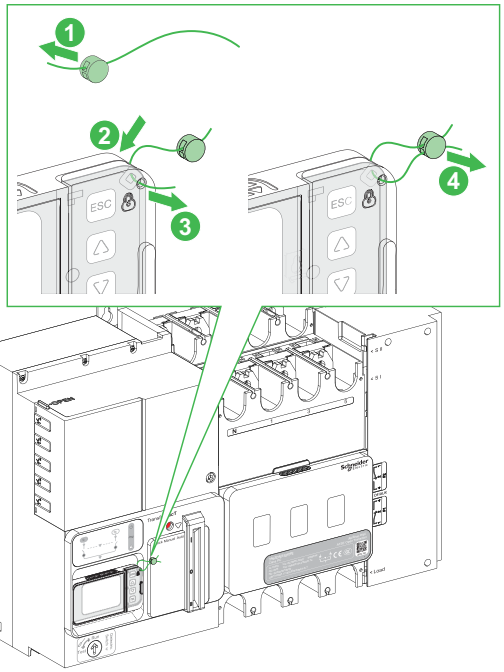
支持以下安全功能：

- 可通过拥有 Schneider 公钥基础设施 (PKI) 数字签名的固件安全地执行固件更新。
- 验证设备中存储的数据的完整性，以防止配置、业务数据和任何其他数据被篡改。
- 可靠的输入验证功能，可防止来自 Modbus-RTU 和/或 CANopen 的远程攻击。
- 任何配置修改都受密码保护。
- 密码存储为加盐哈希，且可以复位。有关密码复位，请参阅用户指南 DOCA0214ZH-01。
- 通讯控制功能缺省为禁用状态，只能在本地启用后才使用。在不需要时及时将其禁用。

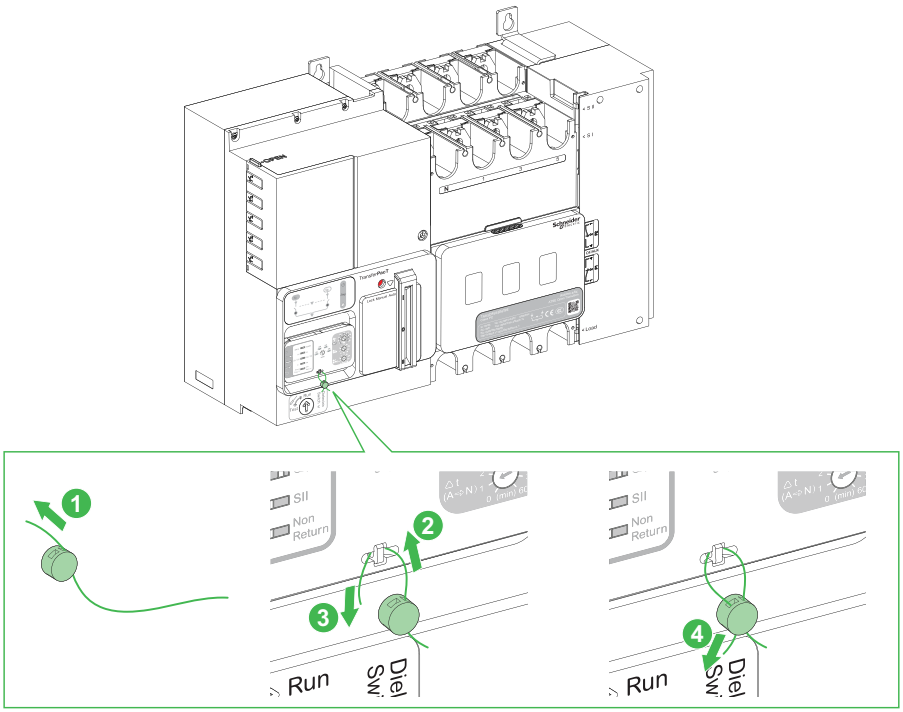
  注: 仅 TransferPact Active Automatic 支持通讯控制功能。有关更多信息，请参阅用户指南 DOCA0214ZH-01。
- 密码尝试失败 3 次后，设备将锁定 10 分钟，用于防止暴力攻击。
- 生成审计日志，记录重要的操作和业务逻辑，以用于分析和预测、事后跟踪、调查和证据收集。

- 带孔的塑料盖，用于支持用户安装铅封，以防止未经授权使用按钮（适用于 TransferPact Active Automatic）或旋转开关（适用于 TransferPact Automatic）。

TransferPacT Active Automatic



TransferPacT Automatic



设备安全

固件更新

为设备设计的固件拥有 Schneider Electric 公钥基础设施 (PKI) 签名，以确保设备上运行的固件的完整性和真实性。

- 在 Schneider Electric Cybersecurity Support Portal 上注册。
- 请联系 Schneider Electric 技术支持或本地代理，帮助您更新设备固件。

密码

缺省密码为 **0000**，首次使用时需修改此密码。

注: 避免使用旧密码。如果忘记密码或要更改密码，请联系现场服务或参阅用户指南 DOCA0214ZH-01。

日期和时间

设备中提供了证书和数字签名，以及审计日志。为了避免错误，必须保持日期和时间同步。有关日期和时间的更多信息，请参阅用户指南 DOCA0214ZH-01。

审计日志

生成审计日志，其中记录了诸如无效登录、固件更新等事件。

审计日志不包含任何个人和敏感信息。

如要检测非预期行为（比如，频繁重启、不正确的固件更新、或无效登录），建议定期监视审计日志。

设备报废

设备包含在调试期间配置的保密信息、当前数据值和日志。例如，这些信息可能包括密码、Modbus 设备拓扑、功耗测量值。

在报废设备之前，需要执行配置复位并恢复缺省密码。设备通电时，您必须具有实际使用设备的权限。有关如何复位为出厂设置的详细步骤，请参阅用户指南 DOCA0214ZH-01。

注: 针对运行期间和设备报废之前的设备退役制定相关计划，是至关重要的。

注: 在停用设备之前，确保导出最新的事件日志。

设备的物理安全

以下是安装设备时应牢记的重要物理安全要点：

- 建议按照 Schneider Electronic 建议的深度防御方法来部署和使用开关设备，以降低开关设备遭受攻击的风险。
- 将 ATSE 安装在以适当方式（例如使用挂锁或钥匙）保护的机柜中，以避免安装过程中的风险或非法使用设备的风险。
- 应安全地部署 I/O 附件（如有），以防止未经授权的使用，从而降低正在使用的预定义应用的开关设置遭受更改的风险。
- 对于被业内视为安全风险的 Modbus-RTU 附件（如有），建议采用物理安全措施（如专用管道）来保护通讯电缆免遭未经授权的使用、通讯中断、数据泄漏和篡改等。
- 对于 HMI（如有），应使用铅封，以防止对按钮或旋转开关的未授权使用。
- 对于独立的 HMI（如有），强烈建议将其与 ATSE 一起部署在同一机柜中，以确保 CANopen 通讯安全，或采用物理安全措施（如专用管道）来保护通讯电缆。

建议的维护操作

建议在设备的整个寿命期内定期进行维护：

- 确保更新到最新固件。
- 检查审计日志，查看是否存在异常行为，如无效登录或频繁重启。
- 定期更改管理员密码。
- 定期检查 I/O 电缆以确保它们正确连接且未遭到非法使用。
- 定期检查 Modbus-RTU 和 CANopen 通讯电缆，以确保未遭到非法使用。
- 在不需要时，请及时禁用通讯控制功能。有关更多信息，请参阅用户指南 DOCA0214ZH-01。

Schneider Electric Cybersecurity Support Portal

概述

Schneider Electric Cybersecurity Support Portal 概括了 Schneider Electric 隐患管理策略。

Schneider Electric 隐患管理策略旨在处理影响 Schneider Electric 产品和系统的网络安全隐患，从而为现有的解决方案、客户和环境提供有效保护。

Schneider Electric 与研发人员、网络应急响应小组 (CERT) 和资产所有人密切合作，确保及时提供准确信息，适时保护系统安全。

Schneider Electric 的企业产品 CERT (CPCERT) 负责管理并发出与影响产品和解决方案的隐患和漏洞有关的警示。

CPCERT 协调相关 CERT、独立研发人员、产品经理和所有受影响客户之间的沟通。

Schneider Electric Cybersecurity Support Portal 上的信息

该支持门户提供以下信息：

- 有关产品网络安全隐患的信息。
- 有关网络安全事件的信息。
- 让用户能够声明网络安全事件或隐患的界面

漏洞报告与管理

可以通过 Schneider Electric 网站（报告漏洞）来报告网络安全事件和潜在漏洞。

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

由于各种标准、规范和设计不时变更，请索取对本出版物中给出的信息的确认。

DOCA0215ZH-01