PacT-Reihe

Transfer**PacT** Active Automatic (LCD)
Transfer**PacT** Automatic (Drehend)

Anleitung zur Cybersicherheit

Pact series bietet erstklassige Leistungsschalter und Schalter.

DOCA0215DE-01
06/2022

www.se.com

Rechtliche Hinweise

Die Marke Schneider Electric sowie alle anderen in diesem Handbuch enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein. Dieses Handbuch und seine Inhalte sind durch geltende Urheberrechtsgesetze geschützt und werden ausschließlich zu Informationszwecken bereitgestellt. Ohne die vorherige schriftliche Genehmigung von Schneider Electric darf kein Teil dieses Handbuchs in irgendeiner Form oder auf irgendeine Weise (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder anderweitig) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Handbuchs oder seiner Inhalte, ausgenommen der nicht exklusiven und persönlichen Lizenz, die Website und ihre Inhalte in ihrer aktuellen Form zurate zu ziehen.

Produkte und Geräte von Schneider Electric dürfen nur von Fachpersonal installiert, betrieben, instand gesetzt und gewartet werden.

Da sich Standards, Spezifikationen und Konstruktionen von Zeit zu Zeit ändern, können die in diesem Handbuch enthaltenen Informationen ohne vorherige Ankündigung geändert werden.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der Verwendung der hierin enthaltenen Informationen entstehen.

Als verantwortungsbewusstes und offenes Unternehmen aktualisieren wir unsere Inhalte, die nicht-inklusive Terminologie enthalten. Bis dieser Vorgang abgeschlossen ist, können unsere Inhalte allerdings nach wie vor standardisierte Branchenbegriffe enthalten, die von unseren Kunden als unangemessen betrachtet werden.

Inhaltsverzeichnis

Sicherheitshinweise

Wichtige Informationen

HINWEISE

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠⚠ DANGER

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

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

BITTE BEACHTEN

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Montage, der Konstruktion und des Betriebs elektrischer Geräte verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

SICHERHEITSHINWEIS ZUR CYBERSICHERHEIT

⚠WARNUNG

MÖGLICHE BEEINTRÄCHTIGUNG DER VERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT DES SYSTEMS

- Ändern Sie das Standardpasswort bei der ersten Verwendung, um jeden unberechtigten Zugriff auf die Geräteeinstellungen, Steuerelemente und Informationen zu unterbinden.
- Deaktivieren Sie nicht verwendete Ports/Dienste und Standardkonten, um potenzielle Zugänge für bösartige Angreifer zu blockieren.
- Richten Sie mehrere Cyber-Schutzschichten vor allen Netzwerkgeräten ein (z. B. Firewalls, Netzwerksegmentierung, Netzwerkangriffserkennung (Intrusion Detection) und -schutz).
- Wenden Sie die Best Practices zur Cybersicherheit an (z. B. „Least Privilege“ (Prinzip der geringsten Rechte), „Segregation of Duties“ (Funktionstrennung)), um die unberechtigte Offenlegung von Daten, Datenverlust oder die Änderung von Daten und Protokollen bzw. die Unterbrechung der Dienstebereitstellung zu verhindern.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Über das Handbuch

Deckungsbereich des Dokuments

Dieses Handbuch enthält Informationen zu Aspekten der Cybersicherheit für Geräte, um System-Designer und -Betreiber bei der Förderung einer sicheren Betriebsumgebung für das Produkt zu unterstützen. Dieses Handbuch geht nicht auf das allgemeinere Thema zur Sicherung Ihres betrieblichen Technologienetzwerks oder Ihres Ethernet-Netzwerks in Ihrem Unternehmen ein. Eine allgemeine Einführung in Cybersicherheitsbedrohungen und dem Umgang mit ihnen finden Sie unter How Can I Reduce Vulnerability to Cyber Attacks

HINWEIS: In diesem Handbuch bezieht sich der Begriff „Sicherheit“ auf die Cybersicherheit.

Gültigkeitshinweis

Die Informationen in diesem Handbuch beziehen sich auf Geräte, die für Transfer**PacT** Automatic und Transfer**PacT** Active Automatic Transfer-Schalter relevant sind.

Online-Informationen

Die in diesem Dokument enthaltenen Informationen können jederzeit aktualisiert werden. Schneider Electric empfiehlt nachdrücklich, dass Sie die jeweils neueste und zuletzt veröffentlichte Version auf der Website www.se.com/ww/en/download verwenden.

Die im vorliegenden Dokument beschriebenen technischen Merkmale sind ebenfalls online verfügbar. Um auf die Online-Informationen zuzugreifen, gehen Sie zur Homepage von Schneider Electric www.se.com.

Die in diesem Handbuch vorgestellten technischen Merkmale sollten denen entsprechen, die online angezeigt werden. Wenn Sie einen Unterschied zwischen den Informationen in diesem Handbuch und den Online-Informationen feststellen, verwenden Sie die Online-Informationen.

Informationen zur Konformität mit Umweltrichtlinien wie RoHS, REACH, PEP und EOLI finden Sie unter *www.se.com/green-premium*.

Verwandte Dokumentation

Dokumenttitel	**Dokumentnummer**
TransferPacT Active Automatic - Netzumschalter (ATSE) - Benutzerhandbuch	DOCA0214DE-01
How Can I reduce Vulnerability to Cyber Attacks	How Can I reduce Vulnerability to Cyber Attacks

Eine Einführung in die Cybersicherheit

Einführung

Cybersicherheit schützt das Kommunikationsnetz und die Geräte vor Funktionsstörungen (Verfügbarkeit), Änderungen der Einstellungen (Integrität) oder der Offenlegung vertraulicher Informationen (Vertraulichkeit).

Die Ziele der Cybersicherheit sind:

- Bereitstellung eines höheren Schutzgrads für Daten und physische Ressourcen, um diese vor Diebstahl, Beschädigung, Missbrauch oder Unfällen zu schützen, und dabei gleichzeitig den Zugriff für die vorgesehenen Benutzer aufrechtzuerhalten.
- Der Entwurf sicherer Systeme, die den Zugriff mithilfe physischer und digitaler Methoden einschränken, Benutzer identifizieren sowie die Sicherheitsverfahren und Best Practices umsetzen.

Richtlinien von Schneider Electric

Zusätzlich zu den Empfehlungen in diesem Handbuch, die sich speziell auf Geräte beziehen, sollten Sie das „Defense-in-Depth-Konzept“ von Schneider Electric im Bereich Cybersicherheit befolgen.

Dieses Konzept wird in der technischen Mitteilung des Systems How Can I Reduce Vulnerability to Cyber Attacks beschrieben.

Darüber hinaus können Sie viele nützliche Ressourcen und aktuelle Informationen im Support-Portal für Cybersicherheit auf der globalen Website von Schneider Electric finden.

Gerätefunktionen

Überblick

Der Transfer**PacT**-ATSE (Automatic Transfer Switching Equipment - Automatischer Netzumschalter) wurde mit Sicherheitsfunktionen entwickelt. Diese Funktionen sind voreingestellt und können an Ihre spezifischen Installationsanforderungen angepasst werden. Das Gerät darf nur von qualifiziertem Personal konfiguriert und eingestellt werden, da sich die Deaktivierung oder Änderung von Einstellungen auf die Gesamtsicherheit des Geräts und des Kommunikationsnetzwerks auswirkt.

In diesem Handbuch sowie im Benutzerhandbuch DOCA0214DE-01 finden Sie detaillierte Informationen zur Konfiguration der Funktionen und Einstellungen des Geräts.

Merkmale der Kommunikation

Die Kommunikation mit dem TransferPacT-ATSE erfolgt über folgende Schnittstellentypen:

- Kabelgebundene Kommunikation über:
  - Modbus-RTU
  - CANopen
- Mensch-Maschine-Interaktion (HMI) über:
  - LCD-Bildschirm mit Tasten für Anzeige und Betrieb.
  - Drehschalter und DIP-Schalter mit LED für den Betrieb.

Unterstützte Protokolle

- Modbus-RTU für die Kommunikation mit OT-Geräten/Systemen (Operational Technology).
- CANopen für die interne Kommunikation zwischen der Hauptsteuerung und dem Zubehör (z. B. DI/DO-Modul, Modbus-Kommunikationsmodul).

  HINWEIS: Modbus-RTU und CANopen sind Vorgängerprotokolle, die inhärente Sicherheitsmängel aufweisen, die durch zusätzliche physische Sicherheit in Ihrer Anwendung kompensiert werden müssen.

Sicherheitsfunktionen

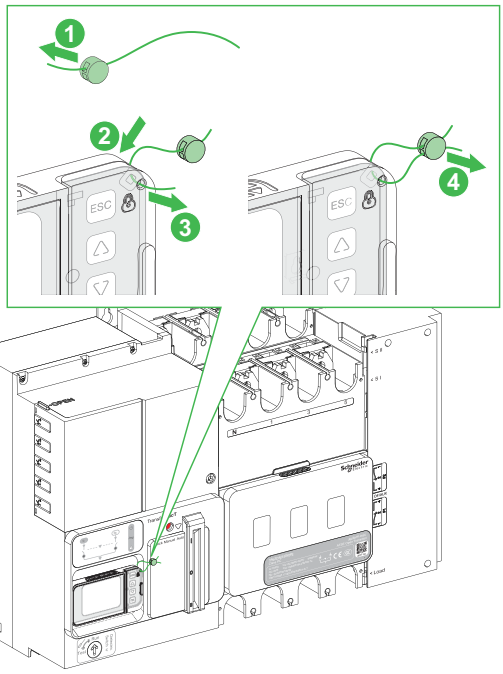
Die folgenden Sicherheitsfunktionen werden unterstützt:

- Firmwareaktualisierung über die Firmware, die von der Schneider Public Key-Infrastruktur (PKI) digital signiert wird.
- Prüfung der Integrität der im Gerät gespeicherten Daten, um zu verhindern, dass Konfigurationen, Geschäftsdaten und andere Daten manipuliert werden.
- Robuste Eingangsvalidierung zur Verhinderung von Fernangriffen über Modbus-RTU und/oder CANopen.
- Jede Konfigurationsänderung ist passwortgeschützt.
- Das Passwort wird als Salted-Hash gespeichert und kann zurückgesetzt werden. Informationen zum Zurücksetzen des Passworts finden Sie im Benutzerhandbuch DOCA0214DE-01.
- Die Kommunikationssteuerungsfunktion ist standardmäßig deaktiviert und kann nur verwendet werden, nachdem sie lokal aktiviert wurde. Deaktivieren Sie sie rechtzeitig, wenn sie nicht benötigt wird.

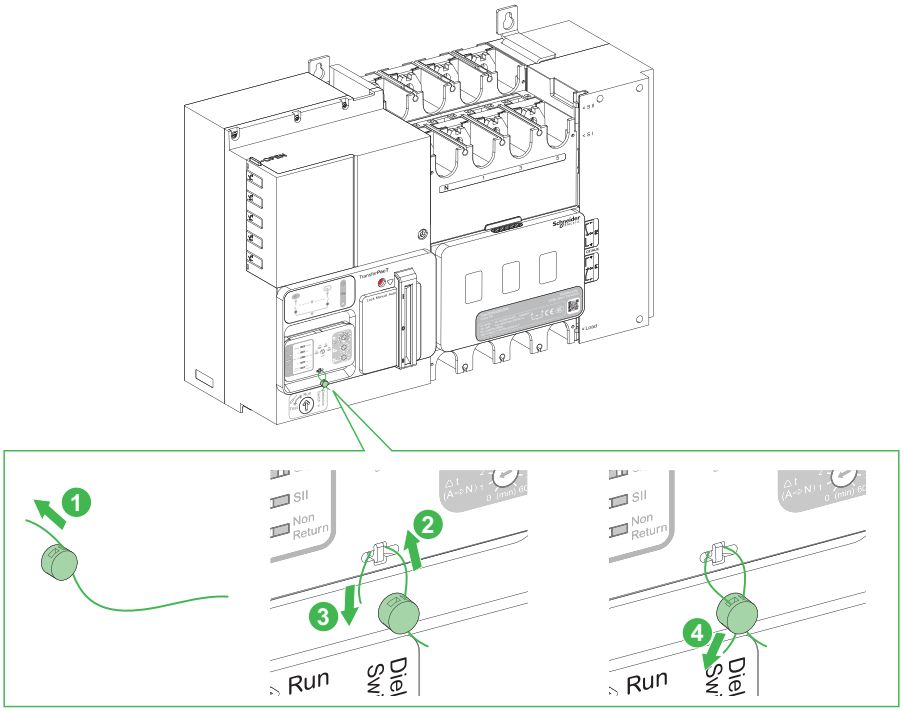
  HINWEIS: Die Kommunikationssteuerungsfunktion wird nur von TransferPact Active Automatic unterstützt. Weitere Informationen finden Sie im Benutzerhandbuch DOCA0214DE-01.
- Das Gerät wird nach 3 fehlgeschlagenen Passwortversuchen für 10 Minuten gesperrt, was der Verhinderung von Brute-Force-Angriffen dient.
- Generierung von Überwachungsprotokollen, um wichtige Vorgänge und Geschäftslogik für Analyse und Prognose, Post-Event-Nachverfolgung, Untersuchung und Beweisaufnahme aufzuzeichnen.

- Kunststoffabdeckung mit Bohrung zur Unterstützung des Benutzers beim Anbringen einer Plombe, um unbefugten Zugriff auf die Taster (für TransferPact Active Automatic) oder Drehschalter (für TransferPact Automatic) zu verhindern.

TransferPacT Active Automatic



TransferPacT Automatic



Gerätesicherheit

Firmwareaktualisierung

Die für das Gerät entwickelte Firmware wird von der Public Key-Infrastruktur (PKI) von Schneider Electric signiert, um die Integrität und Authentizität der auf dem Gerät ausgeführten Firmware zu gewährleisten.

- Registrieren Sie sich im Support-Portal für die Cybersicherheit von Schneider Electric.
- Wenden Sie sich an den technischen Support von Schneider Electric oder einen örtlichen Kundendienstmitarbeiter, um Sie bei der Aktualisierung der Gerätefirmware zu unterstützen.

Passwort

Das Standardpasswort lautet **0000**. Es muss bei der ersten Verwendung geändert werden.

HINWEIS: Vermeiden Sie die Wiederverwendung alter Passwörter. Wenden Sie sich an den Kundendienst oder ziehen Sie das Benutzerhandbuch DOCA0214DE-01 zu Rate, falls Sie das Passwort vergessen haben oder es ändern möchten.

Datum und Uhrzeit

Im Gerät sind Zertifikate und digitale Signaturen sowie Überwachungsprotokolle vorhanden. Um Fehler zu vermeiden, müssen das Datum und die Uhrzeit synchronisiert bleiben. Weitere Informationen zu Datum und Uhrzeit finden Sie im Benutzerhandbuch DOCA0214DE-01.

Überwachungsprotokolle

Generieren Sie die Überwachungsprotokolle, die alle Ereignisse aufzeichnen, z. B. ungültige Anmeldeversuche und fehlgeschlagene Firmwareaktualisierungen.

Die Überwachungsprotokolle enthalten keine persönlichen oder vertraulichen Informationen.

Um unerwartete Verhaltensweisen (z. B. häufige Neustarts, nicht ordnungsgemäße Firmwareaktualisierungen oder ungültige Anmeldeversuche) zu erkennen, wird empfohlen, regelmäßig die Überwachungsprotokolle zu prüfen.

Entsorgung des Geräts

Das Gerät enthält vertrauliche Informationen, die während der Inbetriebnahme konfiguriert wurden, sowie aktuelle Datenwerte und Protokolle. Diese Informationen können Passwort, Modbus-Gerätetopologie, gemessene Stromverbrauchswerte usw. umfassen.

Es ist erforderlich, die Konfiguration zurückzusetzen und das Standardpasswort wiederherzustellen, bevor das Gerät entsorgt wird. Sie müssen physischen Zugriff auf das Gerät haben, während es eingeschaltet ist. Detaillierte Anweisungen zum Zurücksetzen auf die Werkseinstellungen finden Sie im Benutzerhandbuch DOCA0214DE-01.

HINWEIS: Es ist wichtig, die Außerbetriebnahme während des Betriebs und vor der Entsorgung des Geräts zu planen.

HINWEIS: Stellen Sie sicher, dass die neuesten Ereignisprotokolle exportiert werden, bevor das Gerät außer Betrieb genommen wird.

Physische Sicherheit des Geräts

Die folgenden physischen Sicherheitsaspekte müssen bei der Installation des Geräts beachtet werden:

- Wir empfehlen, die Schaltanlage gemäß einem von Schneider Electric empfohlenen Defense-in-Depth-Ansatz einzusetzen und zu verwenden, um das Risiko eines Angriffs auf die Schaltanlage zu reduzieren.
- Installieren Sie den ATSE in einem Schrank, der angemessen gesichert ist, z. B. mit einem Vorhängeschloss oder einem Schlüssel, um Risiken während der Installation oder die Gefahr eines unbefugten physischen Zugriffs zu vermeiden.
- Das E/A-Zubehör (falls vorhanden) muss auf sichere Weise bereitgestellt werden, um unbefugten Zugriff zu verhindern und die Gefahr einer Änderung der Schaltereinstellungen für die vordefinierte aktive Anwendung zu begrenzen.
- Für Modbus-RTU-Zubehör (sofern vorhanden), das in der Branche als Sicherheitsrisiko erkannt wird, werden physische Sicherheitsmaßnahmen (wie spezielle Leitungen) empfohlen, um Kommunikationskabel vor unberechtigtem Zugriff, Kommunikationsverlust, Datenlecks und Manipulation usw. zu schützen.
- Für das HMI (falls vorhanden) muss eine Plombe verwendet werden, um unbefugten Zugriff auf Taster oder Drehschalter zu verhindern.
- Für das unabhängige HMI (falls vorhanden) wird dringend empfohlen, die Schnittstelle mit dem ATSE im selben Schaltschrank zu installieren, um die Sicherheit der CANopen-Kommunikation zu gewährleisten oder die Kommunikationskabel durch physische Sicherheitsmaßnahmen (wie dedizierte Leitungen) zu schützen.

Empfohlene Wartungsvorgänge

Die empfohlene Wartung muss während der gesamten Lebensdauer des Geräts regelmäßig durchgeführt werden:

- Stellen Sie sicher, dass auf die neueste Firmware aktualisiert wurde.
- Überprüfen Sie die Überwachungsprotokolle auf unerwartete Verhaltensweisen, z. B. ungültige Anmeldeversuche oder häufige Neustarts.
- Ändern Sie das Administratorpasswort regelmäßig.
- Überprüfen Sie die E/A-Kabel regelmäßig, um sicherzustellen, dass sie ordnungsgemäß angeschlossen sind und kein unbefugter Zugriff erfolgt.
- Überprüfen Sie die Modbus-RTU- und CANopen-Kommunikationskabel regelmäßig, um sicherzustellen, dass kein unbefugter Zugriff erfolgt.
- Deaktivieren Sie die Kommunikationssteuerungsfunktion rechtzeitig, wenn sie nicht benötigt wird. Weitere Informationen finden Sie im Benutzerhandbuch DOCA0214DE-01.

Schneider Electric Support-Portal für Cybersicherheit

Überblick

Das Schneider Electric Cybersicherheit-Support-Portal beschreibt die Schwachstellen-Managementstrategie von Schneider Electric.

Das Ziel der Schwachstellen-Managementstrategie von Schneider Electric ist es, Schwachstellen in der Cybersicherheit zu beseitigen, die Produkte und Systeme von Schneider Electric betreffen, um installierte Lösungen, Kunden und die Umwelt zu schützen.

Schneider Electric arbeitet in einer kooperativen Vorgehensweise mit Forschern, Cyber Emergency Response Teams (CERTs) und Anlagenbesitzern zusammen, um sicherzustellen, dass genaue Informationen rechtzeitig bereitgestellt werden, um ihre Anlagen angemessen zu schützen.

Das Corporate Product CERT (CPCERT) von Schneider Electric ist für das Management und die Ausgabe von Warnmeldungen zu Schwachstellen und Minderungsmaßnahmen, die Produkte und Lösungen betreffen, verantwortlich.

Das CPCERT koordiniert die Kommunikation zwischen relevanten CERTs, unabhängigen Forschern, Produktmanagern und allen betroffenen Kunden.

Verfügbare Informationen im Support-Portal für Cybersicherheit von Schneider Electric

Das Support-Portal bietet folgendes:

- Informationen über die Schwachstellen der Cybersicherheit von Produkten.
- Informationen über Cybersicherheitsvorfälle.
- Eine Schnittstelle, über die Benutzer Cybersicherheitsvorfälle oder -Schwachstellen melden können.

Meldung und Management von Schwachstellen

Cybersicherheitsvorfälle und potenzielle Schwachstellen können über die Website von Schneider Electric Eine Schwachstelle melden gemeldet werden.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Frankreich

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, sollten Sie um Bestätigung der in dieser Veröffentlichung gegebenen Informationen nachsuchen.

DOCA0215DE-01