Serie PacT

TransferPacT Active Automatic (LCD)
TransferPacT Automatic (A rotazione)

Guida alla sicurezza informatica

Pact series offre interruttori e selettori di altissimo livello.

DOCA0215IT-01
06/2022

www.se.com

Informazioni di carattere legale

Sommario

Informazioni di sicurezza

Informazioni importanti

AVVISO

Leggere attentamente queste istruzioni e osservare l’apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avvertimento” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

⚠ DANGER

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

⚠ AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un ***AVVISO*** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

NOTA

Installazione, uso, manutenzione e riparazione delle apparecchiature elettriche vanno affidati solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall’uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, l'installazione e il funzionamento di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

AVVISO SULLA SICUREZZA INFORMATICA

⚠AVVERTIMENTO

POSSIBILITÀ DI COMPROMETTERE LA DISPONIBILITÀ, L'INTEGRITÀ E LA CONFIDENZIALITÀ DEL SISTEMA.

- Cambiare le password predefinite al primo utilizzo per evitare accessi non autorizzati a impostazioni, controlli e informazioni del dispositivo.
- Disattivare porte/servizi e account predefiniti non utilizzati per ridurre al minimo la possibilità di attacchi dannosi.
- Inserire i dispositivi di rete all'interno di numerosi livelli di difesa (come firewall, segmentazione della rete e rilevamento e protezione dalle intrusioni nella rete).
- Seguire le procedure consigliate per la sicurezza informatica (ad esempio, minimo privilegio, separazione dei doveri) per evitare l'esposizione non autorizzata, perdita o malfunzionamento di dati e registri o interruzione dei servizi.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Informazioni sul manuale

Ambito del documento

Questa guida fornisce informazioni sugli aspetti di sicurezza informatica dei dispositivi per aiutare i progettisti e gli operatori di sistema a promuovere un ambiente operativo sicuro per il prodotto. Questa guida non tratta l'argomento più generale relativo alla protezione della rete tecnologica operativa o della rete Ethernet aziendale. Per un'introduzione generale alle minacce alla sicurezza informatica e come affrontarle, consultare il documento How Can I Reduce Vulnerability to Cyber Attacks (Come ridurre la vulnerabilità agli attacchi informatici)

NOTA: in questa guida, il termine sicurezza è utilizzato per indicare la sicurezza informatica.

Nota di validità

Le informazioni contenute in questa guida sono pertinenti ai dispositivi Transfer**PacT** Automatic e Transfer**PacT** Active Automatic Transfer Switches.

Informazioni in linea

Le informazioni contenute in questo documento potrebbero essere aggiornate in qualsiasi momento. Schneider Electric raccomanda di scaricare la versione più recente e aggiornata disponibile su www.se.com/ww/en/download.

Le caratteristiche tecniche dei dispositivi descritti nel presente documento sono consultabili anche online. Per accedere alle informazioni online, consultare la homepage di Schneider Electric www.se.com.

Le caratteristiche tecniche presentate in questa guida dovrebbero essere uguali a quelle che appaiono online. Se si nota una differenza tra le informazioni contenute in questa guida e quelle online, utilizzare le informazioni online.

Per la conformità dei prodotti alle direttive ambientali quali RoHS, REACH, PEP e EOLI, visitare il sito *www.se.com/green-premium*.

Documentazione correlata

Titolo documento	Numero documento
Apparecchiatura di commutazione trasferimento TransferPacT Active Automatic (ATSE) - Guida utente	DOCA0215IT-01
How Can I reduce Vulnerability to Cyber Attacks	How Can I Reduce Vulnerability to Cyber Attacks

Introduzione alla sicurezza informatica

Introduzione

La sicurezza informatica protegge la rete di comunicazione e i dispositivi da eventuali interruzioni operative (disponibilità), modifiche delle impostazioni (integrità) o divulgazione di informazioni riservate (riservatezza).

L'obiettivo della sicurezza informatica è:

- contribuire ad aumentare i livelli di protezione dei beni materiali e delle informazioni contro furti, danni, usi impropri o incidenti, mantenendone nel contempo l'accessibilità per gli utenti autorizzati.
- Progettare sistemi sicuri, limitando l'accesso mediante metodi fisici e digitali, identificando gli utenti, implementando procedure di sicurezza e migliori prassi.

Linee guida Schneider Electric

Oltre alle raccomandazioni fornite in questa guida e specifiche per i dispositivi, occorre seguire l'approccio di difesa in profondità di Schneider Electric alla sicurezza informatica.

Questo approccio è descritto nella nota tecnica del sistema How Can I Reduce Vulnerability to Cyber Attacks.

Molte risorse utili e informazioni aggiornate sono inoltre disponibili sul portale per il supporto alla sicurezza informatica nel sito Web globale Schneider Electric.

Caratteristiche del dispositivo

Panoramica

Il dispositivo **TransferPacT** ATSE (Automatic Transfer Switching Equipment, Apparecchiatura di commutazione trasferimento automatico) è progettato con funzionalità di attivazione della sicurezza, con tali funzionalità preimpostate, e possono essere modificate per rispondere alle esigenze della propria installazione. Il dispositivo deve essere configurato e impostato solo da personale qualificato, in quanto la disattivazione o la modifica delle impostazioni influirà sulla sicurezza generale del dispositivo e della rete di comunicazione.

Utilizzare questa guida insieme alla guida utente DOCA0214IT-01 per una configurazione dettagliata delle funzionalità e delle impostazioni del dispositivo.

Caratteristiche della comunicazione

La comunicazione con TransferPacT ATSE avviene tramite i seguenti tipi di interfaccia:

- Comunicazione cablata tramite:
  - Modbus-RTU
  - CANopen
- HMI (Human Machine Interaction) tramite:
  - Schermo LCD con pulsanti per il display e il funzionamento.
  - Selettori a rotazione e microinterruttori con LED per il funzionamento.

Protocolli supportati

- Modbus-RTU per la comunicazione con i dispositivi/sistemi OT (Operational Technology).
- CANopen per comunicazione interna tra il controller principale e gli accessori (ad esempio, modulo DI/DO, modulo di comunicazione Modbus)

  NOTA: Modbus-RTU e CANopen sono protocolli preesistenti che presentano carenze intrinseche nella sicurezza e devono essere compensati con un'ulteriore sicurezza fisica nell'applicazione.

Funzionalità di sicurezza

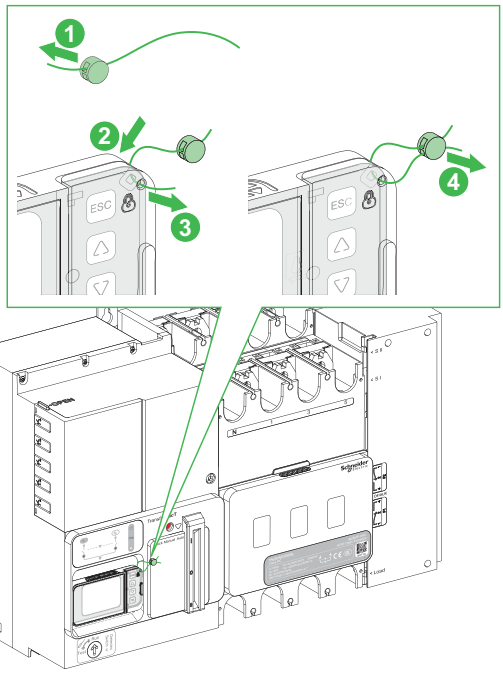
Sono supportate le seguenti funzionalità di sicurezza:

- Il firmware può essere aggiornato in modo sicuro tramite il firmware firmato digitalmente dalla PKI (Public Key Infrastructure) di Schneider.
- Verifica l'integrità dei dati memorizzati nel dispositivo per evitare manomissioni di configurazioni, dati aziendali e altri dati.
- Convalida affidabile dell'ingresso per prevenire attacchi remoti da Modbus-RTU e/o CANopen.
- Qualsiasi modifica alla configurazione è protetta da password.
- La password viene memorizzata come salted hash e può essere reimpostata. Per la reimpostazione della password, consultare la guida utente DOCA0214IT-01.
- La funzionalità di controllo della comunicazione è disattivata per impostazione predefinita e può essere utilizzata solo dopo essere stata attivata localmente. Disattivarla quando non è necessaria.

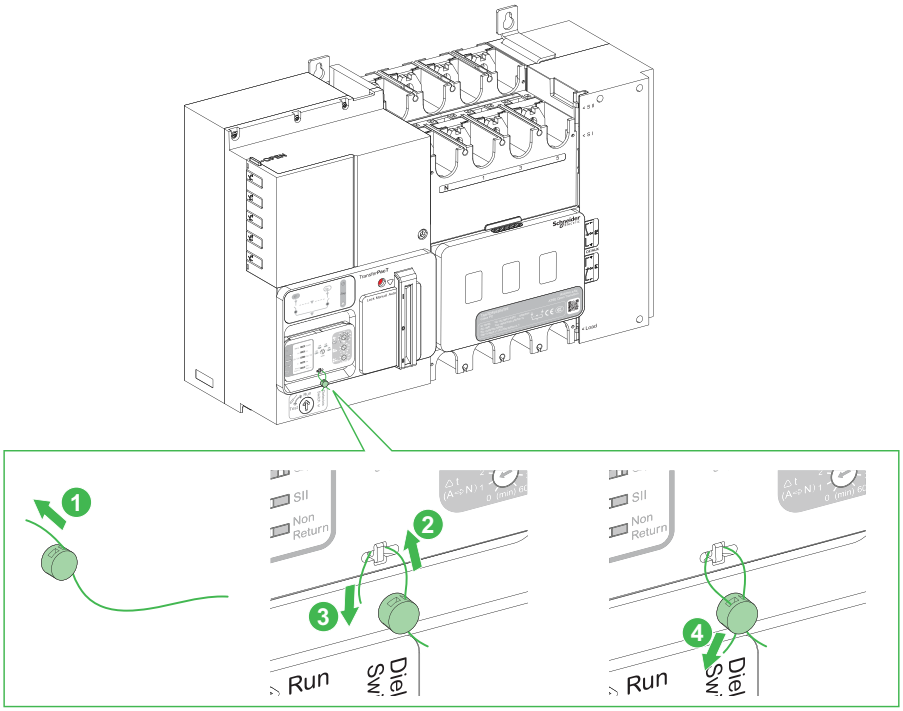
  NOTA: la funzionalità di controllo della comunicazione è supportata solo con TransferPact Active Automatic. Per ulteriori informazioni, vedere la guida utente DOCA0214IT-01.
- Il dispositivo verrà bloccato per 10 minuti dopo 3 tentativi con password non riusciti, utilizzati per prevenire attacchi brute force.
- Genera log di audit per registrare operazioni e logiche aziendali importanti per analisi e previsione, monitoraggio post-evento, indagini e raccolta di prove.

- Coperchio di plastica con foro per consentire agli utenti di applicare una piombatura per impedire l'accesso fisico non autorizzato ai pulsanti (per TransferPact Active Automatic) o ai selettori a rotazione (per TransferPact Automatic).

TransferPacT Active Automatic



TransferPacT Automatic



Sicurezza del dispositivo

Aggiornamento firmware

Il firmware progettato per il dispositivo è firmato dalla PKI (Public Key Infrastructure, infrastruttura a chiave pubblica) di Schneider Electric per assicurare l'integrità e l'autenticità del firmware in esecuzione sul dispositivo.

- Registrarsi sul portale per il supporto alla sicurezza informatica di Schneider Electric.
- Contattare l'assistenza tecnica di Schneider Electric o un agente locale per assistenza nell'aggiornamento del firmware del dispositivo.

Password

La password predefinita è **0000** e deve essere modificata quando viene utilizzata per la prima volta.

NOTA: non utilizzare vecchie password. Se si dimentica la password, contattare l'assistenza locale o consultare la guida utente DOCA0214IT-01.

Data e ora

Nel dispositivo sono presenti certificati e firme digitali, nonché registri di controllo. Per evitare errori, è importante mantenere data e ora sincronizzate. Per ulteriori informazioni su data e ora, consultare la guida utente DOCA0214IT-01.

Registri di controllo

Generare i registri di controllo che tengono nota degli eventi, ad esempio tentativi di accesso non validi e aggiornamento del firmware.

I registri di controllo non contengono informazioni personali e riservate.

Per rilevare comportamenti imprevisti (ad esempio riavvio frequente, aggiornamento firmware errato o tentativi di accesso non validi), si consiglia di monitorare regolarmente i registri di controllo.

Smaltimento dei dispositivi

Il dispositivo contiene informazioni riservate configurate durante la messa in servizio, dati recenti e registri. Ad esempio, queste informazioni possono includere password, topologia del dispositivo Modbus, assorbimenti misurati.

È necessario eseguire il reset della configurazione e ripristinare la password predefinita prima di smaltire il dispositivo. È necessario disporre dell'accesso fisico al dispositivo mentre è acceso. Per la procedura dettagliata su come ripristinare le impostazioni di fabbrica, consultare la guida utente DOCA0214IT-01.

NOTA: è fondamentale pianificare lo smantellamento durante il funzionamento e prima dello smaltimento del dispositivo.

NOTA: verificare che i registri eventi più recenti vengano esportati prima di mettere fuori servizio il dispositivo.

Sicurezza fisica del dispositivo

Di seguito sono elencati i punti di sicurezza fisica importanti da tenere in considerazione per l'installazione del dispositivo:

- Raccomandare di distribuire e utilizzare l’apparecchiatura di commutazione in base a un approccio di difesa in profondità consigliato da Schneider Electronic per ridurre il rischio di attacchi all’apparecchiatura di commutazione.
- Installare l'ATSE in un armadio protetto in modo adeguato, ad esempio con lucchetto o serratura, per evitare rischi durante l'installazione o il rischio di accesso fisico non autorizzato.
- Gli accessori di I/O (se presenti) devono essere distribuiti in modo sicuro per prevenire l'accesso non autorizzato e ridurre il rischio di modifica delle impostazioni degli switch per l'applicazione predefinita in uso.
- Per gli accessori Modbus-RTU (se presenti) riconosciuti come rischi per la sicurezza nel settore, si raccomandano misure di sicurezza fisica (come tubi dedicati) per proteggere i cavi di comunicazione da accessi non autorizzati, cadute di comunicazione, perdite di dati e manomissioni, ecc.
- Per HMI (se presente), utilizzare un sigillo in piombo per impedire l'accesso non autorizzato ai pulsanti o ai selettori a rotazione.
- Per HMI indipendente (se presente), si consiglia di distribuirla con l'ATSE nello stesso armadio per garantire la sicurezza della comunicazione CANopen o per proteggere i cavi di comunicazione con misure di sicurezza fisiche (ad esempio tubi dedicati).

Operazioni di manutenzione consigliate

La manutenzione raccomandata è richiesta regolarmente per tutto il ciclo di vita del dispositivo:

- Accertarsi che il firmware più recente sia aggiornato.
- Controllare i registri di controllo per individuare eventuali comportamenti imprevisti, ad esempio tentativi di accesso non validi o riavvio frequente.
- Modificare regolarmente la password amministratore.
- Controllare regolarmente i cavi di I/O per accertare che siano collegati correttamente e che non vi siano accessi non autorizzati.
- Controllare regolarmente i cavi di comunicazione Modbus-RTU e CANopen per verificare che non vi siano accessi non autorizzati.
- Disattivare la funzionalità di controllo della comunicazione quando non è necessaria. Per ulteriori informazioni, vedere la guida utente DOCA0214IT-01.

Portale per il supporto alla sicurezza informatica Schneider Electric

Panoramica

Il portale per il supporto alla sicurezza informatica Schneider Electric delinea la politica di gestione della vulnerabilità di Schneider Electric.

La politica di gestione della vulnerabilità di Schneider Electric ha lo scopo di affrontare le vulnerabilità di sicurezza informatica che colpiscono i prodotti e i sistemi Schneider Electric, per proteggere le soluzioni installate, i clienti e l'ambiente.

Schneider Electric opera nell'ambito di un approccio collaborativo con ricercatori, team di risposta alle emergenze informatiche (CERT, Cyber Emergency Response Teams) e proprietari delle risorse per garantire la disponibilità tempestiva di informazioni accurate per proteggere adeguatamente le loro installazioni.

Il CPCERT (Corporate Product CERT) di Schneider Electric è responsabile della gestione e dell'emissione di avvisi sulle vulnerabilità e le soluzioni che interessano prodotti e soluzioni.

Il CPCERT coordina le comunicazioni tra i CERT pertinenti, i ricercatori indipendenti, i product manager e tutti i clienti interessati.

Informazioni disponibili sul portale per il supporto alla sicurezza informatica di Schneider Electric

Il portale per il supporto fornisce:

- Informazioni sulle vulnerabilità di sicurezza informatica dei prodotti.
- Informazioni sugli incidenti di sicurezza informatica.
- Un'interfaccia che consente agli utenti di dichiarare gli incidenti o le vulnerabilità di sicurezza informatica.

Gestione e segnalazione delle vulnerabilità

Gli incidenti di sicurezza informatica e le potenziali vulnerabilità possono essere segnalati tramite Report a Vulnerability (Segnala una vulnerabilità) del sito Web di Schneider Electric.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

DOCA0215IT-01