A série PacT

TransferPacT Active Automatic (LCD)
TransferPacT Automatic (rotativo)

Manual de cibersegurança

Pact series fornece disjuntores e comutadores de nível internacional.

DOCA0215PT-01
06/2022

www.se.com

Informações legais

A marca Schneider Electric e quaisquer marcas comerciais da Schneider Electric SE e das respetivas subsidiárias mencionadas neste guia são propriedade da Schneider Electric SE ou das respetivas subsidiárias. Todas as outras marcas podem ser marcas comerciais dos respetivos proprietários. Este guia e o respetivo conteúdo estão protegidos ao abrigo das leis de direitos de autor aplicáveis e são disponibilizados apenas para fins informativos. Não é permitido reproduzir ou transmitir nenhuma parte deste manual em qualquer forma ou através de qualquer meio (eletrónico, mecânico, fotocópia, gravação ou qualquer outro), para quaisquer fins, sem a autorização prévia por escrito da Schneider Electric.

A Schneider Electric não concede qualquer direito ou licença para utilização comercial do guia ou do respetivo conteúdo, exceto para uma licença não-exclusiva e pessoal para a respetiva consulta no "estado atual".

A instalação, o funcionamento, os serviços e a manutenção dos produtos e equipamentos da Schneider Electric devem ser efetuados apenas por pessoal qualificado.

Tendo em conta que, por vezes, as normas, as especificações e os projetos são alterados, as informações presentes neste guia podem estar sujeitas a alterações sem aviso prévio.

Na medida do permitido pela legislação aplicável, a Schneider Electric e as respetivas subsidiárias não assumem qualquer responsabilidade por quaisquer erros ou omissões no conteúdo informativo deste material ou consequências decorrentes ou resultantes da utilização das informações nele contidas.

Como parte de um grupo de empresas responsáveis e inclusivas, estamos a atualizar as nossas comunicações que contêm terminologia não inclusiva. No entanto, até concluirmos este processo, o nosso conteúdo poderá ainda conter termos uniformizados da indústria, que poderão ser considerados inadequados pelos nossos clientes.

Conteúdos

Informações de segurança

Informações importantes

AVISO

Leia com atenção estas instruções e observe o equipamento para familiarizar-se com o dispositivo antes de o tentar instalar, utilizar, colocar em funcionamento ou efetuar a manutenção. As seguintes mensagens especiais podem surgir ao longo deste documento ou no equipamento para avisá-lo de possíveis perigos ou para chamar-lhe a atenção relativamente a informação que esclareça ou simplifique os procedimentos.

A existência deste símbolo em um rótulo de segurança de “Perigo” ou “Atenção” indica perigo de choque elétrico, que pode resultar em ferimentos, se as instruções não forem seguidas.

Este é o símbolo de aviso de segurança. É utilizado para o alertar quanto a possíveis ferimentos pessoais. Obedeça a todas as mensagens de segurança que acompanham o símbolo para evitar possíveis ferimentos ou morte.

DANGER

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

ATENÇÃO

ATENÇÃO indica uma situação perigosa que, se não for evitada, **pode resultar em** morte ou ferimentos graves.

CUIDADO

CUIDADO indica uma situação perigosa que, se não for evitada, **pode resultar em** ferimentos leves ou moderados.

AVISO

AVISO é utilizado para abordar práticas não relacionadas com lesões corporais.

NOTA

A instalação, utilização e manutenção do equipamento elétrico devem ser efetuadas exclusivamente por pessoal qualificado. A Schneider Electric não assume qualquer responsabilidade pelas consequências resultantes da utilização deste material.

Uma pessoa qualificada tem aptidões e conhecimentos relacionados com a construção, instalação e funcionamento de equipamento elétrico e recebeu formação de segurança para reconhecer e evitar os perigos envolvidos.

AVISO DE SEGURANÇA À CIBERSEGURANÇA

⚠ATENÇÃO

RISCO POTENCIAL PARA A DISPONIBILIDADE, INTEGRIDADE E CONFIDENCIALIDADE

- Altere as palavras-passe predefinidas quando utilizar pela primeira vez para ajudar a evitar o acesso não autorizado a definições, controlos e informações do dispositivo.
- Desative portas/serviços não utilizados e contas predefinidas para ajudar a minimizar o acesso a atacantes maliciosos.
- Coloque os dispositivos ligados à rede atrás de várias camadas de defesa cibernética (como firewalls, segmentação de rede e deteção de intrusão e proteção de rede).
- Utilize as melhores práticas de cibersegurança (por exemplo, menos privilégios, separação de funções) para ajudar a evitar a exposição não autorizada, perda, modificação de dados e registos ou a interrupção dos serviços.

O não cumprimento destas instruções pode resultar em morte, lesões graves ou danos no equipamento.

Acerca do manual

Âmbito do documento

Este manual fornece informações sobre os aspetos da cibersegurança para dispositivos para ajudar designers de sistemas e operadores a promover um ambiente de funcionamento seguro para o produto. Este manual não aborda o tópico mais abrangente sobre como proteger a sua rede de tecnologia operacional ou a rede Ethernet da sua empresa. Para obter uma introdução geral a ameaças de cibersegurança e como abordá-las, consulte Como posso reduzir a vulnerabilidade a ataques cibernéticos

NOTA: Neste manual, o termo segurança é utilizado para referir-se à cibersegurança.

Nota de validade

A informação indicada neste manual é relevante para dispositivos relevantes para comutadores de transferência **TransferPacT** Automatic e comutadores de **TransferPacT** Active Automatic.

Informações online

É provável que as informações contidas neste documento sejam atualizadas em qualquer altura. A Schneider Electric recomenda vivamente que tenha a versão mais recente e atualizada disponível em www.se.com/ww/en/download.

As características técnicas dos dispositivos descritos no presente documento estão também indicadas online. Para aceder as informações online, aceda à página inicial da Schneider Electric www.se.com.

As características técnicas apresentadas neste manual devem ser iguais às que aparecem online. Se houver alguma diferença entre as informações contidas neste manual e as informações online, utilize as informações online.

Para obter informações sobre a conformidade dos produtos com as diretivas ambientais, tais como RoHS, REACH, PEP e EOLI, vá para *www.se.com/green-premium*.

Documentação relacionada

Título do documento	Número do documento
Manual do utilizador do equipamento (ATSE) TransferPacT Active Automatic	DOCA0214EN-01
Como posso reduzir a vulnerabilidade a ataques cibernéticos	Como posso reduzir a vulnerabilidade a ataques cibernéticos

Introdução à cibersegurança

Introdução

A cibersegurança protege a rede de comunicação e os dispositivos contra quaisquer operações de interrupção (disponibilidade), modificação de definições (integridade) ou divulgação de quaisquer informações sensíveis (confidencialidade).

Os objetivos da cibersegurança são:

- Fornecer níveis acrescidos de proteção de informações e ativos físicos contra roubo, corrupção, uso indevido ou acidentes, mantendo o acesso aos utilizadores desejados.
- Conceber sistemas seguros, restringir o acesso utilizando métodos físicos e digitais, identificar utilizadores, bem como implementar procedimentos de segurança e melhores práticas.

Diretrizes elétricas da Schneider

Além das recomendações fornecidas neste manual que são específicas para dispositivos, deve seguir a abordagem de defesa em profundidade da segurança cibernética da Schneider Electric.

Esta abordagem é descrita na nota técnica do sistema Como posso reduzir a vulnerabilidade a ataques cibernéticos.

Além disso, estão disponíveis muitos recursos úteis e informações atualizadas no Portal de apoio à segurança cibernética no Website global da Schneider Electric.

Funcionalidades do dispositivo

Descrição geral

O **TranferPacT** ATSE (Equipamento de comutação automática de transferência) foi concebido com funcionalidades de ativação de segurança, e estas funcionalidades estão num estado predefinido e podem ser modificadas para satisfazer as suas necessidades de instalação. O dispositivo só pode ser configurado e definido por pessoal qualificado, uma vez que a desativação ou alteração das definições afetará a robustez da segurança em geral do dispositivo e da rede de comunicação.

Utilize este manual em conjunto com o manual do utilizador DOCA0214PT-01 para obter uma configuração detalhada das funcionalidades e definições do dispositivo.

Características de comunicação

A comunicação com TransferPacT ATSE é efetuada através dos seguintes tipos de interface:

- Comunicação com fios através de:
  - Modbus-RTU
  - CANopen
- Interação Homem-Máquina (HMI) através de:
  - Ecrã LCD com botões para visualização e funcionamento.
  - Comutadores rotativos e oscilantes com LED para funcionamento.

Protocolos suportados

- Modbus-RTU para comunicação com os dispositivos/sistemas de Tecnologia Operacional (OT).
- CANopen para comunicação interna entre o controlador principal e os acessórios (por exemplo, módulo DI/DO, módulo de comunicação Modbus)

  NOTA: O Modbus-RTU e o CANopen são protocolos antigos, que apresentam deficiências inerentes à segurança e necessitam de ser compensados com segurança física adicional na respetiva aplicação.

Funcionalidades de segurança

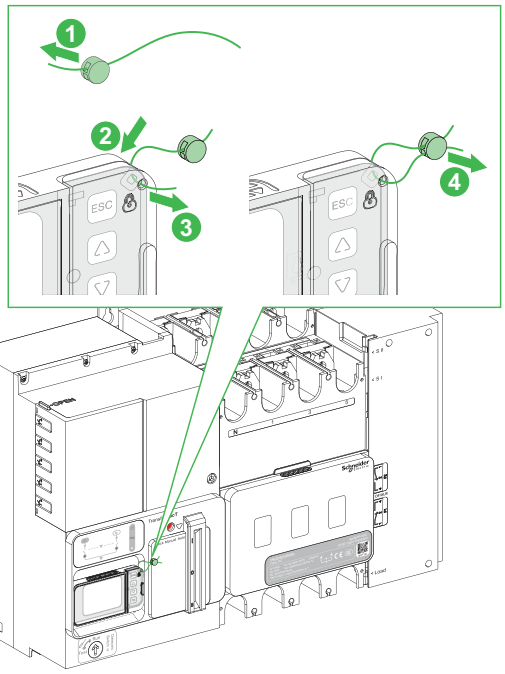
São suportadas as seguintes funcionalidades de segurança:

- O firmware pode ser atualizado com segurança através do firmware assinado digitalmente pela Infraestrutura de chaves públicas da Schneider (PKI).
- Verifica a integridade dos dados armazenados no dispositivo para evitar que configurações, dados empresariais e quaisquer outros dados sejam adulterados.
- Validação robusta da entrada para evitar ataques remotos de Modbus-RTU e/ou CANopen.
- Qualquer modificação de configuração está protegida por palavra-passe.
- A palavra-passe é armazenada como um salted hash e pode ser redefinida. Para repor a palavra-passe, consulte o manual do utilizador DOCA0214PT--01.
- A funcionalidade de controlo de comunicação está desativada por predefinição e só pode ser utilizada depois de ser ativada a nível local. Desative-a a tempo quando não for necessária.

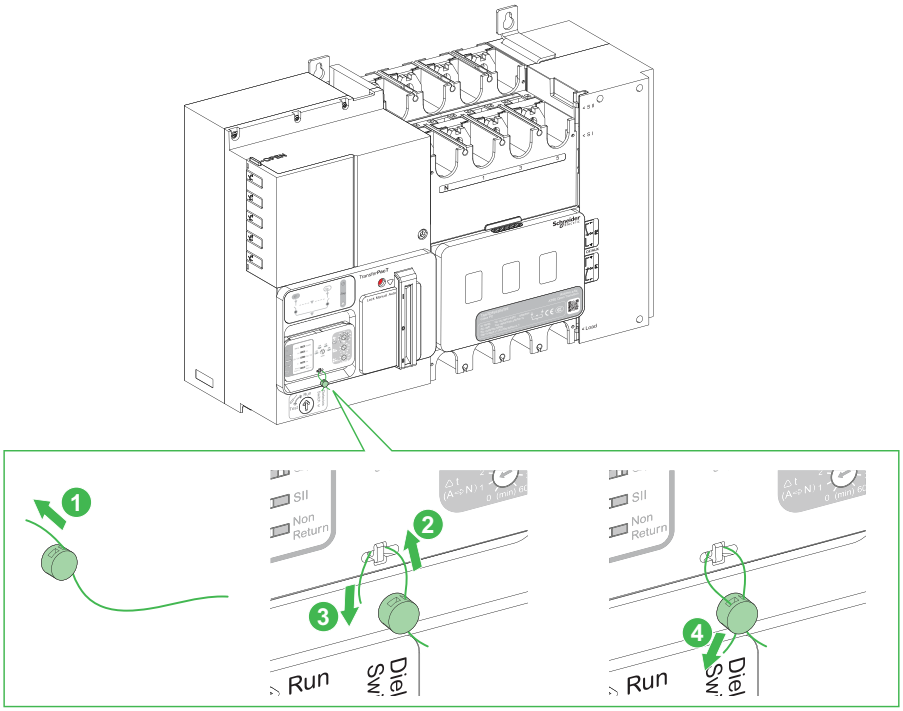
  NOTA: A funcionalidade de controlo de comunicação só é suportada em TransferPact Ative Automático. Para obter mais informações, consulte o guia do utilizador DOCA0214PT–01.
- O dispositivo será bloqueado durante 10 minutos após 3 tentativas falhadas de introdução da palavra-passe, que são utilizadas para evitar ataques de força bruta.
- Gera registos de auditoria para gravar operações importantes e lógica empresarial para análise e previsão, controlo pós-evento, investigação e recolha de provas.

- Cobertura de plástico com orifício para ajudar os utilizadores a instalar a vedação de chumbo, para evitar o acesso físico não autorizado aos botões (para TransferPact Active Automático) ou interrutores rotativos (para TransferPact Automático).

TransferPacT Active Automatic



TransferPacT Automatic



Segurança do dispositivo

Atualização de firmware

O firmware concebido para o dispositivo é assinado pela Infraestrutura de chaves públicas (PKI) da Schneider Electric para garantir a integridade e autenticidade do firmware em execução no dispositivo.

- Efetue o registo no portal de apoio à cibersegurança da Schneider Electric.
- Contacte o apoio da Schneider Electric ou um técnico local para ajudá-lo a atualizar o firmware do dispositivo.

Palavra-passe

A palavra-passe predefinida é **0000**, deve ser alterada quando utilizá-la pela primeira vez.

NOTA: Evite utilizar palavras-passe antigas. Se não se lembrar da palavra--passe, contacte o serviço de campo ou consulte o manual do utilizador DOCA0214PT-01.

Data e hora

O dispositivo inclui certificados e assinaturas digitais, bem como registos de auditoria. Para evitar erros, é importante manter a data e a hora sincronizadas. Para obter mais informações sobre data e hora, consulte o manual do utilizador DOCA0214PT01.

Registos de auditoria

Crie registos de auditoria que gravem os eventos, tais como tentativas de início de sessão inválidas e atualização do firmware.

Os registos de auditoria não contêm quaisquer informações pessoais e sensíveis.

Para detetar comportamentos inesperados (por exemplo, reinicialização frequente, atualização de firmware incorreta ou tentativas de início de sessão inválidas), é recomendável monitorizar registos de auditoria com frequência.

Eliminação do dispositivo

O dispositivo contém informações confidenciais configuradas durante a colocação em funcionamento, valores de dados recentes e registos. Por exemplo, estas informações podem incluir a palavra-passe, topologia do dispositivo Modbus, consumos de energia medidos.

É necessário efetuar a reposição da configuração e restaurar a palavra-passe predefinida antes de eliminar o dispositivo. Deve ter acesso físico ao dispositivo enquanto este estiver ligado. Para obter o procedimento detalhado sobre como repor as definições de fábrica, consulte o manual do utilizador DOCA0214PT-01.

NOTA: É fundamental planear a desativação durante o funcionamento e antes da eliminação do dispositivo.

NOTA: Certifique-se de que os registos de eventos mais recentes são exportados antes do dispositivo ser desativado.

Segurança física do dispositivo

Seguem-se os pontos de segurança física importantes a ter em consideração para instalar o dispositivo:

- Recomendamos que implemente e utilize o equipamento de comutação de acordo com uma abordagem de defesa profunda recomendada pela Schneider Electric para reduzir o risco de ataque ao equipamento de comutação.
- Instale a ATSE num armário protegido de forma adequada, por exemplo com um cadeado ou chave, para evitar riscos durante a instalação ou o risco de acesso físico não autorizado.
- Os acessórios de E/S (se houver) devem ser implantados com firmeza para evitar o acesso não autorizado para atenuar o risco de alterar as definições do interrutor para a aplicação predefinida que estiver a ser utilizada.
- Para os acessórios Modbus-RTU (se houver) reconhecidos como um risco de segurança na indústria, é recomendável tomar medidas de segurança física (como tubos específicos) para proteger os cabos de comunicação contra acessos não autorizados, quedas de comunicação, fugas de dados e adulteração, etc.
- No caso do HMI (caso exista), deve ser utilizado um selo de segurança para impedir o acesso não autorizado a botões ou interrutores rotativos.
- Para o HMI independente (se existente), recomenda-se vivamente implementá-lo com o ATSE no mesmo armário para garantir a segurança da comunicação CANopen ou proteger os cabos de comunicação com medidas de segurança físicas (tais como tubos específicos).

Operações de manutenção recomendadas

É necessário efetuar com frequência uma manutenção recomendada ao longo da vida útil do dispositivo:

- Certifique-se de que o firmware mais recente está atualizado.
- Verifique se existem comportamentos inesperados nos registos de auditoria, tais como tentativas de início de sessão inválidas ou reinicialização frequente.
- Altere com frequência a palavra-passe do administrador.
- Verifique regularmente os cabos de E/S para garantir que estão ligados corretamente e que não há acesso não autorizado.
- Verifique regularmente os cabos de comunicação Modbus-RTU e CANopen para garantir que não existe acesso não autorizado.
- Desative a funcionalidade de controlo de comunicação em tempo útil quando não for necessário. Para obter mais informações, consulte o guia do utilizador DOCA0214PT–01.

Portal de apoio à cibersegurança da Schneider Electric

Descrição geral

O Portal de apoio à cibersegurança da Schneider Electric descreve a política de gestão da vulnerabilidade da Schneider Electric.

O objetivo da política de gestão da vulnerabilidade da Schneider Electric é abordar as vulnerabilidades da segurança cibernética que afetam os produtos e sistemas da Schneider Electric, para proteger as soluções instaladas, os clientes e o ambiente.

A Schneider Electric adota uma abordagem de colaboração com investigadores, equipas de resposta a emergências cibernéticas (CERT) e proprietários de ativos para garantir que são fornecidas informações rigorosas de maneira atempada para proteger as suas instalações de maneira adequada.

O CERT (Corporate Product CERT) da Schneider Electric é responsável pela gestão e emissão de alertas sobre vulnerabilidades e mitigação que afetam produtos e soluções.

O CPCERT coordena as comunicações entre CERT relevantes, investigadores independentes, gestores de produtos e todos os clientes afetados.

Informações disponíveis no Portal de apoio à cibersegurança da Schneider Electric

O portal de apoio fornece o seguinte:

- Informações sobre as vulnerabilidades de cibersegurança dos produtos.
- Informações sobre incidentes de cibersegurança.
- Uma interface que permite aos utilizadores declararem vulnerabilidades ou incidentes de cibersegurança.

Relatórios e gestão da vulnerabilidade

Os incidentes de cibersegurança e potenciais vulnerabilidades podem ser comunicados através do Website da Schneider Electric, Comunicar uma vulnerabilidade.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
França

+ 33 (0) 1 41 29 70 00

www.se.com

Como as normas, especificações e desenhos são periodicamente actualizados, solicite a confirmação das informações incluídas nesta publicação.

DOCA0215PT-01