EcoStruxure Panel Server

Handbuch zur Cybersicherheit

Konzentrator für Wireless-Geräte und Modbus-Gateway, Datenprotokollierer und Energieserver

EcoStruxure stellt eine IoT-fähige Architektur und Plattform bereit.

DOCA0211DE-11
01/2025

www.se.com

Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument 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.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

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 sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

Inhaltsverzeichnis

Sicherheitshinweise....5
Informationen zum Dokument....6
Eine Einführung in die Cybersicherheit....9
Geräteeigenschaften....10
Gerätefunktionen....12
Netzwerksicherheit....14
Cloud-Anwendungssicherheit....17
Physische Sicherheit des Geräts....19
Sicherheitsempfehlungen für die Wartung....20
Glossar....23

Sicherheitshinweise

Wichtige Informationen

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.

⚠ GEFAHR

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

⚠ 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 Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Informationen zum Dokument

Geltungsbereich des Dokuments

Dieses Handbuch enthält Informationen zu Aspekten der Cybersicherheit für den EcoStruxure™ Panel Server, um Systemdesigner und -betreiber bei der Bereitstellung einer sicheren Betriebsumgebung für das Produkt zu unterstützen.

Dieses Handbuch geht nicht auf das allgemeinere Thema zur Sicherung des OT- (Operational Technology) oder Ethernet-Netzwerks in Ihrem Unternehmen ein. Eine allgemeine Einführung in Cybersicherheitsbedrohungen und deren Bekämpfung finden Sie unter Allgemeine Informationen zur Cybersicherheit, Seite 7.

HINWEIS: In diesem Handbuch bezieht sich der Begriff **Sicherheit** auf Cybersicherheit.

Gültigkeitshinweis

Die Informationen in diesem Handbuch beziehen sich auf den EcoStruxure Panel Server.

Online-Informationen

Die in diesem Handbuch enthaltenen Informationen können jederzeit Änderungen unterliegen. Schneider Electric empfiehlt nachdrücklich, dass Sie stets die jeweils neueste, auf der Website www.se.com/ww/en/download verfügbare Version verwenden.

Die technischen Merkmale der in diesem Handbuch beschriebenen Geräte sind ebenfalls online abrufbar. Sie finden die Online-Informationen auf der Hompage von Schneider Electric unter www.se.com.

Allgemeine Informationen zur Cybersicherheit

In den letzten Jahren hat sich durch die wachsende Anzahl an vernetzten Maschinen und Produktionsanlagen das Potenzial für Cyberbedrohungen wie unbefugter Zugriff, Datenverletzungen und Betriebsunterbrechungen entsprechend erhöht. Sie müssen daher alle möglichen Maßnahmen zur Cybersicherheit in Betracht ziehen, um Anlagen und Systeme vor solchen Bedrohungen zu schützen.

Um die Sicherheit und den Schutz Ihrer Schneider Electric-Produkte zu gewährleisten, ist es in Ihrem Interesse, die Best Practices für die Cybersicherheit umzusetzen, die im Dokument Cybersecurity Best Practices beschrieben sind.

Schneider Electric bietet zusätzliche Informationen und Unterstützung:

- Abonnieren Sie den Sicherheits-Newsletter von Schneider Electric.
- Besuchen Sie die Webseite Cybersecurity Support Portal, um:
  - Sicherheitshinweise zu suchen
  - Schwachstellen und Vorfälle zu melden
- Besuchen Sie die Webseite Schneider Electric Cybersecurity and Data Protection Posture, um:
  - auf den Cybersicherheitsstatus zuzugreifen
  - mehr über Cybersicherheit in der Cybersecurity Academy zu erfahren
  - die Cybersicherheits-Services von Schneider Electric zu entdecken

Produktbezogene Informationen zur Cybersicherheit

⚠WARNUNG

MÖGLICHE BEEINTRÄCHTIGUNG DER VERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT DES SYSTEMS

- Deaktivieren Sie nicht verwendete Ports/Dienste, 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 Dienstbereitstellung zu verhindern.

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

Verfügbare Sprachen des Dokuments

Dieses Dokument ist in folgenden Sprachen verfügbar:

- Englisch (DOCA0211EN)
- Französisch (DOCA0211FR)
- Deutsch (DOCA0211DE)
- Italienisch (DOCA0211IT)
- Portugiesisch (DOCA0211PT)
- Spanisch (DOCA0211ES)

Weiterführende Dokumente

Titel der Dokumentation	Referenznummer
EcoStruxure Panel Server - Benutzerhandbuch	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
Best Practices für die Cybersicherheit	7EN52-0390
EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide	ESXP2TG003EN

Sie können diese technischen Veröffentlichungen sowie andere technische Informationen von unserer Website unter www.se.com/ww/en/download/.

Informationen zu nicht-inklusiver oder unsensibler Terminologie

Als verantwortungsbewusstes, integratives Unternehmen aktualisiert Schneider Electric kontinuierlich seine Kommunikationen und Produkte, die nicht-integrative oder unsensible Terminologie enthalten. Trotz dieser Bemühungen können unsere Inhalte jedoch nach wie vor Begriffe enthalten, die von einigen Kunden als unangemessen betrachtet werden.

Marken

QR Code ist eine eingetragene Marke von DENSO WAVE INCORPORATED in Japan und anderen Ländern.

Eine Einführung in die Cybersicherheit

EcoStruxure Master-Baureihe

EcoStruxure ist eine IoT-fähige, offene und interoperable Plug&Play-Architektur und -Plattform von Schneider Electric für Haushalte, Gebäude, Rechenzentren, Infrastrukturen und Industrie. Innovation auf jeder Ebene von verbundenen Produkten bis hin zu Edge Control, Anwendungen, Analyselösungen und Diensten.

Einführung

Cybersicherheit soll dazu beitragen, Ihr Kommunikationsnetzwerk und alle damit verbundenen Geräte vor Angriffen zu schützen, die den Betrieb unterbrechen (Verfügbarkeit), Informationen ändern (Integrität) oder vertrauliche Informationen offenlegen (Vertraulichkeit) könnten. Ziel der Cybersicherheit ist es, einen höheren Schutzgrad für Daten und physische Ressourcen bereitzustellen, um diese vor Diebstahl, Beschädigung, Missbrauch oder Unfällen zu schützen, und dabei gleichzeitig den Zugriff für die vorgesehenen Benutzer aufrechtzuerhalten. Cybersicherheit umfasst viele Aspekte, darunter den Entwurf sicherer Systeme, die Einschränkung des Zugriffs mithilfe physischer und digitaler Methoden, die Identifizierung von Benutzern sowie die Umsetzung von Sicherheitsverfahren und Best Practices.

Richtlinien von Schneider Electric

Zusätzlich zu den Empfehlungen in diesem Handbuch, die speziell für den Panel Server gelten, sollten Sie den Defense-in-Depth-Ansatz für Cybersicherheit von Schneider Electric sowie die allgemeinen Informationen zur Cybersicherheit, Seite 7 beachten.

Schneider Electric Richtlinien und Regeln für die Cybersicherheit

Schneider Electric wendet einen Secure Development Lifecycle (SDL)-Prozess an, ein wichtiges Framework, das sich auf die Produktentwicklung konzentriert und sicherstellt, dass Produkte in allen Lebenszyklusphasen sicheren Entwurfsprozessen folgen. Der SDL-Prozess von Schneider Electric entspricht IEC 62443-4.1.

Der SDL-Prozess umfasst Folgendes:

- SDL-Verfahren, die auf interne Entwicklungsmaßnahmen in der gesamten Lieferkette angewendet werden.
- Abschließende Sicherheitsüberprüfung für die Freigabe erforderlich.
- Sicherheitsschulung für Personal, das in der Produktentwicklung tätig ist.

Geräteeigenschaften

Überblick

Der EcoStruxure Panel Server ist mit Sicherheitsfunktionen ausgestattet. Diese Funktionen sind voreingestellt und können an Ihre Installationsanforderungen angepasst werden. Der Panel Server darf nur von qualifiziertem Personal konfiguriert und eingestellt werden, da sich die Deaktivierung oder Änderung von Einstellungen auf die Gesamtsicherheit des Panel Server und Ihre Netzwerksicherheit auswirkt.

Verwenden Sie dieses Handbuch in Verbindung mit dem DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8 für eine detaillierte Konfiguration der Funktionen und Einstellungen des Panel Server.

Schnittstellen des EcoStruxure Panel Server

In der folgenden Tabelle werden die mit dem Panel Server verfügbaren Kommunikationsarchitekturen nach Modell zusammengefasst:

Hauptmerkmale		**EcoStruxure Panel Server**								
		Entry	**Universal**					**Advanced**		
		PAS400	**PAS600**	**PAS600T**	**PAS600L**	**PAS600LWD**	**PAS600PWD**	**PAS800**	**PAS800L**	**PAS800P**
10/100BASE-T Ethernet	Ein RJ45-Port	✓	-	-	-	-	-	-	-	-
	Zwei RJ45-Ports	-	✓	✓	✓	✓	✓	✓	✓	✓
Vorgeschaltete Modbus TCP/IP-Konnektivität		✓	✓	✓	✓	✓	✓	✓	✓	✓
Vorgeschaltete Wi-Fi-Konnektivität		✓	✓	✓	✓	-	-	✓	✓	✓
Nachgeschaltete Modbus TCP/IP-Konnektivität		-	✓	✓	✓	✓	✓	✓	✓	✓
Nachgeschaltete IEEE 802.15.4-Konnektivität		✓	✓	✓	✓	-	-	✓	✓	✓
Nachgeschaltete Modbus SL-Konnektivität		-	✓	✓	✓	✓	✓	✓	✓	✓
Zwei Digitaleingänge (für WAGES (Wasser, Luft, Gas, Elektrizität, Dampf))		-	-	-	✓	✓	-	-	✓	-
Externe Wi-Fi-Antenne		-	✓	✓	✓	-	-	✓	✓	✓
Externe IEEE 802.15.4-Antenne		-	-	-	-	-	-	✓	✓	✓

Konvention

EcoStruxure Panel Server wird im Folgenden kurz Panel Server genannt.

Unterstützte Protokolle

Der EcoStruxure Panel Server unterstützt die folgenden Protokolle:

- DHCP für die netzwerkbasierte IP-Adressierung
- DNS für die Netzwerknamensauflösung
- DPWS für die Netzwerkerkennung

- HTTPS (TLS v1.2) zur Konfiguration über Konfigurationstools und integrierte Webseiten
- IEEE 802.15.4 für die Wireless-Kommunikation im ISM-Funkfrequenzband 2,4 GHz (nicht verfügbar für Modelle „Wired by Design“)
- Modbus TCP und Modbus SL für die Kommunikation mit anderen OT-Geräten (Operational Technology: Betriebstechnologie)
- NTP für die Zeitsynchronisation
- RSTP für robuste Ethernet-Ringtopologien für kritische Anwendungen
- SFTP für die Veröffentlichung von CSV-Dateien auf einem SFTP-Server
- VPN-Client für den Fernzugriff (zugänglich für das Customer Care Center von Schneider Electric)
- WPA2 und WPA für die Wi-Fi-Kommunikation (nicht verfügbar für Modelle „Wired by Design“)

Sicherheitsfunktionen

Der EcoStruxure Panel Server unterstützt die folgenden Sicherheitsfunktionen:

- Nur von Schneider Electric digital signierte Firmware kann auf dem Panel Server installiert werden.
- Bei jedem Start wird die digitale Firmware-Signatur vor der Ausführung validiert, um sicherzustellen, dass sie nicht manipuliert wurde.
- Benutzerpasswörter werden als mit Salt versehene und gehashte Passwörter (SHA256) gespeichert.
- Über die Schaltfläche zum Neustart können Sie alle Informationen aus dem Panel Server löschen.
- Das Gerät verfügt über eine interne Uhr und speichert Datum und Uhrzeit für einige Monate ohne Stromversorgung.
- Der Authentizitätsschlüssel des Panel Server ist in einem hochsicheren Chip des Typs Common Criteria CC EAL6+ gespeichert.

Gerätefunktionen

Firmwareaktualisierung

Aktualisieren Sie den EcoStruxure Panel Server auf die neueste Firmwareversion, um die neuesten Funktionen und die aktuellen Sicherheitspatches zu erhalten. Die für den EcoStruxure Panel Server entwickelte Firmware wird mit der Public Key-Infrastruktur (PKI) von Schneider Electric signiert, um die Integrität und Authentizität der auf dem EcoStruxure Panel Server ausgeführten Firmware zu gewährleisten. Um einen ordnungsgemäßen PKI-Betrieb zu gewährleisten, muss das Gerätedatum synchronisiert werden (siehe Datum und Uhrzeit, Seite 12).

Registrieren Sie sich für Security Notifications im Support-Portal für Cybersicherheit von Schneider Electric, um über Sicherheitsupdates informiert zu werden.

Datum und Uhrzeit

Es ist wichtig, Datum und Uhrzeit für die folgenden Zwecke synchronisiert zu halten:

- Um Fehler bei Zertifikaten und digitalen Signaturen im EcoStruxure Panel Server zu vermeiden
- Zur Bereitstellung eines genauen Zeitstempels in Audit-Protokollen zur Unterstützung der forensischen Sicherheit

Weitere Informationen zu Datum und Uhrzeit finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

Deaktivieren nicht verwendeter Funktionen

Mit dem EcoStruxure Panel Server können Sie nicht verwendete Ports/Dienste deaktivieren, um potenzielle Zugänge für bösartige Angreifer zu blockieren.

Es wird empfohlen, Folgendes zu deaktivieren:

- Wi-Fi-Aktivierung und Wi-Fi-Infrastruktur. Das Wi-Fi kann bei Bedarf dauerhaft deaktiviert werden.
- Wi-Fi-Zugangspunkt (standardmäßig aktiviert). Wenn der Zugangspunkt deaktiviert ist, wird durch Drücken der Taste an der Frontseite des Panel Server keine Zugangspunktaktivierung ausgelöst. Durch die Deaktivierung der Wi-Fi-Aktivierung wird auch der Wi-Fi-Zugangspunkt deaktiviert und jede aktive Verbindung unterbrochen.
- IEEE 802.15.4 (standardmäßig nicht aktiviert). IEEE 802.15.4 kann dauerhaft deaktiviert werden.
- Modbus-Gateway-Dienste (standardmäßig aktiviert). Können an jeder Schnittstelle (Ethernet 1, Ethernet 2 und/oder Wi-Fi) auf den Panel Server-Webseiten deaktiviert werden.
- DPWS (Erkennungsprotokoll über IP v4/6) (standardmäßig aktiviert).
- RSTP Rapid Spanning Tree Protocol (standardmäßig nicht aktiviert).

  HINWEIS: Wi-Fi und IEEE 802.15.4 sind nativ auf Wired by Design (WD)-Modellen, die über keinen Wireless-Chipsatz verfügen, nicht verfügbar.

Weitere Informationen zum Deaktivieren nicht verwendeter Funktionen des EcoStruxure Panel Server finden Sie hier: DOCA0172••*EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

TCP-Ports

Die folgenden TCP-Ports werden im EcoStruxure Panel Server verwendet:

- Port 443: HTTPS
- Port 502: Modbus
- Port 5357: DPWS (kann geändert werden)

HINWEIS: Panel Server integriert keinen SSH-Server.

Audit-Protokolle

Der EcoStruxure Panel Server generiert Audit-Protokolle, in denen Ereignisse wie beispielsweise ungültige Anmeldeversuche und Firmwareaktualisierungen aufgezeichnet werden.

Die Protokolle enthalten keine personenbezogenen Informationen.

Um unerwartetes Verhalten (z. B. häufige Neustarts, falsche Firmwareaktualisierungen oder ungültige Anmeldeversuche) zu erkennen, wird empfohlen, die Audit-Protokolle regelmäßig zu prüfen. Weitere Informationen zu Diagnoseprotokollen finden Sie hier: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

Entsorgung des Geräts

Der EcoStruxure Panel Server enthält vertrauliche Informationen, die bei der Inbetriebnahme konfiguriert werden, sowie aktuelle Datenwerte und Protokolle. Diese Informationen können beispielsweise eine Modbus-Gerätetopologie, ein Wireless-Netzwerke, Wi-Fi-Passwörter oder den gemessenen Stromverbrauch umfassen.

Vor der Entsorgung des EcoStruxure Panel Server ist eine Rücksetzung auf die Werkseinstellungen erforderlich. Sie müssen physischen Zugriff haben, um den EcoStruxure Panel Server während der Ausführung dieses Verfahrens aus- und wieder einschalten zu können. Anweisungen zum Zurücksetzen des EcoStruxure Panel Server auf die Werkseinstellungen finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

Netzwerksicherheit

Einführung

Der EcoStruxure Panel Server ist nicht für eine direkte Verbindung mit dem öffentlichen Internet ausgelegt. Er muss mindestens hinter der NAT (Network Address Translation: Netzwerkadressübersetzung) oder vorzugsweise hinter mehreren Firewalls installiert werden. Weitere Informationen finden Sie auf den folgenden Webseiten:

- Beratungsservices zur Cybersicherheit von Schneider Electric
- National Institute of Standards and Technology (NIST)
- Agentur der Europäischen Union für Cybersicherheit (ENISA)

Netzwerksegmentierung

Der EcoStruxure Panel Server ist ein Gateway. Er richtet eine Brücke (Bridge) zwischen verschiedenen Netzwerken ein. Die Netzwerksegmentierung trägt zur Gewährleistung der Cybersicherheit bei. Zur Verbesserung der Netzwerksegmentierung verfügen Panel Server Universal und Advanced über zwei Ethernet-Ports. Sie können im getrennten Modus eingesetzt werden, um einen Port speziell für die Informationstechnologie (IT) und einen Port für die Betriebstechnologie (OT) zu nutzen. Die Netzwerksegmentierung ermöglicht eine Abgrenzung der OT- und IT-Netzwerke, da Netzwerkpakete nicht von einer Seite zur anderen übertragen werden.

Es wird empfohlen, das Netzwerk im getrennten Modus zu konfigurieren (weitere Informationen zu den Netzwerkeinstellungen finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8).

Auf diese Weise können Sie den Panel Server mit folgenden Komponenten verbinden:

- Nachgeschalteten OT-Geräten per Modbus TCP über den einen Ethernet-Port
- Einem vorgeschalteten IT-PC mit SCADA-System und Inbetriebnahmesoftware über den anderen Ethernet-Port

HTTPS und Modbus sind verfügbar auf Panel Server-Ethernet-Schnittstellen (ETH1, ETH2) und Wi-Fi.

In der folgenden Tabelle werden die Standardeinstellungen für jede Schnittstelle aufgeführt:

Schnittstelle		**Modbus**
Ethernet in geschalteter Topologie		Aktiviert
Ethernet in getrennter Topologie	ETH1-Port	Aktiviert
	ETH2-Port	Deaktiviert
Wi-Fi-Infrastruktur		Deaktiviert
Wi-Fi-Zugangspunkt		Nicht verfügbar

Es wird empfohlen, den Modbus-Dienst in Netzwerken zu deaktivieren, in denen er nicht verwendet wird. Weitere Informationen zur Dienstaktivierung finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

Webserver-Zertifikat des Produkts

Um eine sichere HTTP-Kommunikation zu unterstützen, ist der EcoStruxure Panel Server standardmäßig mit einem X.509v3-Zertifikat ausgestattet. Mit diesem Zertifikat wird die Integrität und Vertraulichkeit beim Einrichten der HTTPS-Kommunikation sichergestellt.

Webbrowser erkennen nur Zertifikate für öffentliche Websites. Da der Panel Server in einem lokalen Netzwerk (LAN) installiert ist, können Webbrowser einen Panel Server nicht von einem anderen unterscheiden. Daher wird im Webbrowser bei der Verbindungsherstellung zum Panel Server eine Sicherheitsmeldung angezeigt.

Eine direkte Kabelverbindung trägt zur Sicherung des Kommunikationspfads mit dem Panel Server bei. Weitere Informationen zum ersten Zugriff auf die Webseiten des EcoStruxure Panel Server über einen PC finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

Fingerabdruck des SFTP-Server-Schlüssels

Wenn Sie Ihre Daten auf einem SFTP-Server veröffentlichen, müssen Sie sicherstellen, dass der Fingerabdruck des Schlüssels, der bei der Konfiguration der Serveradresse angezeigt wird, mit dem SFTP-Schlüssel Ihres Servers übereinstimmt.

Wenn Sie den SFTP-Schlüssel auf Ihrem Server erneuern, kann der Panel Server die Dateien nicht mehr senden, da die Verbindung nicht authentifiziert wird. Sie müssen die Veröffentlichung für den Panel Server neu konfigurieren, um den neuen SFTP-Schlüssel-Fingerabdruck aufzuzeichnen.

Wireless-Netzwerk

Funkprotokolle sind anfällig für physische Sicherheitsverletzungen. So kann beispielsweise ein Denial-of-Service-Angriff das Funksignal mit einem leistungsstarken Störsender in der Nähe blockieren.

Es wird daher empfohlen, die physische Sicherheit an die Kritikalität der Informationen anzupassen, die über Funkprotokolle übertragen werden. Zu diesem Zweck können die Wireless-Netzwerke (Wi-Fi und IEEE 802.15.4) im Panel Server dauerhaft deaktiviert werden. Wenn Sie sicher sind, dass Sie nie Wireless-Netzwerke (Wi-Fi und IEEE 802.15.4) benötigen, und nur in diesem Fall, können Sie sie dauerhaft deaktivieren. Weitere Informationen zur permanenten und gleichzeitigen Deaktivierung der Wireless-Netzwerke finden Sie in folgendem Handbuch: DOCA0172•• *EcoStruxure Panel Server - Benutzerhandbuch*, Seite 8.

> **HINWEIS:** Mit den Wired by Design (WD)-Modellen des Panel Server können Sie die Richtlinien für Nicht-Wireless-Geräte einhalten, da diese keinen Wireless-Chipsatz enthalten.

Es wird empfohlen, die Inbetriebnahme von Wireless-Geräten gemäß IEEE 802.15.4 an einem Ort durchzuführen, der vor nicht autorisierten Funksendern sicher ist, z. B. in einem Administratorraum.

Für Wi-Fi-Netzwerke wird die Verwendung des Protokolls WPA2 (Wi-Fi Protected Access Version 2) empfohlen.

> **HINWEIS:** Das TKIP-Protokoll (Temporal Key Integrity Protocol) wird nicht unterstützt.

Fernzugriff (VPN)

Der Panel Server bietet eine Fernzugriffsfunktion, die dem Schneider Electric Customer Care Center (CCC) den Aufbau einer Verbindung zu den Panel Server-Webseiten ermöglicht.

Der Zugriff ist standardmäßig nicht aktiviert und erfordert die Aktivierung der Verbindung durch die Firewall. Weitere Informationen finden Sie unter Erwartete Endpunkte, Seite 17.

Die Fernzugriffsfunktion basiert auf einem VPN der Schicht 3, das standardmäßig keinen Zugriff auf das Netzwerk, sondern nur auf den Panel Server hat. Darüber hinaus ist nur HTTPS für das Tunneling über dieses VPN autorisiert.

Verbundene Geräte

Es wird empfohlen, die Liste der Geräte, die mit dem IEEE 802.15.4-Netzwerk des Panel Server verbunden sind, regelmäßig zu überprüfen. Wenn ein unbekanntes verbundenes Gerät vorhanden ist, suchen und entfernen Sie es. Sie können auch das Netzwerk neu erstellen und nur die identifizierten Geräte erneut verbinden.

Cloud-Anwendungssicherheit

Sicherheit für Daten in Bewegung („Data in Motion“)

Schneider Electric implementiert mit EcoStruxure-Cloud-Anwendungen Best Practices wie:

- Die gesamte Kommunikation zwischen dem EcoStruxure Panel Server und internen Schneider Electric-Systemen oder externen Drittanbietersystemen wird mit HTTPS verschlüsselt (erforderliche Mindeststufe ist TLS 1.2).
- Das Zertifikat, das für diese verschlüsselten Sitzungen verwendet wird, nutzt den sicheren SHA 256-Hash-Algorithmus. Dies gilt für die Kommunikation zwischen der Panel Server-Anwendung und den Servern auf Microsoft Azure-Cloudplattformen.

Sicherheit für ruhende Daten („Data at Rest“)

Schneider Electric hält sich in jeder nur erdenklichen sinnvollen Weise an Best Practices zur Erstellung sicherer Lösungen und zur Begrenzung des Risikos einer Kompromittierung von Daten, wobei gleichzeitig Datenschutz, Kontrolle und Autonomie der Daten jedes Kunden unabhängig von anderen geschützt werden.

Alle System-zu-System-Anmeldeinformationen und Token werden auf Microsoft Azure-Cloudplattformen gespeichert und verschlüsselt.

Erwartete Endpunkte

Schneider Electric empfiehlt, nur den Zugriff auf erforderliche Domänen entsprechend Ihren Anforderungen zu gewähren.

In der folgenden Tabelle werden die Domänennamen und Protokolle aufgeführt, die verwendet werden, wenn der Panel Server eine Verbindung zur Cloud herstellt.

Domänenname	Protokoll	Beschreibung
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (TCP-Port 443)	Wird bei der ersten Verbindung des Panel Server mit der Cloud (oder nach einem Zurücksetzen auf die Werkseinstellungen) verwendet, um den Panel Server zu authentifizieren und zu registrieren.
etp.prod.StruXureWareCloud.com	HTTPS (TCP-Port 443)	Wird zum Herunterladen eines Firmware-Updates verwendet.
cnm-ih-na.Azure-devices.net	HTTPS (TCP-Port 443)	Wird für die Kommunikation des Panel Server mit Cloud-Services von Schneider Electric wie Konfiguration, Daten oder Alarme verwendet.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (TCP-Port 443)	Erlaubt dem Customer Care Center von Schneider Electric den Fernzugriff auf die Panel Server-Webseiten über VPN.
cnmdapiappstna.Blob.Core.Windows.net	HTTPS (TCP-Port 443)	Ermöglicht dem Panel Server den Upload von Protokollen und Diagnosedateien auf Anfrage vom Customer Care Center von Schneider Electric.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (TCP-Port 443)	Ermöglicht dem Panel Server den Upload einer Topologie in die Schneider Electric Cloud-Services.
time.gl.StruXureWareCloud.com	NTP (UDP-Port 123)	Der NTP-Server ermöglicht die kontinuierliche Synchronisation der Uhr des Panel Server.

HINWEIS: Bei Domänennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Physische Sicherheit des Geräts

Etikett mit Manipulationsanzeige

Der EcoStruxure Panel Server ist mit einem Etikett mit Manipulationsanzeige versehen, das den physischen Schutz des Geräts gewährleistet. Es muss sauber sein und darf keine Manipulationen aufweisen (z. B. Risse oder Kratzer). Schneider Electric rät davon ab, ein Gerät zu verwenden, das sichtbar manipuliert wurde.

Installation

Um die physische Sicherheit des Geräts zu gewährleisten, wird die folgende Installation empfohlen:

- Installieren Sie den EcoStruxure Panel Server in einem Schaltschrank, der entsprechend der Risikostufe Ihrer Installation gesichert ist (z. B. in einem Schaltschrank mit Vorhängeschloss oder Schlüssel).
- Wenn der EcoStruxure Panel Server in einer Schaltanlage montiert wird, installieren Sie die Schaltanlage in einem gesicherten Raum (z. B. mit verschlossener Tür oder Kamera).

  HINWEIS: Der Schutz der physischen Sicherheit des Geräts umfasst den Schutz des QR-Codes. Der QR-Code ermöglicht den Zugriff auf den Gerätecode des Panel Server, der als Anmeldedaten für das Gerät betrachtet werden sollte. Er wird verwendet:

  - Bei der sicheren Inanspruchnahme des Geräts für Cloud-Anwendungen
  - Als Passwort für die Verbindung mit dem Wi-Fi-Zugangspunkt

Passwortverwaltung

Um das Gerät vor böswilligen Angriffen zu schützen, ändern Sie das Passwort des Wi-Fi-Zugangspunkts des Panel Server über die Panel Server-Webseiten.

Das Passwort muss den folgenden Regeln entsprechen:

- Zwischen 8 und 32 Zeichen
- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- Darf nur die folgenden Sonderzeichen enthalten: ! "# $ % & ‘ ( ) * + - , . ; : / ~ < > = ? @ [ ] \ ^ _ ` { } |
- Leerzeichen sind zulässig.

Sicherheitsempfehlungen für die Wartung

Wartungsvorgänge

Während der Lebensdauer des EcoStruxure Panel Server wird empfohlen, regelmäßig folgende Vorgänge durchzuführen:

- Überprüfen Sie die physische Sicherheit des EcoStruxure Panel Server (siehe Etikett mit Manipulationsanzeige, Seite 19).
- Stellen Sie sicher, dass Sie über das neueste Firmware-Update verfügen. Sie sollten sich registriert haben, um Sicherheitsbenachrichtigungen, Seite 12 zu erhalten.
- Überprüfen Sie die verbundenen Geräte, Seite 16 auf das Vorhandensein unbekannter Geräte.
- Überprüfen Sie die Audit-Protokolle, Seite 13 auf unerwartete Verhaltensweisen, z. B. ungültige Anmeldeversuche oder häufige Neustarts.
- Überprüfen Sie Datum und Uhrzeit, Seite 12, um eine Abweichung vom aktuellen Datum zu vermeiden.
- Stellen Sie sicher, dass alle nicht benötigten Dienste und Funktionen deaktiviert sind, Seite 12.

Überprüfung der Sicherheitsfunktionen

Anhand der folgenden Tests können Sie den vorgesehenen Betrieb von Sicherheitsfunktionen über die EcoStruxure Panel Server-Webseiten überprüfen.

Webauthentifizierung

1. Versuchen Sie, sich ohne Passwort bei den EcoStruxure Panel Server-Webseiten anzumelden oder geben Sie ein falsches Passwort ein.

   Ergebnis: Der EcoStruxure Panel Server gewährt Ihnen keinen Zugriff auf die Webseiten.
2. Wiederholen Sie diese Aktion weitere 9 Mal.

   Ergebnis: Der EcoStruxure Panel Server wird 10 Minuten lang gesperrt.
3. Versuchen Sie es weitere 5 Mal.

   Ergebnis: Der EcoStruxure Panel Server wird 60 Minuten lang gesperrt.

Webautorisierung

1. Melden Sie sich bei den EcoStruxure Panel Server-Webseiten an.
2. Setzen Sie ein Lesezeichen für eine Webseite (z. B. **Einstellungen**).
3. Öffnen Sie in Ihrem Browser ein privates Navigationsfenster und öffnen Sie die zuvor mit einem Lesezeichen versehene Webseite.

   Ergebnis: Sie können nicht auf die Webseite zugreifen, Sie werden jedoch auf die Anmeldeseite umgeleitet.

Audit

1. Greifen Sie nach einigen oder allen vorhergehenden Tests auf die Protokoll-Webseite zu.

2. Laden Sie die Protokolldateien herunter.
3. Vergewissern Sie sich, dass die fehlgeschlagenen Versuche in den Protokollen vorhanden sind.

Firmwareaktualisierung

1. Rufen Sie die Webseite **Firmwareaktualisierung** auf.
2. Laden Sie eine beliebige Datei hoch (z. B. ein Bild oder ein Textdokument).

   Ergebnis: Der EcoStruxure Panel Server meldet eine falsche Signatur.
3. Greifen Sie auf die Audit-Protokolle zu.
4. Vergewissern Sie sich, dass die fehlgeschlagene Firmwareaktualisierung in den Protokollen vorhanden ist.

Deaktivieren der Dienste

1. Um das Menü aufzurufen und die Dienste zu deaktivieren, wählen Sie **Einstellungen > Netzwerkkommunikation > DPWS** aus.
2. Verbinden Sie einen PC mit dem Windows-Betriebssystem mit demselben lokalen Netzwerk.
3. Klicken Sie im Datei-Explorer auf „Netzwerk“.

   Ergebnis: Der EcoStruxure Panel Server wird nicht erkannt und erscheint daher nicht in der Liste der Geräte im Netzwerk.

Deaktivieren der Wireless-Dienste

So greifen Sie auf die Menüs zu, um die Wireless-Dienste vorübergehend zu deaktivieren:

- Navigieren Sie für W-Fi zu **Einstellungen > Netzwerkkommunikation > Wi-Fi**, klicken Sie auf den Schieberegler **Wi-Fi-Aktivierung** und speichern Sie Ihre Änderungen.

  Ergebnis: In Ihrer Schnittstelle zur Wi-Fi-Zugangspunktverwaltung ist kein EcoStruxure Panel Server verbunden.
- Navigieren Sie für IEEE 802.15.4 zu **Einstellungen > Drahtlose Geräte > Netzwerkkonfiguration**, klicken Sie auf den Schieberegler **Drahtlose Aktivierung** und speichern Sie Ihre Änderungen.

  Ergebnis: Alle unter **Einstellungen > Drahtlose Geräte > Drahtlose Geräte** aufgelisteten Wireless-Geräte weisen nach einer bestimmten Zeit den Status **Nicht angeschlossen** auf, abhängig vom Wireless-Gerät (weitere Informationen finden Sie in der Dokumentation Ihres Geräts).

Glossar

D

DPWS - Devices Profile for Web Services (Geräteprofil für Webdienste):

Minimaler Satz von Implementierungsbeschränkungen, um sicheres Webdienst-Messaging, -Erkennung, -Beschreibung und -Ereignisse auf ressourcenbeschränkten Geräten zu ermöglichen.

H

HTTP - Hypertext Transfer Protocol:

Netzwerkprotokoll zur Übertragung von Dateien und Daten im World Wide Web.

HTTPS - Hypertext Transfer Protocol Secure:

Eine Variante des Standard-Internetübertragungsprotokolls (HTTP), das eine Sicherheitsschicht für die Daten, die übertragen werden, durch eine Secure Socket Layer (SSL)- oder Transport Layer Security (TLS)-Protokollverbindung hinzufügt.

I

IP - Internetprotokoll:

IP-Adressen werden verwendet, um Geräte zu identifizieren, die mit dem Intranet des Unternehmens oder mit dem Internet verbunden sind.

IT - Informationstechnologie:

Die Informationssysteme und das Informationsnetzwerk des Unternehmens im Gegensatz zu seinem OT-Netzwerk.

L

LAN - Lokales Netzwerk:

Das Intranet des Unternehmens oder das IT-Netzwerk.

M

Modbus TCP/IP:

Ein Protokoll, das eine Client/Server-Kommunikation zwischen Geräten und TCP/IP über eine Ethernet-Verbindung herstellt.

O

OT - Betriebstechnologie:

Die Hardware- und Softwaresysteme, die das Unternehmen zur direkten Überwachung und Steuerung von Produktionsprozessen und Anlagen verwendet, auch als „Industrial Control (IC) Network“ bezeichnet. OT wird häufig verwendet, um auf das Betriebstechnologienetzwerk des Unternehmens im Gegensatz zu seinem IT-Netzwerk zu verweisen.

P

PKI - Public Key-Infrastruktur:

Definiert eine Reihe von Diensten, die zum Generieren und Authentifizieren digitaler Signaturen verwendet werden. Eine Public Key-Infrastruktur soll Vertraulichkeit, Integrität und Authentizität von Informationen garantieren.

S

SCADA - Supervisory control and data acquisition:

Systeme, die entwickelt wurden, um Echtzeitdaten über Produktionsprozesse und Anlagen zur Fernüberwachung und Fernsteuerung zu erhalten.

SFTP - Secure File Transfer Protocol:

Eine sichere Version des File Transfer Protocol, das den Datenzugriff und die Datenübertragung über einen Secure Shell (SSH)-Datenstrom erleichtert.

Sicherheitsstrategie:

Unter einer Systemsicherheitsstrategie werden die Sicherheitseinstellungen verstanden, die auf das gesamte gesicherte System angewendet werden. Eine Sicherheitsstrategie bezieht sich im Allgemeinen auf die Anwendung von Normen. Sie wird verwendet, um alle sicherheitsrelevanten Konfigurationen für alle Geräte zu definieren.

T

TCP/IP - Transmission control protocol/Internet protocol:

Protokolle, die für die Kommunikation über das Internet verwendet werden.

V

VPN - Virtuelles privates Netzwerk:

Ein VPN wird verwendet, um einen sicheren / privaten „Tunnel“ zwischen einem authentifizierten externen Zugangspunkt und dem vertrauenswürdigen Unternehmensnetzwerk einzurichten.

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.

DOCA0211DE-11