



SPEICHERPROGRAMMIERBARE STEUERUNG

Sicherheitsleitfaden



FP-Industry 4.0 Communicator
(FP-I4C)

Haftung und Copyright

Dieses Handbuch ist urheberrechtlich geschützt. Dieses Handbuch darf ohne schriftliche Zustimmung von Panasonic Electric Works Europe AG (PEWEU) weder ganz noch teilweise kopiert werden.

PEWEU verbessert das Design und die Leistung seiner Produkte kontinuierlich. Aus diesem Grund behalten wir uns das Recht vor, das Handbuch/Produkt ohne Ankündigung zu ändern. In keinem Fall ist PEWEU für direkte, spezielle, zufällige oder Folgeschäden jeglicher Art haftbar, die aufgrund eines eventuellen Mangels oder Fehlers des Produkts oder der Dokumentation entstanden sind, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Bitte richten Sie Supportanfragen und technische Fragen an Ihren lokalen Panasonic-Vertriebspartner oder das Panasonic Service Center.

Panasonic Electric Works Europe AG (PEWEU)

Caroline-Herschel-Straße 100
85521 Ottobrunn, Deutschland
Tel: +49 89 45 354-1000

Inhaltsverzeichnis

Haftung und Copyright.....	2
1 Informationen zu diesem Dokument	4
2 Sicherheitskonzept für Produkte von Panasonic	4
3 Standardkonfiguration des FP-I4C-Moduls	4
4 Mögliche Bedrohungsszenarien.....	6
5 Allgemeine Sicherheitsvorkehrungen.....	7
6 Bewährte Verfahren zur Absicherung Ihres FP-I4C-Moduls.....	8
6.1 Systemeinstellungen	8
6.1.1 Passwortschutz.....	8
6.1.2 Firewall-Einstellungen	8
6.1.3 Protokolldateien und SSH-Debugging-Funktionen	9
6.2 Anwendungseinstellungen.....	9
7 FAQ.....	12
8 Checkliste für die Sicherheitskonfiguration	13
Panasonic Hotline	14
Änderungsverzeichnis	15

1 Informationen zu diesem Dokument

Interne und externe Cybersicherheitsrisiken entwickeln sich mit der zunehmenden Digitalisierung und der steigenden Vernetzung weiter.

So veröffentlichte das BSI (Bundesamt für Sicherheit in der Informationstechnik) einen Bericht mit den zehn häufigsten Bedrohungen und definierte Regeln und Empfehlungen für Netzwerkprodukte in industriellen Steuerungssystemen (ICS):

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- DDoS-Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld

Quelle: <https://www.bsi.bund.de/ICS>

Dieses Dokument enthält die Geräteinformationen, die Sie für Ihr Netzwerkmanagement benötigen, und unterstützt Sie dabei, das FP-I4C-Modul vor Sicherheitsrisiken zu schützen.

2 Sicherheitskonzept für Produkte von Panasonic

Produkte und Dienstleistungen von Panasonic unterliegen einem kontinuierlichem Verbesserungsprozess. Die Produkte werden unter strenger Beachtung von Sicherheitsrichtlinien entwickelt und vor Auslieferung ausführlich getestet. Das Sicherheitskonzept von Panasonic basiert auf internationalen Richtlinien entsprechend IEC 62443 und ISO/IEC 27001.

Das [Panasonic Product Security Incident Response Team](#) (Panasonic PSIRT) ist das zentrale Koordinationsteam, an das Sicherheitsrisiken im Zusammenhang mit Produkten von Panasonic gemeldet werden können.

3 Standardkonfiguration des FP-I4C-Moduls

Die integrierten Netzwerkfunktionen des FP-I4C-Moduls stellen ein potenzielles Sicherheitsrisiko dar. Achten Sie darauf, die Standardeinstellungen anzupassen, um dieses Risiko zu beseitigen oder zu minimieren.

- Für die Konfiguration des FP-I4C-Moduls wurde ein werkseitiges Standardpasswort festgelegt. Wir empfehlen, das Standardpasswort so bald wie möglich zu ändern.
- Die beiden Ethernet-Ports ETH0 und ETH1 haben unterschiedliche Konfigurationen: ETH0 ist als DHCP-Client und ETH1 ist mit der festen IP-Adresse 192.168.0.1 konfiguriert.
- Standardmäßig sind die folgenden Ports geöffnet und befinden sich im Listening-Modus:

Port-Nr.	Protokoll	Funktion
80, 8081, 443	TCP	Für die Browserkonfiguration und für Benutzer-Webseiten verwendet
53	TCP	Für den DNS-Dienst verwendet
990- 991	UDP	Für Geräteerkennung über Broadcast verwendet
21	TCP	Laufzeit- und Projektmanagement (passiver FTP-Modus: 16384-17407/TCP, 18756-18759/TCP)
16384-17407, 18756-18759	TCP	Passiver FTP-Modus

- Alle Funktionen und Dienste des FP-I4C-Moduls, die ein Sicherheitsrisiko darstellen könnten, wurden werkseitig deaktiviert.
Die Dienste sind unter IP/machine_config/#/services aufgeführt.

Dienst	Sicherheitsrisiko
Autorun-Skripte	Anwendungen, die von einem externen Speichermedium, z. B. einem USB-Stick, gestartet werden
Avahi-Dämon	Öffnet Port 5353 (zum Erfassen von Informationen und zur Suche nach Funktionen)
Cloud-Dienst	Beispiel: eine OpenVPN-Serverkonfiguration aus einer früheren Nutzung
DHCP-Server	Öffnet Port 67, 68
SNMP-Server	Öffnet Port 161, 10161 (zum Erfassen von Informationen)
SSH-Server	Öffnet Port 22 (Anmeldung mit Administratorrechten und Ausführung von Befehlen)
VNC-Server	Öffnet Port 5900 (Webseite und Gerätesteuerung)

- Standardmäßig ist die im FP-I4C-Modul implementierte Firewall (IP/machine_config/#/services) deaktiviert.
- Das FP-I4C-Modul schreibt Protokolldaten und untypische Nutzungsinformationen in Protokolldateien. Diese Dateien werden auf dem Modul gespeichert und können mit Administratorrechten heruntergeladen werden.

Hinweis:

Verwenden Sie die Firewall, um ungenutzte Ports zu schließen, stellen Sie jedoch sicher, dass die Ethernet-Ports 80 und 443 geöffnet sind und in der Firewall-Konfiguration enthalten sind. Andernfalls wird der Zugriff auf die Systemeinstellungsseite dauerhaft verweigert.

Verwandte Themen:

[Firewall-Einstellungen](#)

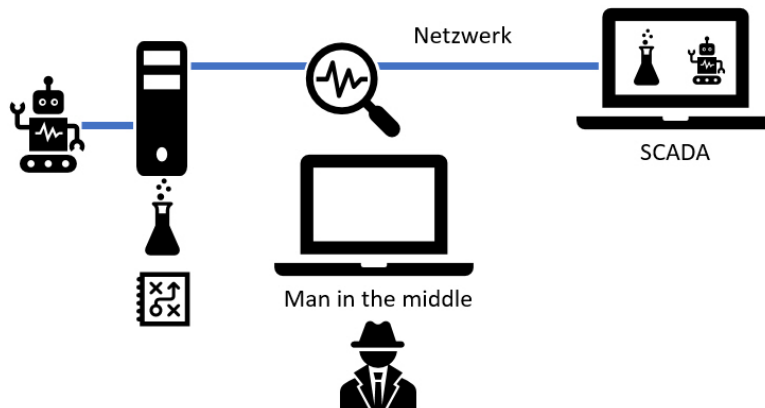
4 Mögliche Bedrohungsszenarien

Damit Sie sich möglicher Cyber-Bedrohungen bewusst werden und diese besser verstehen, sind im Folgenden einige typische Beispiele aufgeführt.

- Abfangen von Daten

Es gibt viele Tools, mit denen der Datenverkehr im Netz ausgelesen werden kann, einschließlich Benutzernamen, Passwörtern und anderen sensiblen Daten wie Rezepturen oder Prozessdaten.

Besonders wenn Ihr Datenverkehr im Netz nicht verschlüsselt ist, wird es Spionen sehr leicht gemacht, nach auslesbaren Informationen zu suchen.

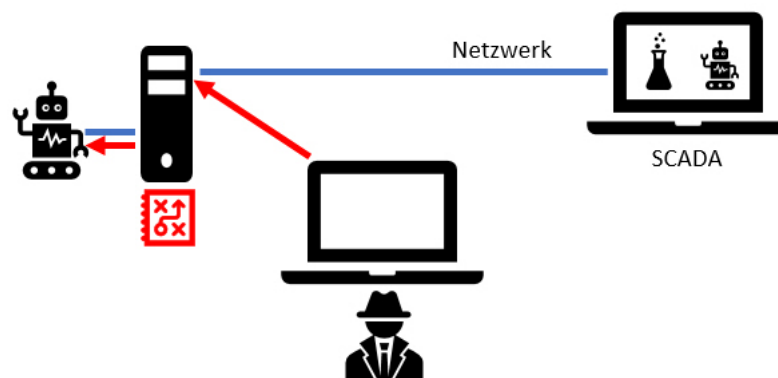


Gegenmaßnahmen:

Verwenden Sie die FTP- oder Telnet-Protokolle nicht außerhalb eines gekapselten Netzwerks, um sensible Daten zu übertragen. Diese Protokolle stellen ein hohes Sicherheitsrisiko dar, da Benutzernamen und Kennwörter in Klartext (unverschlüsselt) übertragen werden.

- Eingriff in Steuerungssysteme

Wenn Zugangsdaten oder das verwendete Protokoll bekannt sind, können unter Umständen Störungen oder Schäden an Maschinen verursacht werden, und Geräte können in Botnets abgefangen oder so manipuliert werden, dass sie andere Geräte angreifen.

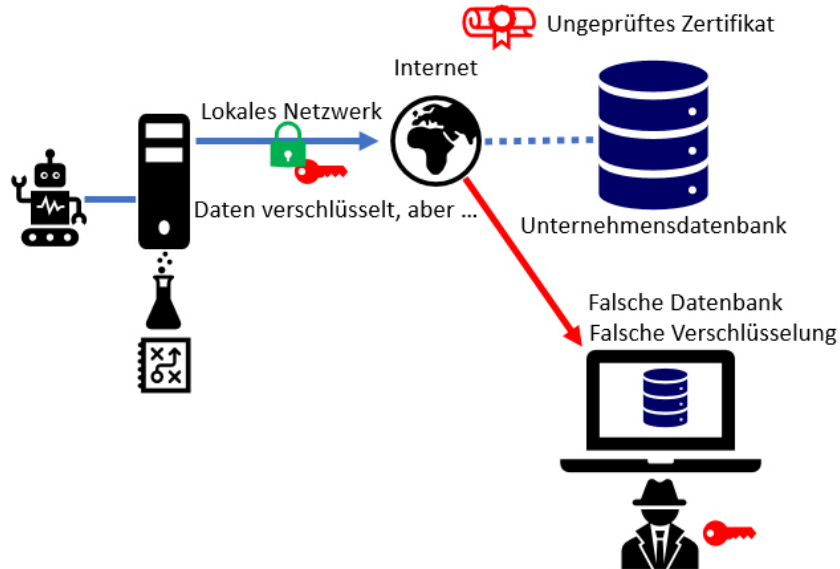


Gegenmaßnahmen:

Stellen Sie sicher, dass fremde Computer keinen Zugriff bzw. keine Kontrolle erhalten.

- Identitätsdiebstahl

Verbindungen zu Webseiten, die nicht von einer Zertifizierungsstelle überprüft werden, können gefährlich sein, da sie Identitätsdiebstahl und die Umleitung der Kommunikation erleichtern. Dies gibt Angreifern die Möglichkeit, sensible Informationen (z. B. Benutzernamen, Kennwörter, Prozessdaten oder Rezepturen) zu erlangen und durch die Manipulation von Maschinen Schaden anzurichten.



Gegenmaßnahmen:

Stellen Sie sicher, dass Sie Zertifikate verwenden, um die Identität des Zielservers zu authentifizieren.

5 Allgemeine Sicherheitsvorkehrungen

Die Implementierung von Maßnahmen zum Schutz Ihres Netzwerks ist entscheidend, damit Ihr Netzwerk und der zugehörige Datenverkehr sicher sind.

Da Sie dieses Produkt in einem Netzwerk verwenden, wird auf folgende Sicherheitsrisiken hingewiesen:

- Datenlecks oder Datendiebstahl mithilfe dieses Produkts
- Verwendung dieses Produkts für illegale Aktivitäten durch Personen mit böswilligen Absichten
- Störung oder Abschaltung dieses Moduls durch Personen mit böswilligen Absichten
- Es liegt in Ihrer Verantwortung, Sicherheitsvorkehrungen, beispielsweise die im Folgenden beschriebenen Maßnahmen, zu ergreifen, um sich vor den oben genannten Netzwerksicherheitsrisiken zu schützen.
- Wenn dieses Produkt zusammen mit PCs in einem Netzwerk verwendet wird, sorgen Sie dafür, dass das System nicht mit Computerviren oder anderen böswilligen Entitäten infiziert ist (durch Verwendung eines regelmäßig aktualisierten Antivirenprogramms, Anti-Spyware-Programms usw.).
- Verwenden Sie dieses Produkt in einer Umgebung, die über ein LAN, ein VPN (virtuelles privates Netzwerk) oder ein Standleitungsnetzwerk verfügt.
- Verwenden Sie dieses Produkt in einer Umgebung, in der nur Personen mit kontrollierten Zugriffsrechten Zugang haben.
- Verwenden Sie dieses Produkt und andere über ein Netzwerk angeschlossene Ge-

räte wie PCs und Tablets nur, wenn Sie Schutzmaßnahmen getroffen haben, um die Sicherheit zu gewährleisten.

- Installieren Sie dieses Produkt nicht an Orten, an denen das Produkt oder die Kabel von Personen mit böswilligen Absichten zerstört oder beschädigt werden können.

Beachten Sie, dass eine falsche Anschlusseinstellung zum bestehenden LAN zu Fehlfunktionen bei den Geräten im Netzwerk führen kann. Wenden Sie sich vor dem Anschluss an Ihren Netzwerkadministrator.

6 Bewährte Verfahren zur Absicherung Ihres FP-I4C-Moduls

Sie können Sicherheitsrisiken minimieren, indem Sie vorbeugende Maßnahmen ergreifen und die richtigen System- und Anwendungseinstellungen vornehmen. Verwenden Sie die in diesem Leitfaden enthaltene Checkliste, um sicherzustellen, dass Sie alle erforderlichen Maßnahmen zur Absicherung des FP-I4C-Moduls ergreifen.

Verwandte Themen:

[Checkliste für die Sicherheitskonfiguration](#)

6.1 Systemeinstellungen

Wechseln Sie zu "System Settings" (IP/machine_config), um Passwort- und Firewall-Einstellungen vorzunehmen, auf Protokolldateien zuzugreifen und die SSH-Debugging-Funktionen zu nutzen.

6.1.1 Passwortschutz

Das werkseitig voreingestellte Passwort wird für die ersten Schritte verwendet. Legen Sie ein sicheres Passwort fest, das Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (außer Leerzeichen) enthält.

Verwenden Sie unterschiedliche FTP-Server-Passwörter für HMWIN Studio und für das FP-I4C-Modul.

6.1.2 Firewall-Einstellungen

Verwenden Sie die Firewall (IP/machine_config/#/services), um alle nicht verwendeten Ports zu schließen.

Wenn Sie den "Firewall Service" (IP/machine_config/#/services) aktivieren, werden alle verwendeten Funktionen mit den angegebenen Einstellungen und Ports aktiviert. Deaktivieren Sie ungenutzte Dienste und Ports oder verweigern Sie den Zugriff auf dedizierte Schnittstellen (ETH0 oder ETH1).

Hinweis:

Vergewissern Sie sich, dass "Web server - HTTP" und "Web server - HTTPS" aktiviert sind und die Ethernet-Ports 80 und 443 geöffnet sind. Andernfalls wird der Zugriff auf die Systemeinstellungsseite dauerhaft verweigert.

Beispiel für die Firewall-Einstellungen:

Name	Quell-Schnittstelle	Port oder Bereich	Protokoll	Erforderlich
Webserver - HTTP (für die Konfiguration erforderlich)	Beliebige	80	TCP	✓
Webserver - HTTPS (für die Konfiguration erforderlich)	Beliebige TCP	443	TCP	✓
Geräteerkennung	Beliebige	990–991	UDP	✓
FTP-Befehls-Port, erforderlich für HMWIN Studio-Betrieb	Beliebige	21	TCP	
Passiver FTP-Modus, erforderlich für HMWIN Studio-Betrieb	Beliebige	18756–18760	TCP	
SSH-Server	Beliebige	22	TCP	
VNC-Server	Beliebige	5900	TCP	
DHCP-Server	Beliebige	67	UDP	
SNMP-Server	Beliebige	161	UDP	
PEW-Schnittstellen	Beliebige	9094–9097	TCP	

6.1.3 Protokolldateien und SSH-Debugging-Funktionen

Diese Funktionen können verwendet werden, um eine untypische Nutzung zu erkennen. Sie können nur mit Administratorrechten verwendet werden.

6.2 Anwendungseinstellungen

Wechseln Sie zu "Application Settings" (IP/fp_config), um anwendungsspezifische Sicherheitseinstellungen auf der entsprechenden Konfigurationsseite vorzunehmen.

- Port-Konfiguration

Sie können TCP-Listening-Ports auf der Seite "Port" der FP-I4C-Web-Schnittstelle konfigurieren. Da die meisten industriellen Kommunikationsprotokolle keinen Zugriffsschutz bieten, verwenden Sie diese Ports nur für die interne Kommunikation innerhalb eines gekapselten Netzwerks.

Ergreifen Sie die folgenden zusätzlichen Maßnahmen, um das Risiko zu minimieren, dass ein Angreifer unbefugte Kontrolle über die angeschlossene SPS erlangt:

- Entfernen Sie alle ungenutzten Port-Einstellungen.
- Erlauben Sie, wenn möglich, nur Lesezugriff auf Ihre Daten.
- Blockieren Sie die Datenübertragung für alle ausschließlich intern genutzten SPS-Daten.
- Minimieren Sie insbesondere die Anzahl der Kontrollregister (z. B. Sollwerte oder Befehle), die für Schreibvorgänge benötigt werden.
- Definieren Sie IP-Adressen, die zur Kommunikation zugelassen sind. Weisen Sie für die geräteinterne Kommunikation (z. B. Zugriff über eine Webseite) die IP-Adresse 127.0.0.1 (localhost) zu.
- Jede angeschlossene SPS sollte über einen eigenen Zugriffsschutz verfügen, da-

mit das laufende SPS-Programm nicht verändert werden kann.

- **Datenlogger-Dienst**

Der Datenlogger öffnet keine Listening-Ports. Stattdessen werden die Daten über RS232-, RS485-, USB- und Ethernet-TCP-Client-Verbindungen erfasst. Keines der unterstützten Protokolle verwendet Verschlüsselung.

Wenn Sie Daten über öffentliche Netzwerke erfassen, sollten Sie eine VPN-Lösung verwenden.

- **MQTT-Dienst**

Das IoT-Protokoll (Internet of Things) unterstützt einfache (unverschlüsselte) und verschlüsselte Kommunikation sowie zusätzliche Zugriffskontrolle.

- Verwenden Sie bei der Übertragung von Daten über öffentliche Netze Root-Zertifikate, um die Identität des Brokers/Servers zu überprüfen.
- Verwenden Sie verschlüsselte Verbindungen zwischen dem FP-I4C-Modul und dem Broker.

Sensible Daten werden innerhalb des Brokers nicht verschlüsselt und können über einfache (unverschlüsselte) Verbindungen weitergeleitet werden. Der Broker muss durch eine rollenbasierte Zugriffskontrolle vor unberechtigtem Zugriff geschützt sein.

- **FTP-Client-Dienst**

Die FTP-Client-Funktion stellt Verbindungen zu FTP-Servern für Dateiübertragungen her. Benutzeranmeldungen werden bei Standard-FTP-Übertragungen nicht verschlüsselt. Wir empfehlen Ihnen, nur sichere FTPS-Übertragungen zu verwenden. Verwenden Sie bei der Übertragung von Daten über öffentliche Netzwerke zusätzlich Root-Zertifikate.

Wenn der FTP-Server die verschlüsselte Verbindung ablehnt, schlägt der Handshake fehl und die Übertragung wird beendet.

- **Skript-Dienst**

Bei der implementierten Skriptfunktion handelt es sich um einen sehr kleinen, gekapselten Interpreter mit begrenzten Funktionen, mit dem Geräteinformationen für eine angeschlossene SPS bereitgestellt werden.

- Für eine Skriptänderung sind Administratorrechte erforderlich.
- Es wurde keine Skriptfunktion zum Öffnen von Listening-Ports implementiert.
- Es wurde nur eine Funktion für die Datenübertragung als TCP-Client implementiert.

- **SQL-Client-Dienst**

Die SQL-Client-Funktion ermöglicht es, mit Datenbanken zu kommunizieren. Normalerweise verwenden Datenbanken ihre eigene verschlüsselte Authentifizierung. Da Datenbanken sensible Daten enthalten können, sollten Sie Ihre Datenbankinfrastruktur unbedingt absichern.

Verwenden Sie den SQL-Client nur für die Verbindung zu nicht sensiblen Teilen der Datenbankinfrastruktur.

- **IEC60870-Dienst**

Das IEC60870-Fernwirkprotokoll verwendet einen Listening-Port ohne Benutzer-Zugriffsschutz. Achten Sie darauf, dieses Protokoll nur in gekapselten Netzwerken zu verwenden.

Die Möglichkeit, die angeschlossene SPS, Maschine oder Unterstation zu steuern, stellt ein zusätzliches Risiko dar. Um dieses Risiko zu minimieren, empfehlen wir die folgenden Maßnahmen:

- Legen Sie die zulässigen Partner-IP-Adressen fest.
- Verwenden Sie verschlüsselte VPN-Tunnel.
- Alle Sollwerte und Befehle werden in der SPS verwaltet. Eingehende Telegramme werden zuerst im FP-I4C-Modul und dann in der SPS verarbeitet. Implementieren Sie ein SPS-Verfahren zur Identifizierung unzulässiger Befehle.
- Verwenden Sie Zeitstempeldaten bei allen Befehlen in Steuerungsrichtung.
- Alle angeschlossenen SPS sollten über einen eigenen Zugriffsschutz verfügen, damit das laufende SPS-Programm nicht verändert werden kann.
- HTTP-Client-Dienst

Der HTTP-Client funktioniert wie ein Browser, um Informationen von einem HTTP-Server (Cloud-Server) abzurufen oder an diesen zu senden.

 - Achten Sie bei der Datenübertragung über öffentliche Netzwerke darauf, dass Sie Root-Zertifikate verwenden, um sicherzustellen, dass das FP-I4C-Modul mit dem richtigen HTTP-Server verbunden ist.
 - Verwenden Sie verschlüsselte Verbindungen zwischen dem FP-I4C-Modul und dem HTTP-Server.
- E-Mail-Client-Dienst

Der E-Mail-Client kommuniziert mit einem E-Mail-Server. Dieser Server sollte für eine sichere und verschlüsselte Kommunikation vorbereitet sein, und es sollten Benutzerzugriffsrechte festgelegt werden. Der E-Mail-Client kann Nachrichten mit oder ohne Anhänge übertragen, jedoch keine ausführbaren Dateien.

 - Wenn Sie Daten über öffentliche Netzwerke übertragen, sollten Sie mit Hilfe von Root-Zertifikaten sicherstellen, dass das FP-I4C-Modul mit dem richtigen E-Mail-Server verbunden ist.
 - Verwenden Sie für das Anmeldeverfahren verschlüsselte Verbindungen zwischen dem FP-I4C-Modul und dem E-Mail-Server.
- REST-API-Dienst

Die REST-API arbeitet als HTTP-Server, um Informationen über die angeschlossene SPS bereitzustellen und die SPS zu steuern.

Um Sicherheitsrisiken zu minimieren, nehmen Sie die folgenden Einstellungen auf der Seite "Port" vor:

 - Erlauben Sie, wenn möglich, nur Lesezugriff auf Ihre Daten.
 - Blockieren Sie die Datenübertragung für alle ausschließlich intern genutzten SPS-Daten.
 - Minimieren Sie insbesondere die Anzahl der Kontrollregister (z. B. Sollwerte oder Befehle), die für Schreibvorgänge benötigt werden.
 - Legen Sie IP-Adressen fest, die zur Kommunikation zugelassen sind.
 - Verwenden Sie verschlüsselte Verbindungen zwischen dem FP-I4C-Modul (als HTTPS-Server) und dem Client.

7 FAQ

1. Kann ich Software-Patches und Firmware-Updates erhalten?
Kostenlose Downloads der neuesten Versionen sind auf der Panasonic-Website verfügbar:
[Downloads | Panasonic Industry Europe GmbH](#)
2. Ist eine Hintertür auf dem Modul installiert?
Es ist keine Hintertür auf dem Modul installiert. Wenn Sie Ihr Passwort verlieren, gibt es keine Möglichkeit, um Ihre Einstellungen wiederherzustellen.
3. Ruft das Modul Panasonic-Server auf?
Mit den Werkseinstellungen gibt es keinen Prozess, um automatisch einen Panasonic-Server aufzurufen.

8 Checkliste für die Sicherheitskonfiguration

Verwenden Sie diese Checkliste, um sicherzustellen, dass Sie alle erforderlichen Maßnahmen zur Absicherung des FP-I4C-Moduls ergriffen haben. Haken Sie alle Punkte ab, die Sie erledigt haben. Am Ende der Liste ist Platz für zusätzliche Punkte.

Erledigt	Risiko ¹⁾	Bereich	Konfigurationsseite	Zu erledigen
	Hoch	Passwörter (admin, user)	IP/machine_config/##/authentication	Standard-Administrator- und Benutzerpasswörter ändern
	Hoch	Dienst: Autorun-Skripte	IP/machine_config/##/services	Deaktivieren
	Hoch	Dienst: SSH-Server	IP/machine_config/##/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Avahi-Dämon	IP/machine_config/##/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Cloud-Dienst	IP/machine_config/##/services	Deaktivieren, wenn nicht benötigt
	Niedrig	DHCP-Server	IP/machine_config/##/services	Deaktivieren, wenn nicht benötigt
	Niedrig	VNC-Dienst	IP/machine_config/##/services	Deaktivieren, wenn nicht benötigt
	Niedrig	Firewall	IP/machine_config/##/services	Aktivieren und Einstellungen anpassen
	Hoch	HMWIN-Passwörter (mindestens admin, user, log) ²⁾	HMWIN Studio Project/Configuration/Security	Standard-Administrator- und Benutzerpasswörter ändern
	Mittel	HMWIN OPC UA-Funktion ²⁾	HMWIN Studio Project/Configuration/Security	Serverzugriff prüfen
	Hoch	Port-Konfiguration	IP/fp_config → "Port"	Datenbereichszugriff konfigurieren (lesen, schreiben oder unterbrechen)
	Mittel	MQTT-Dienst	IP/fp_config → "MQTT"	Verschlüsselung und Zertifikate verwenden
	Mittel	FTP-Client-Dienst	IP/fp_config → "FTP-Client"	Verschlüsselung und Zertifikate verwenden
	Mittel	HTTP-Client-Dienst	IP/fp_config → "HTTP-Client"	Verschlüsselung und Zertifikate verwenden
	Mittel	E-Mail-Client-Dienst	IP/fp_config → "Email-Client"	Verschlüsselung, Zertifikate und Passwörter verwenden
	Mittel	REST-API-Dienst	IP/fp_config → "REST API"	"Externe Anfragen erlauben" deaktivieren, wenn nicht benötigt
			IP/fp_config → "Port"	Datenbereichszugriff konfigurieren (lesen oder schreiben)

¹⁾ Das Risikoniveau hängt von Ihrer Anwendung ab.

²⁾ Wenn installiert

Panasonic Hotline

Sollten Sie Fragen haben, die sich nicht über die Informationen in den Handbüchern oder in der Online-Hilfe klären lassen, wenden Sie sich bitte an Ihren Distributor.

Europa

Österreich: 02236 / 2 68 46, info.pewat@eu.panasonic.com

Benelux: 0499 / 37 27 27, info.pewswe@eu.panasonic.com

Frankreich: 01 / 60 13 57 57, info.pewswef@eu.panasonic.com

Deutschland: 089 / 45 354 2748, plc.peweu@eu.panasonic.com

Irland: 01 / 4 60 09 69, info.pewuk@eu.panasonic.com

Italien: 045 / 67 52 711, info.pewit@eu.panasonic.com

Skandinavien: 46 / 8 59 47 66 80, info.pewns@eu.panasonic.com

Spanien: 91 / 3 29 38 75, info.pewes@eu.panasonic.com

Schweiz: 041 / 799 70 50, info.pewch@eu.panasonic.com

Großbritannien: 01908 / 23 15 55, info.pewuk@eu.panasonic.com

Nord- & Südamerika

USA: 1 877 / 624 7872, iasupport@us.panasonic.com

Asien

China: 400-920-9200, <https://industrial.panasonic.cn/ea/>

Korea: +82-2-2052-1050, <http://pidskr.panasonic.co.kr/>

Taiwan: +886-2-2757-1900, <https://industrial.panasonic.com/>

Hong Kong: +852-2306-3128, <https://industrial.panasonic.com/>

Japan: 0120-394-205, <https://industrial.panasonic.com/>

Singapur: +65 / 635 92128, pewapfa@sg.pewg.panasonic.com

Änderungsverzeichnis

Datum	Beschreibung
2021.11, Version 1.1	Erste deutsche Ausgabe