

PROGRAMMABLE CONTROLLER

Security Guide



FP-I4C Unit

Copyright and liability

Copyright and liability information relating to this documentation.

Copyright © 2024 Panasonic Industry Europe GmbH

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Germany

Last modified on: 2024-07-23

This documentation and everything described in it are copyrighted. You may not copy this documentation, in whole or part, without written consent of Panasonic Industry Europe GmbH.

Panasonic Industry Europe pursues a policy of continuous improvement of the design and performance of its products. Therefore we reserve the right to change the documentation/product without notice. In no event will Panasonic Industry Europe be liable for direct, special, incidental, or consequential damage resulting from any defect in the product or its documentation, even if advised of the possibility of such damages.

For technical support, please contact the [Panasonic hotline](#).

Table of contents

1 About this document.....	4
2 Panasonic product security policy.....	5
3 Default configuration of the FP-I4C unit.....	6
4 Potential threat scenarios.....	8
5 General security measures.....	10
6 Best practices to harden your FP-I4C unit.....	11
6.1 System settings.....	11
6.1.1 Password protection.....	11
6.1.2 Firewall settings.....	11
6.1.3 Log files and SSH debugging features.....	12
6.2 Application settings.....	12
7 FAQ.....	16
8 Security configuration checklist.....	17
9 Panasonic hotline.....	19
10 Record of changes.....	21

1 About this document

Internal and external cybersecurity risks continue to evolve with growing digitalization and the increasing interconnectivity of networks.

The BSI (German Federal Office for Information Security), for example, published a report with the top ten threats and defined rules and recommendations for network products in industrial control systems (ICS):


- Infiltration of malware via removable media and external hardware
- Malware infection via Internet and Intranet
- Human error and sabotage
- Compromising of extranet and Cloud components
- Social engineering and phishing
- (D)Dos attacks
- Control components connected to the Internet
- Intrusion via remote access
- Technical malfunctions and force majeure
- Compromising of smartphones in the production environment

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

This document contains the device information needed for your network management and will help you to protect the FP-I4C unit against security risks.

2 Panasonic product security policy

Panasonic products and services are continually being improved. Our product development strictly follows security rules and performs extensive testing prior to shipment. The Panasonic security policy is based on the international guidelines set out in IEC 62443 and ISO/IEC 27001.

The [Panasonic Product Security Incident Response Team](#)  (Panasonic PSIRT) is the coordination center for vulnerabilities related to Panasonic products.

3 Default configuration of the FP-I4C unit

The built-in network capabilities of the FP-I4C unit pose a potential security risk. Be sure to customize the default settings to eliminate or minimize this risk.

- From production in May 2024 there will be no default password set and the first time you connect to the device you will need to set a password with a minimum of predefined rules. Earlier versions have a factory default password and we recommend that you change the default password as soon as possible.
- The two Ethernet ports ETH0 and ETH1 have different configurations: ETH0 is configured as a DHCP client and ETH1 is configured with the fixed IP address 192.168.0.1.
- By default, the following ports are open and in listening mode:

Port No.	Protocol	Function
80, 8081, 443	TCP	Used for browser configuration and user Web pages
53	TCP	Used for DNS service
990-991	UDP	Used for broadcast device discovery
21 (BSP 1.0 before 05/2024)	TCP	FTP data ports (FTP passive mode: 16384-17407/TCP)
18756-18759	TCP	FTP data ports, secured
990 (from BSP 1.3 05/2024)	TCP	Runtime and project management

- All features and services of the FP-I4C unit that could present a vulnerability risk have been disabled at the factory. The services are listed under IP/machine_config/#!/services.

Service	Security risk
Autorun scripts	Applications started from an external storage device, e.g. a USB flash drive
Avahi daemon	Opens port 5353 (used for gathering information and finding features)
Cloud service	E.g., an OpenVPN server configuration from previous usage
DHCP server	Opens ports 67, 68
SNMP server	Opens port 161, 10161 (used for gathering information)
SSH server	Opens port 22 (login with administrator credentials and execution of commands)
VNC server	Opens port 5900 (Web page and device control)

- By default, the firewall implemented in the FP-I4C unit (IP/machine_config/#!/services) is disabled.
- The FP-I4C unit writes log data and untypical usage information into log files. These files are stored in the unit and can be downloaded with administrator credentials.

Note

Use the firewall to close any unused ports, but be sure to open and enter Ethernet port 443 in the firewall configuration (for BSP 1.0, you must also open port 80). Otherwise, access to the system settings page will permanently be denied.

Related topics

[Firewall settings](#) (page 11)

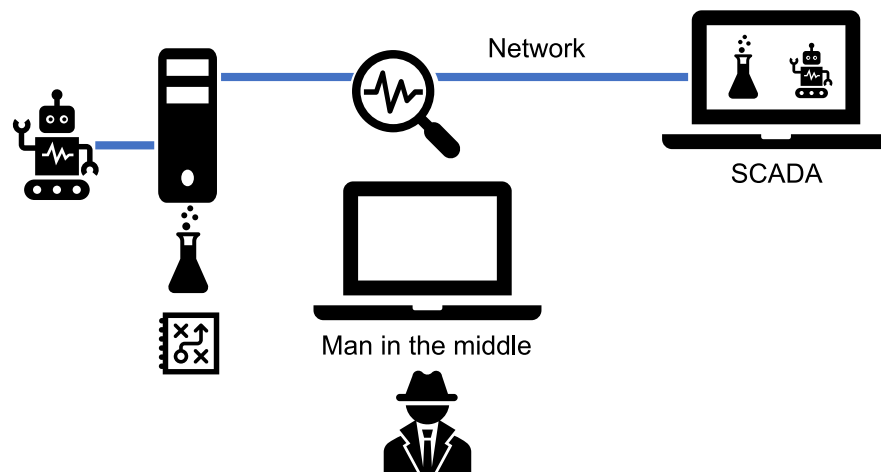
4 Potential threat scenarios

To increase your awareness and understanding, we give you some typical examples of potential cyber threats.

- Capturing data

A lot of tools are available to read the network traffic, including user names, passwords, and other sensitive data such as recipes or process data.

Especially if your network traffic is not encrypted, it is an easy target for a spy searching for readable information.

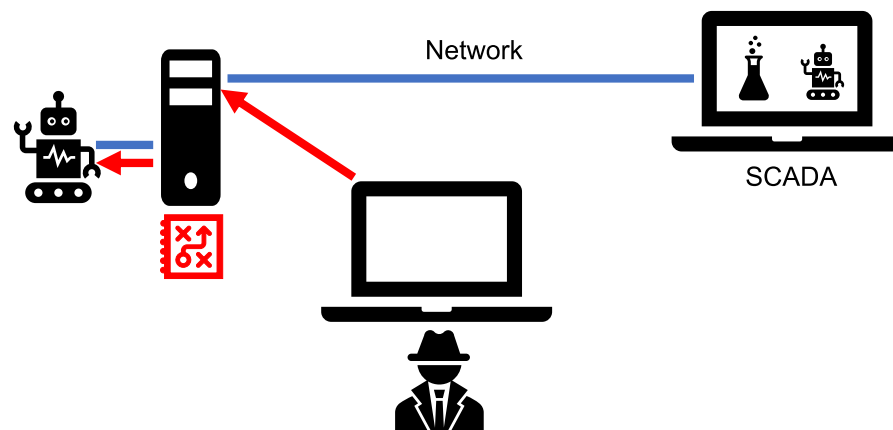


Countermeasures:

Do not use the FTP or Telnet protocols outside an encapsulated network to transmit sensitive data. These protocols create a high security risk because user names and passwords are transmitted in plain text.

- Gaining access to control systems

With the knowledge of credentials or the protocol used, it may become possible to cause failure or damage to machines, and devices can be hijacked into botnets or manipulated to attack other devices.

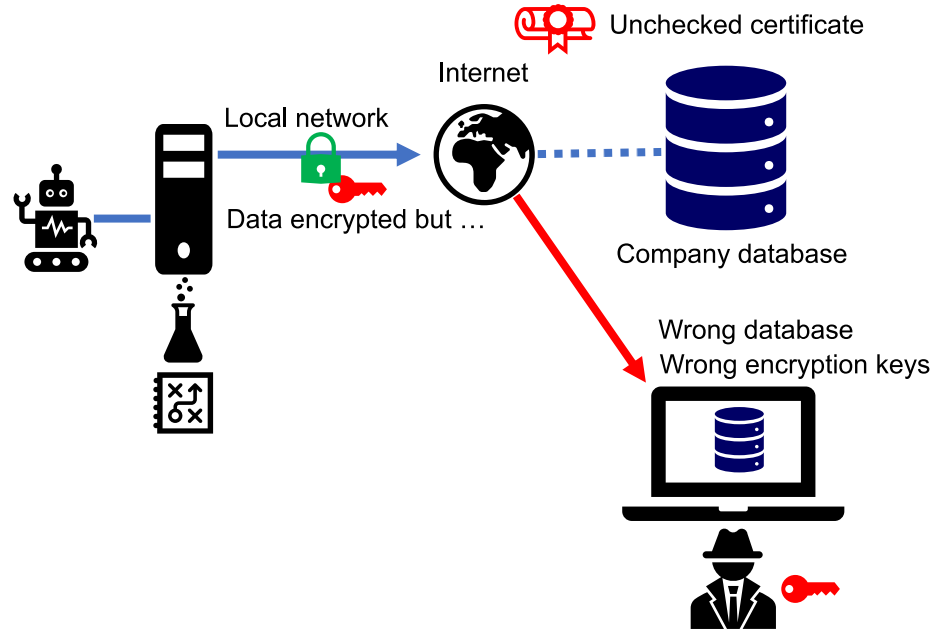


Countermeasures:

Be sure not to allow access or control from third party computers.

- Hijacking the identity

Connections to Web pages that are not verified by a certificate authority can be dangerous because they facilitate identity fraud and the redirection of the communication. This gives attackers the chance to collect sensitive information (e.g. user names, passwords, process data, or recipes) and to cause damage by manipulating machines.



Countermeasures:

Be sure to use certificates to authenticate the identity of the target server.


5 General security measures

Implementing measures to protect your network is crucial to keep your network and its traffic secured.

As you will use this product connected to a network, your attention is called to the following security risks.

- Leakage or theft of information through this product
- Use of this product for illegal operations by persons with malicious intent
- Interference with or stoppage of this product by persons with malicious intent
- It is your responsibility to take precautions such as those described below to protect yourself against the above network security risks.
- If this product is connected to a network that includes PCs, make sure that the system is not infected by computer viruses or other malicious entities (using a regularly updated antivirus program, anti-spyware program, etc.).
- Use this product in an environment that has LAN, VPN (virtual private network), or leased line network.
- Use this product in an environment where only people with controlled access rights can enter.
- Use this product and other devices connected via network such as a PC and tablet only if you have taken protective measures to ensure safety.
- Do not install this product in locations where the product or the cables can be destroyed or damaged by persons with malicious intent.

Note that incorrect setting of the connection to the existing LAN might cause malfunction in the devices on the network. Consult your network administrator before connecting.

There is some very helpful information on the Internet: [MITRE ATT&CK®](#)  is a curated knowledge base and model of cyber adversary behavior.

6 Best practices to harden your FP-I4C unit

You can minimize security risks by taking preventive measures and making the proper system and application settings. Use the checklist provided in this guide to ensure that you take all necessary measures to secure the FP-I4C unit.

Related topics

[Security configuration checklist](#) (page 17)

6.1 System settings

Go to “System Settings” (IP/machine_config) to make password and firewall settings, to access log files, and to use the SSH debugging features.

6.1.1 Password protection

Set a strong password that uses upper- and lowercase letters, numbers, and special characters (except blank spaces).

Use different FTP server passwords for HMWIN Studio and for the FP-I4C unit.

6.1.2 Firewall settings

Use the firewall (IP/machine_config/#/services) to close any unused ports.

When you enable the “Firewall Service” (IP/machine_config/#/services), all features used are enabled with the specified settings and ports. Disable any unused services and ports or deny access to dedicated interfaces (ETH0 or ETH1).

Note

Make sure that “Web Server – HTTP” and “Web Server – HTTPS” are enabled and Ethernet port 443 is open (also port 80 for BSP 1.0). Otherwise, access to the system settings page will permanently be denied.

Example of firewall settings:

Name	Source interface	Port or range	Protocol	Required
Web server - HTTP (needed for configuration)	Any	80	TCP	✓ (BSP 1.0)
Web server - HTTPS (needed for configuration)	Any	443	TCP	✓
Device discovery	Any	990–991	UDP	✓
FTP command port, needed for HMWIN Studio operations	Any	21	TCP	✓ (BSP 1.0)
FTP passive mode, needed for HMWIN Studio operations	Any	18756–18759	TCP	
SSH server	Any	22	TCP	
VNC server	Any	5900	TCP	
DHCP server	Any	67	UDP	
SNMP server	Any	161	UDP	
PLC connection ports	Any	9094–9097	TCP	
HMWIN Studio operations	Any	990	TCP	

6.1.3 Log files and SSH debugging features

These features can be used to detect untypical usage. They can be used with administrator credentials only.

6.2 Application settings

Go to “Application Settings” (IP/fp_config) to make application-specific security settings on the corresponding configuration page.

- Port configuration

You can configure TCP listen ports on the “Port” page of the FP-I4C Web interface. Because most industrial communication protocols do not provide access protection, use these ports only for internal communication within an encapsulated network.

Take the following additional measures to minimize the risk that an attacker gains unauthorized control of the connected PLC:

- Remove all unused port settings.
- Whenever possible, permit read access only to your data.
- Block data transmission for all PLC data that is only used internally.

- Minimize especially the number of control registers (such as set points or commands) needed for write operations.
- Define IP addresses that are allowed to communicate. For device internal communication (e.g. access via Web page), assign the IP address 127.0.0.1 (local host).
- Any connected PLC should have its own access protection so that the running PLC program cannot be modified.

- Data logger service

The data logger does not open any listen ports. Instead, data is collected through RS232, RS485, USB, and Ethernet TCP client connections. None of the supported protocols uses encryption.

When collecting data via public networks, be sure to use a VPN solution.

- MQTT service

The IoT (Internet of Things) protocol supports plain and encrypted communication as well as additional access control.

- When transmitting data via public networks, use root certificates to verify the identity of the broker/server.
- Use encrypted connections between the FP-I4C unit and the broker.

Sensitive data are not encrypted within the broker and can be forwarded via plain connections. The broker must be protected against unauthorized access by role-based access control.

- FTP client service

The FTP client feature establishes connections to FTP servers for file transmission. User logins are not encrypted with standard FTP transmissions. We recommend that you use secure FTPS transmissions only. When transmitting data through public networks, additionally use root certificates.

If the FTP server rejects the encrypted connection, the handshake fails and transmission is terminated.

- Script service

The implemented script feature is a very small encapsulated interpreter with limited features, created to provide device information to a connected PLC.

- Script modification requires admin credentials.
- No script function has been implemented to open listen ports.
- Only one function has been implemented for data transmission as a TCP client.

- SQL client service

The SQL client feature makes it possible to communicate with databases. Typically, databases use their own encrypted authentication. Because databases may contain sensitive data, be sure to secure your database infrastructure.

Use the SQL client only to connect to non-sensitive parts of the database infrastructure.

- IEC60870 service

The IEC60870 telecontrol protocol uses a listen port without any user access protection. Be sure to use this protocol in encapsulated networks only.

The possibility to control the connected PLC, machine, or substation poses an additional risk. To minimize this risk, we recommend the following measures:

- Specify the allowed partner IP addresses.
- Use encrypted VPN tunnels.
- All set points and commands are handled in the PLC. Incoming telegrams are first processed in the FP-I4C unit and then in the PLC. Implement a PLC procedure to identify illegitimate commands.
- Use time stamp data with all commands in control direction.
- All connected PLC should have their own access protection so that the running PLC program cannot be modified.

- HTTP client service

The HTTP client operates like a browser to get or post information to a HTTP server (cloud server).

- When transmitting data via public networks, be sure to use root certificates to verify that the FP-I4C unit is connected to the correct HTTP server.
- Use encrypted connections between the FP-I4C unit and the HTTP server.

- Email client service

The email client communicates with an email server. This server should be prepared for secure and encrypted communication, and user access rights should be defined. The email client can transmit messages with or without attachments but no executable files.

- When transmitting data via public networks, be sure to use root certificates to verify that the FP-I4C unit is connected to the correct email server.
- Use encrypted connections between the FP-I4C unit and the email server for the login procedure.

- REST API service

The REST API operates as an HTTP server to provide information about the connected PLC and to control the PLC.

To minimize security risks, make the following settings on the “Port” page:

- Whenever possible, permit read access only to your data.
- Block data transmission for all PLC data that is only used internally.
- Minimize especially the number of control registers (such as set points or commands) needed for write operations.
- Define IP addresses that are allowed to communicate.
- Use encrypted connections between the FP-I4C unit (as HTTPS server) and the client.

- TLS client/server service




For insecure protocols such as MEWTOCOL, Modbus or IEC60870, this service can be used to create TLS tunnels.

- The feature works as both an inbound and an outbound service, depending on which option (client or server) is used.

Insecure inbound connections should only be used in a limited small network segment, such as a connection to a single PLC, while TLS-based inbound connections should be specified for the external WAN network connection.

- Use server and client certificates.

7 FAQ

1. Can I get software patches and firmware updates?
Free downloads of the newest releases are available on the Panasonic Web site:
[Panasonic Download Center](#)  or the [InfoHub](#) 
2. Is there any backdoor installed on the device?
There is no backdoor installed on the device. If you lose your password, there is no way your settings can be restored.
3. Does the device call any Panasonic servers?
With the factory settings, there is no process to automatically call a Panasonic server.
4. Where do I report a new vulnerability?
Please contact the [Panasonic Product Security Incident Response Team](#)  (Panasonic PSIRT), which is the coordination center for vulnerabilities related to Panasonic products.

8 Security configuration checklist

Use this checklist to ensure that you take all necessary measures to secure the FP-I4C unit. Check off all items you have completed. At the end of the list, there is room for additional items.

Checked	Risk ¹⁾	Area	Configuration page	To do
	High	Passwords (admin, user)	IP/machine_config/##/authentication	Change to secure admin and user passwords
	High	Service: Autorun scripts	IP/machine_config/##/services	Disable
	High	Service: SSH server	IP/machine_config/##/services	Disable if not needed
	Low	Avahi daemon	IP/machine_config/##/services	Disable if not needed
	Low	Cloud service	IP/machine_config/##/services	Disable if not needed
	Low	DHCP server	IP/machine_config/##/services	Disable if not needed
	Low	VNC service	IP/machine_config/##/services	Disable if not needed
	Low	Firewall	IP/machine_config/##/services	Enable and customize the settings
	High	HMWIN passwords (at least admin, user, log) ²⁾	HMWIN Studio Project/Configuration/Security	Change default admin and user passwords
	Medium	HMWIN OPC UA feature ²⁾	HMWIN Studio Project/Configuration/Security	Check server access
	High	Port configuration	IP/fp_config → "Port"	Configure data area access (read, write, or block) and specify permitted IP addresses
	Medium	MQTT service	IP/fp_config → "MQTT"	Use encryption and certificates
	Medium	FTP client service	IP/fp_config → "FTP Client"	Use encryption and certificates
	Medium	HTTP client service	IP/fp_config → "HTTP Client"	Use encryption and certificates
	Medium	Email client service	IP/fp_config → "Email Client"	Use encryption and certificates, and passwords
	Medium	REST API service	IP/fp_config → "REST API"	Specify permitted IP addresses
			IP/fp_config → "Port"	Configure data area access (read or write)
	High	TLS client/server service	IP/fp_config → "TLS Client/Server"	Use ETH0 and ETH1 to split the networks

Checked	Risk ¹⁾	Area	Configuration page	To do
	Low	Backup/restore service	IP/fp_config → “Backup/Restore”	Use password protection for your backup files
	Medium	IEC60870 service	IP/fp_config → “IEC60870”	Specify permitted IP addresses under “IP lock mode”

- 1) The risk level depends on your application.
- 2) If installed.


9 Panasonic hotline

If you have questions that cannot be clarified by the manuals or online help, please contact one of our sales offices.

You can help us by having the following data at hand:

- Your product's serial number and/or version number.
- The version and service pack numbers of MS-Windows installed on your computer.
- The type of hardware you are using.
- The exact wording of any message that appears on your screen.
- What happened and what did you do when the problem occurred?
- How did you attempt to solve the problem?

Dial a hotline number, or use our [contact form](#)  to send us your request.

For inquiries outside of Europe, please visit our [global Web site](#) .

Panasonic Industry Europe GmbH

- Germany and European countries not listed on this page:
 - +49 89 45354-2748 (PLC, FP-I4C, touch panels)
 - +49 89 45354-2737 (sensors)
 - +49 89 45354-2750 (servo drives)
- France:
 - +33 160 135757

Panasonic Industry Austria GmbH

Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Montenegro, Serbia, Slovenia, Switzerland:

+43 2236 26846

Panasonic Industry Benelux B.V.

Belgium, Denmark, Luxembourg, Norway, Sweden, The Netherlands:

+31 499 372727

Panasonic Industry Italia srl

Italy:

+39 045 6752711, support.piit@eu.panasonic.com

Panasonic Industry Poland sp. z o.o.

Baltic states, Czech Republic, Finland, Hungary, Poland, Romania, Slovakia:

+48 42 2309633

Panasonic Industry Iberia S.A.

Portugal, Spain:

+34 91 3293875

Panasonic Industry UK Ltd.

United Kingdom of Great Britain and Ireland:

+44 1908 231555

10 Record of changes

Security Guide Version 1.3, 2024.07

Updated for the new and more secure release of BSP 1.3

Security Guide Version 1.2, 2023.02

Updated company name, updated the section “Panasonic hotline”

Security Guide Version 1.1, 2021.11

Added section 2, changed wording for read access data in section 6.2

Security Guide Version 1.0, 2021.08

First edition