Panasonic
INDUSTRY

TOUCH TERMINALS

Security Guide

HM series

Version 1.0

2024.07

https://industry.panasonic.eu/

Copyright and liability

2

Copyright and liability information relating to this documentation.

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Germany

Last modified on: 2024-07-23

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

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 HM series touch terminal 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 HM series touch terminal

The built-in network capabilities of the HM series touch terminal 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 Ethernet ports are configured as a DHCP client.
- By default, the following ports are open and in listening mode:

Port No.	Protocol	Function
80, 8000, 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 except the feature Autorun scripts of the HM series touch terminal 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 HM series touch terminal (IP/machine_config/#/services) is disabled.
- The HM series touch terminal writes log data and untypical usage information into log files. These files are stored in the device 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)

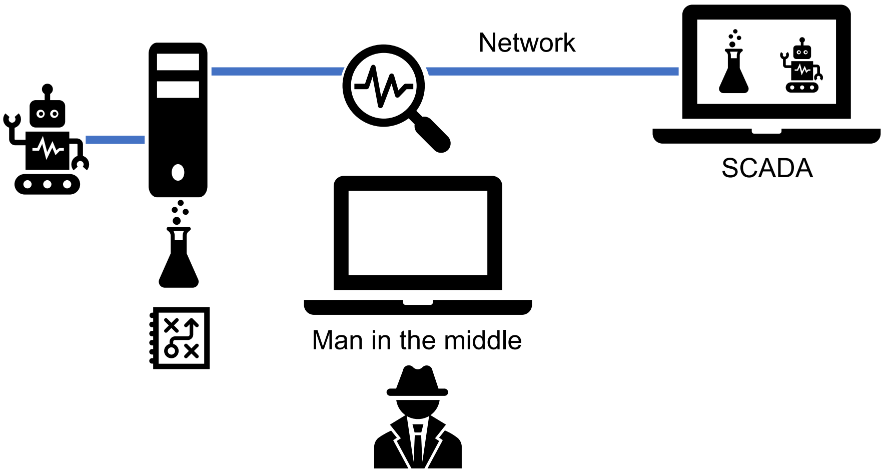
4 Potential threat scenarios

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.

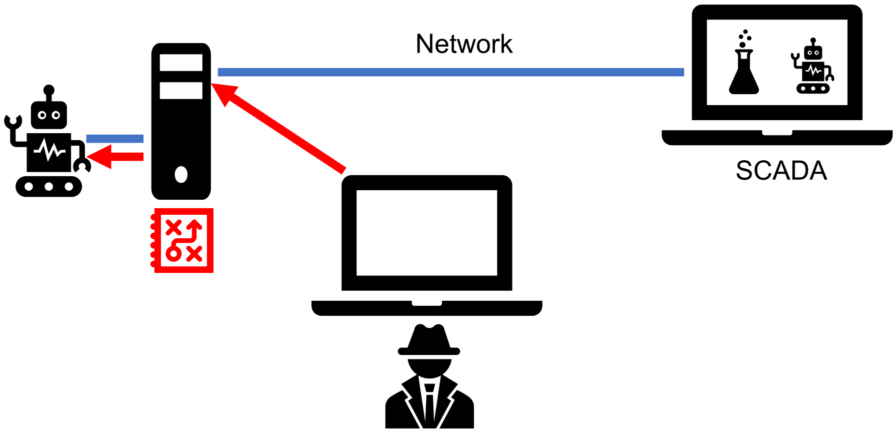
  

  Countermeasures:

  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.

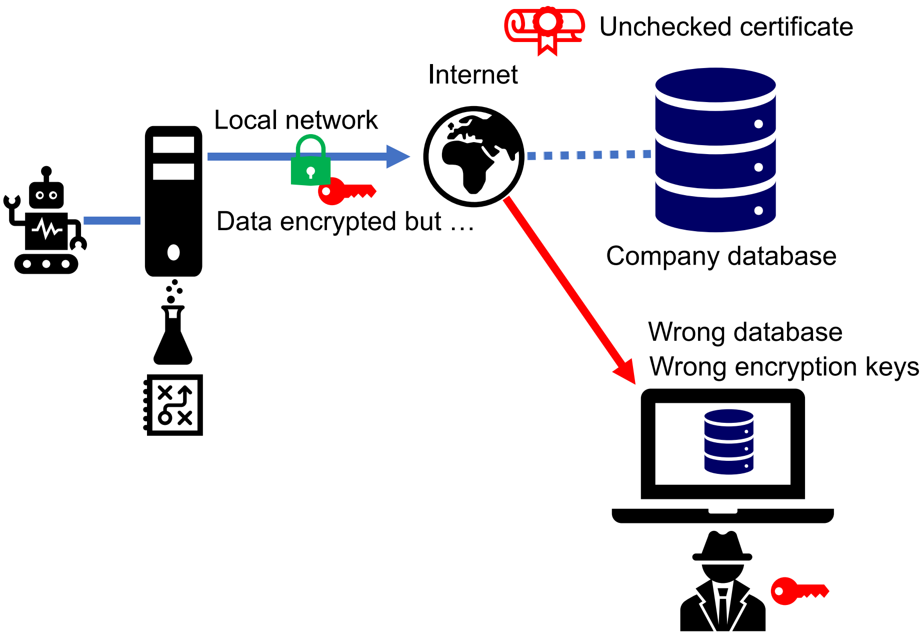
  

  Countermeasures:

  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 HM series touch terminal

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 HM series touch terminal.

Related topics

Security configuration checklist (page 14)

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 applications and for the HM series touch terminal main settings. When a terminal is switched on for the first time, you will be asked to enter a new secure password. This can be done directly on the display or via a browser connected to the device via its IP address (IP/machine_config).

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, ETH1, and ETH2).

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.

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 HM series touch terminal. 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)	HMWIN Studio Project/Configuration/Security	Change default admin and user passwords
	High	Protocol configuration	HMWIN Studio Project/Configuration/Protocols	Disable passthrough features and server protocols if not needed Choose encrypted variants of the fieldbus protocols used
	Medium	HMWIN OPC UA feature	HMWIN Studio Project/Configuration/Interface	Check server access
	Medium	HMWIN MQTT feature	HMWIN Studio Project/Configuration/Interface	Use encryption and certificates
	Medium	SMTP and FTP Javascript features	HMWIN Studio Check your configured events (e.g. email, FTP, web camera ...)	Use encryption and certificates

[1] The risk level depends on your application.

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 1.0, 2024.07

First edition