YASKAWA

HMI

TP-smart | H71-A1A41-0 | Manual

HB160 | TP-smart | H71-A1A41-0 | en | 26-15

smartPanel - TP407-SM



YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Germany
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
Email: info@yaskawa.eu
Internet: www.yaskawa.eu.com

H71-A1A41-0_000_TP407-SM,2,EN - © 2026

Table of contents

1 General. 5
1.1 About this manual. 5
1.2 Copyright © YASKAWA Europe GmbH. 6
1.3 Safety instructions. 7
2 Hardware description. 10
2.1 Safety notes for the user. 10
2.2 Properties. 10
2.3 Structure. 12
2.3.1 Overview. 12
2.3.2 Interfaces. 13
2.3.3 Memory management. 15
2.4 Dimensions. 15
2.5 General data for the smartPanel. 16
2.6 Use in difficult operating conditions. 17
2.7 Technical data. 18
3 Deployment. 20
3.1 Installation. 20
3.2 Commissioning. 21
3.3 System Settings. 23
3.3.1 Overview. 23
3.3.2 Localisation. 23
3.3.3 System. 24
3.3.4 Logs. 24
3.3.5 Date & Time. 24
3.3.6 Network. 24
3.3.7 Security. 25
3.3.8 Applications. 25
3.3.9 Services. 25
3.3.10 Management. 26
3.3.11 Display. 27
3.3.12 Fonts. 27
3.3.13 Authentication. 27
3.3.14 Restart. 27
3.4 Startup Sequence. 27
3.5 Tap-Tap Menu. 28
3.6 Firmware update. 29
3.7 Connection to a PLC system. 30

3.8 Integrated server. 31
3.8.1 FTP server. 31
3.8.2 VNC server. 32
3.8.3 Web server. 32
4 Industrial security and installation guidelines. 33
4.1 Industrial security in information technology. 33
4.1.1 Protection of hardware and applications. 34
4.1.2 Protection of PC-based software. 35
4.2 Installation guidelines. 35

1 General

1.1 About this manual

Objective and contents

This manual describes the smartPanel H71-A1A41-0.

- It contains a description of the structure, project engineering and deployment.
- The manual is written for users with basic knowledge of automation technology.
- The manual consists of chapters. Each chapter describes a completed topic.
- The following guides are available in the manual:
  - An overall table of contents at the beginning of the manual.
  - References with pages numbers.

Validity of the documentation

Product	Order no.	as of version:	
TP 407-SM	H71-A1A41-0	HW: 01	Board Support Package (BSP): V3.1.403

Documentation

In the context of the use of the pertinent Yaskawa product, the manual is to be made accessible to the pertinent qualified personnel in:

- Project engineering
- Installation department
- Commissioning
- Operation

Icons and headings

Important passages in the text are highlighted by following icons and headings:

DANGER

- Immediate danger to life and limb of personnel and others.
- Non-compliance will cause death or serious injury.

CAUTION

- Hazardous situation to life and limb of personnel and others. Non-compliance may cause slight injuries.
- This symbol is also used as warning of damages to property.

NOTICE

- Designates a possibly harmful situation.
- Non-compliance can damage the product or something in its environment.

Supplementary information and useful tips.

Copyright © YASKAWA Europe GmbH

1.2 Copyright © YASKAWA Europe GmbH

All rights reserved

This document contains protected information of Yaskawa and may not be disclosed or used outside of an agreement made in advance with Yaskawa and only in accordance with that agreement.

This document is protected by copyright laws. Reproduction, distribution, or modification of this document or excerpts thereof is not permitted without the written consent of Yaskawa and the owner of this document, except in accordance with applicable agreements, contracts or licenses.

For permission to reproduce or distribute, please contact: YASKAWA Europe GmbH, European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany

Tel.: +49 6196 569 300
Fax.: +49 6196 569 398
E-mail: info@yaskawa.eu
Internet: www.yaskawa.eu.com

Download Center

By entering the product order number in the *'Download Center'* at www.yaskawa.eu.com, the pertinent manuals, data sheets, declarations of conformity, certificates and other helpful information for your product can be found.

Trademarks

Linux is a registered trademark of Linus Torvalds.

All other trademarks, logos and service or product marks specified herein are owned by their respective companies.

General terms of use

Every effort was made by Yaskawa to ensure that the information contained in this document was complete and correct at the time of publication. Nevertheless, the information contained therein is only owed by Yaskawa as it is available at Yaskawa. Correctness is not assured by Yaskawa, the right to change the information contained herein is always reserved by Yaskawa. There is no obligation to inform the customer of any changes. The customer is requested to actively keep this documentation up to date. The use of the products covered by these instructions, together with the associated documentation, is always at the customer's own risk, in accordance with the applicable guidelines and standards. This documentation describes the hardware and software components and functions of the product. It is possible that units are described which the customer does not have. The exact scope of delivery is described in the respective purchase contract.

Document support

Contact your local representative of YASKAWA Europe GmbH if you have errors or questions regarding the content of this document. You can reach YASKAWA Europe GmbH via the following contact:

Email: Documentation.HER@yaskawa.eu

Technical support

Contact your local representative of YASKAWA Europe GmbH if you encounter problems or have questions regarding the product. If such a location is not available, you can reach the Yaskawa customer service via the following contact:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany
Tel.: +49 6196 569 500 (hotline)
Email: support@yaskawa.eu

1.3 Safety instructions

General safety instructions

DANGER

Danger to life due to non-compliance with safety instructions

Non-compliance with the safety instructions in the manual can result in serious injury or death. The manufacturer is not responsible for any injuries or damage to the equipment.

CAUTION

Before commissioning and operating the components described in this manual, it is essential to note the following:

- Modifications to the automation system must only be done in a voltage-free state!
- Connection and modification only by trained electricians
- National regulations and guidelines in the respective country of use must be observed and complied with (installation, protective measures, EMC, etc.)

Intended use

- It is the customer's responsibility to comply with all pertinent standards, codes, or regulations applicable to the use of the product, including those that apply when the Yaskawa product is used in combination with other products.
- The customer must confirm that the Yaskawa product is suitable for the customer's plant, machinery and equipment.
- If the Yaskawa product is used in a manner not specified by this manual, the protection provided by the Yaskawa product may be impaired and the use may result in material or immaterial damage.
- Contact Yaskawa to determine whether use is permitted in the following applications. If the use in the respective application is permissible, the Yaskawa product is to be used by considering additional risk assessments and specifications, and safety measures are to be provided to minimise the dangers in the event of a fault. Special caution is required and protective measures must be taken in the case of:
  - Outdoor use, use with possible chemical contamination or electrical interference, or use under conditions or in environments which are not described in product catalogs or manuals.
  - Nuclear control systems, combustion systems, railway systems, aviation systems, automotive systems, medical devices, amusement machines and equipment that is specifically regulated by industry or government.
  - Systems, machines and devices that can pose a risk to life or property.
  - Systems that require a high degree of reliability, such as gas, water or electricity supply systems or systems that operate 24 hours a day.
  - Other systems that require a similarly high level of security.
- Never use the Yaskawa product in an application where failure of the product could cause serious danger to life, limb, health or property without first ensuring that the system is designed to provide the required level of safety with risk warnings and redundancy to avoid the realisation of such dangers and that the Yaskawa product is properly designed and installed.
- The connection examples and other application examples described in the product catalogs and manuals of Yaskawa are for reference purposes. Check the functionality and safety of the devices and systems actually to be used before using the Yaskawa product.
- To avoid accidental harm to third parties, read and understand all prohibitions on use and precautions, and operate the Yaskawa product correctly.

Field of application

- The Yaskawa product is not suited for use in life-support machines or systems.
- Please contact your Yaskawa representative or Yaskawa distributor if considering the use of the Yaskawa product for special purposes, such as machines or systems used in passenger cars, in medical, aircraft and aerospace applications, for power supply of networks, for electrical power distribution or for underwater applications.

DANGER

The device is not permitted for use

– in explosive environments (EX zone)

The system is designed and manufactured for proper use and use in accordance with the user manual and is designed for:

- Communication and process control
- general control and automation tasks
- for industrial use
- operation within the environmental conditions specified in the technical data
- installation in a cabinet

DANGER

If this Yaskawa product is used in applications where failure of the device can result in the loss of human life, a serious accident or physical injury, you must install appropriate safety devices.

– Death or serious injury can result if you do not install the safety devices properly.

Disclaimer

(1) The contractual and legal liability of Yaskawa and the legal representatives and vicarious agents of Yaskawa for compensation and reimbursement of expenses in relation to the content of this documentation is excluded or limited as follows:

a) For slightly negligent breaches of *Essential Contractual Duties* arising from the contractual obligation, for Yaskawa the amount of liability is limited to the foreseeable damage typical for the contract. *'Essential Contractual Duties'* are those duties that characterise the performance of the contract and on which the Yaskawa customer may reasonably rely.

(b) In each case, Yaskawa is not liable for (i) the slightly negligent breach of duties arising from the duties that are not *Essential Contractual Duties*, as well as (ii) force majeure, i.e. external events that have no operational connection and cannot be averted even by exercising the utmost care that can reasonably be expected.

(2) The aforementioned limitation of liability does not apply (i) in cases of mandatory statutory liability (in particular under the product liability law), (ii) if and to the extent that Yaskawa has assumed a guarantee or same as guaranteed procurement risk according to § 276 BGB, (iii) for culpably caused injuries to life, limb and/or health, also by representatives or vicarious agents, as well as (iv) in case of delay in the event of a fixed completion date.

(3) A reversal of the burden of proof is not associated with the provisions above.

Disposal

National rules and regulations apply to the disposal of the unit!

2 Hardware description

2.1 Safety notes for the user

Handling of electrostatic sensitive modules

The modules make use of highly integrated components in MOS-Technology. These components are extremely sensitive to over-voltages that can occur during electrostatic discharges. The following symbol is attached to modules that can be destroyed by electrostatic discharges.



The Symbol is located on the module, the module rack or on packing material and it indicates the presence of electrostatic sensitive equipment. It is possible that electrostatic sensitive equipment is destroyed by energies and voltages that are far less than the human threshold of perception. These voltages can occur where persons do not discharge themselves before handling electrostatic sensitive modules and they can damage components thereby, causing the module to become inoperable or unusable. Modules that have been damaged by electrostatic discharges can fail after a temperature change, mechanical shock or changes in the electrical load. Only the consequent implementation of protection devices and meticulous attention to the applicable rules and regulations for handling the respective equipment can prevent failures of electrostatic sensitive modules.

Shipping of modules

Modules must be shipped in the original packing material.

Measurements and alterations on electrostatic sensitive modules

When you are conducting measurements on electrostatic sensitive modules you should take the following precautions:

- Floating instruments must be discharged before use.
- Instruments must be grounded.

Modifying electrostatic sensitive modules you should only use soldering irons with grounded tips.



CAUTION

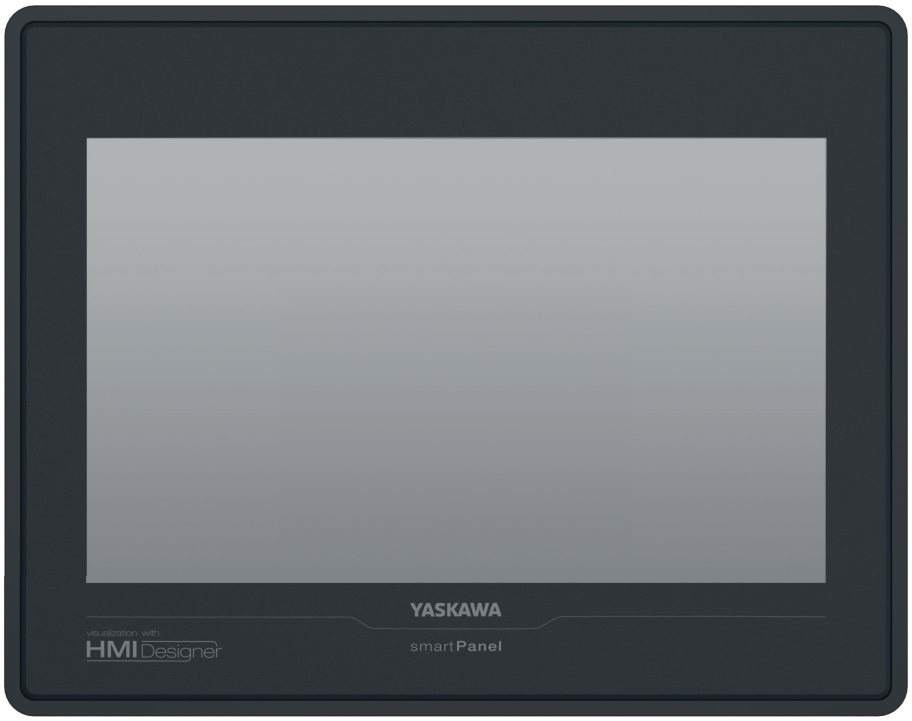
Personnel and instruments should be grounded when working on electrostatic sensitive modules.

2.2 Properties

General

The smartPanel allows you to visualize and alter operating states and recent process values of a connected PLC. The smartPanel is a compact and modular "Embedded PC" based on Linux®. Besides the extensive Linux® functions the smartPanel offers varied communication possibilities like VNC and Web server. Here the smartPanel can simply be configured, controlled and remoted. The smartPanel is particularly suitable for monitoring and controlling of process cycles. For configuration the HMI Designer is to be used.

TP 407-SM



- Linux®
- Configuration via HMI Designer
- Processor ARM Cortex A8 1GHz
- Flash memory 4GB, RAM 512MB DDR
- RS232/RS422/RS485, USB-A- and Ethernet interface
- Robust plastic case
- Display resolution 480 x 800 / 800 x 480, 64K colors
- Clock back up (Goldcap)
- Resistive touch screen
- Easy mounting via mounting clips
- Protection class IP66, Type 2 and 4X (Front) / IP20 (Back)

Order data

Type	Order number	Description
TP 407-SM	H71-A1A41-0	7" TFT color, RS232/RS422/RS485, USB-A, Ethernet RJ45

Spare parts

The following spare parts are available for the smartPanel:

Spare part	Order no.	Description	Packaging unit
	692-9AX00	3-fold connector for power supply smartPanel.	20 pieces

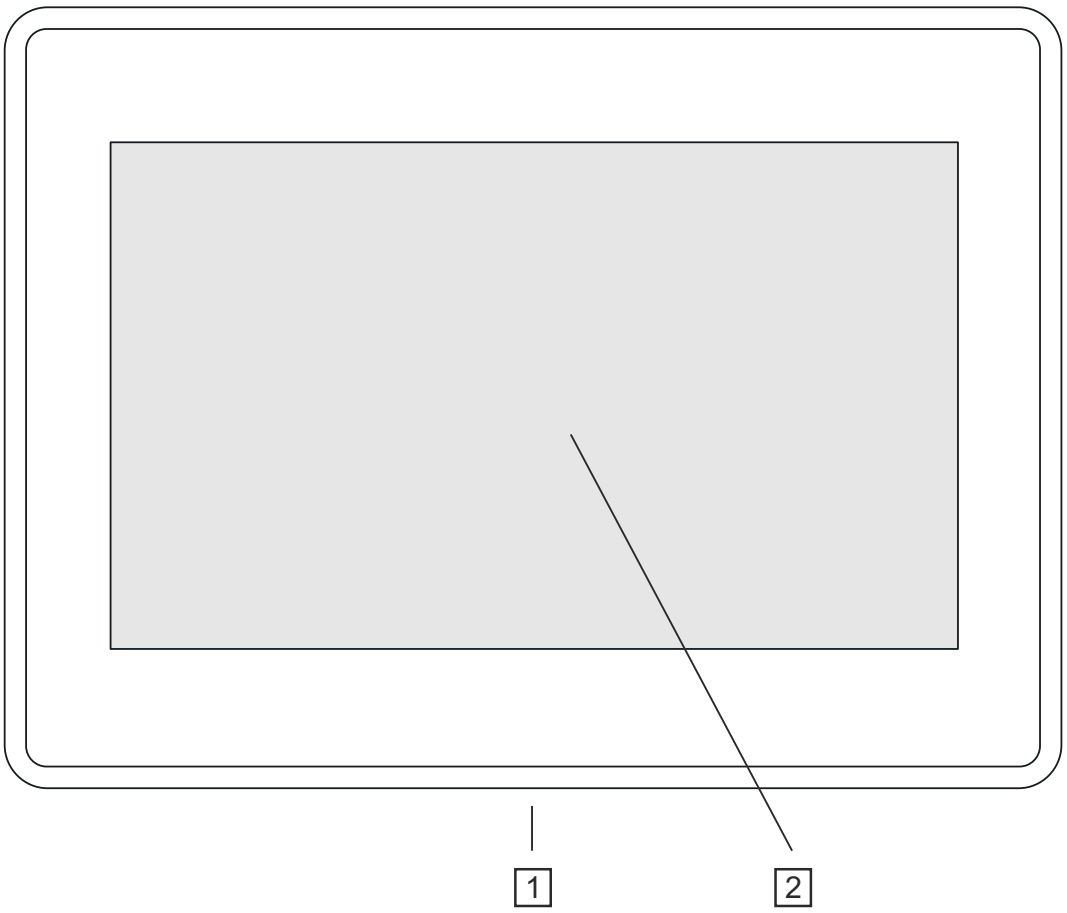
CAUTION

Please note that you may only use the spare parts with Yaskawa modules. Use with third-party modules is not allowed!

2.3 Structure

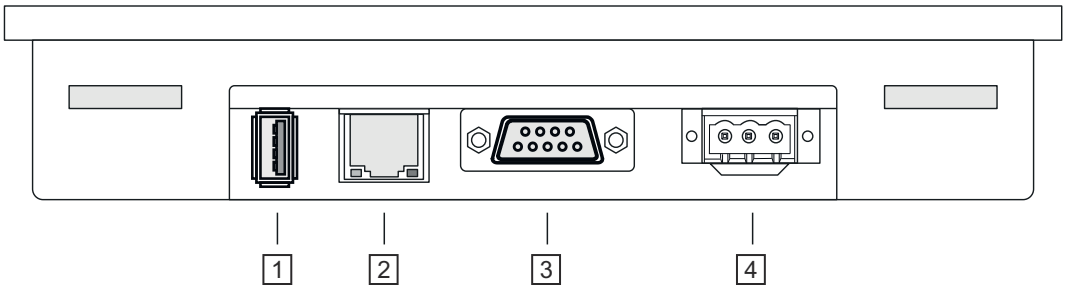
2.3.1 Overview

Front view



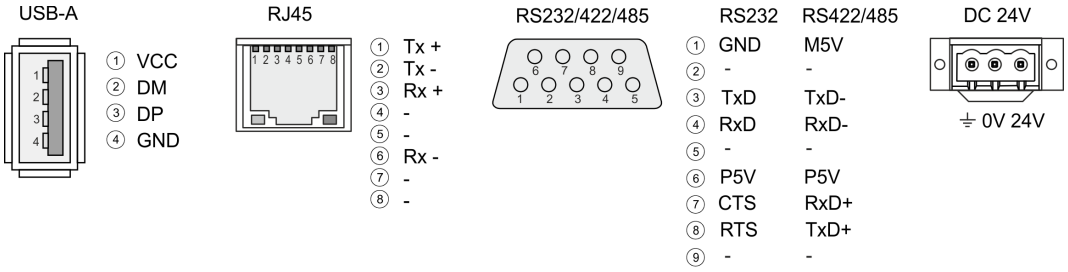
1 Interfaces
2 Display with touch sensitive area (touch screen)

Bottom view



1 USB-A interface USB 2.0
2 RJ45 jack for Ethernet communication LAN
3 RS232/RS422/RS485 interface COM
4 Slot for DC 24V voltage supply

2.3.2 Interfaces



"Host"-USB-A

Using the "Host"-USB-A interface USB mouse, keyboard, stick or USB hard discs can be connected.

Ethernet connection

The RJ45 jack provides the interface to the twisted pair cable, required for Ethernet. The Ethernet interface has got two LEDs for status display.

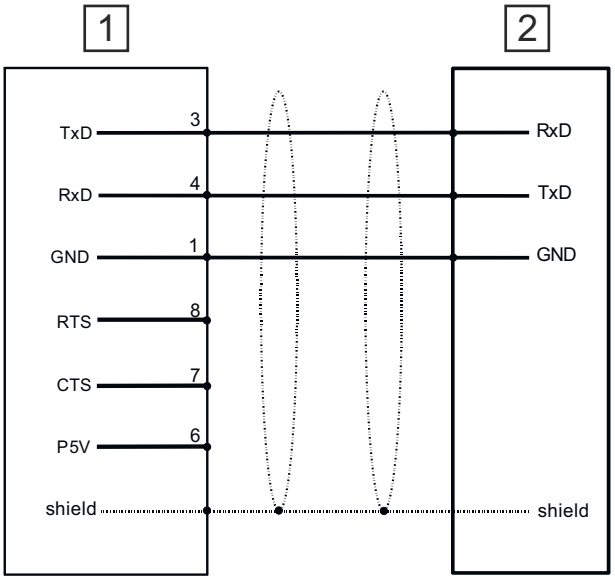
LEDs

green	yellow	Description
on	off	no link
blinks	on	100Mbit/s link
blinks	off	10Mbit/s link

RS232 interface

9 pin SubD plug

- Interface is compatible to the COM interface of a PC
- Logical signals as voltage levels
- Point-to-point links with serial full-duplex transfer in two-wire technology up to 15m distance
- Data transfer rate up to 115.2kbit/s

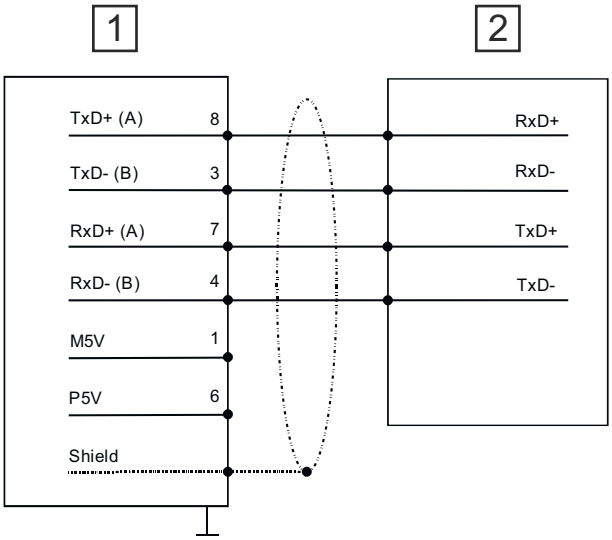


1 RS232 interface
2 Periphery

RS422/485 interface

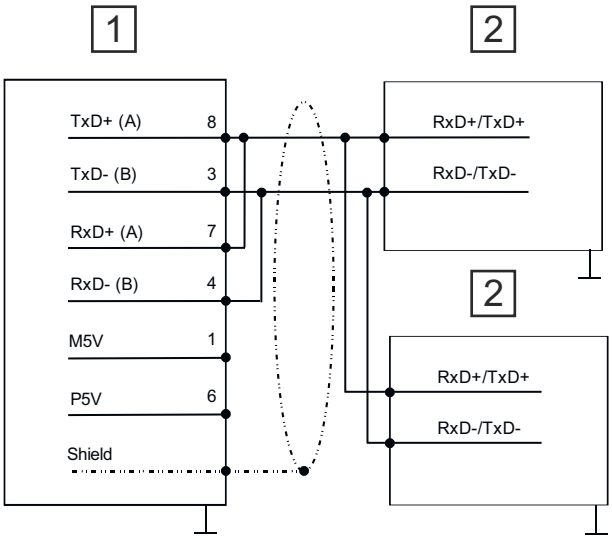
9 pin SubD jack

- Logical states represented by voltage differences between the 4 cores
- Serial bus connection in 4-wire technology using full duplex mode
- Data communications up to a max. distance of 500m
- Data communication rate up to 115.2kBaud



1 Operation as RS422 interface
2 Periphery

- Serial bus connection in 2-wire technology using half duplex mode



1 Operation as RS485 interface
2 Periphery

Power supply

The smartPanel has got an integrated power supply. The power supply has to be provided with DC 24V (10 ... 32 VDC). For this you find an according DC 24V slot at the bottom ➦ *'Connecting the power supply'...page 21*.

2.3.3 Memory management

Overview

The following memory systems are available for the smartPanel:

- 512MB work memory (RAM)
- 4GB user memory (Flash)
- USB storage media using "Host"-USB-A interface

Work memory (RAM)

The smartPanel has a work memory with a size of 512MB. The work memory is not buffered and is deleted after shut down.

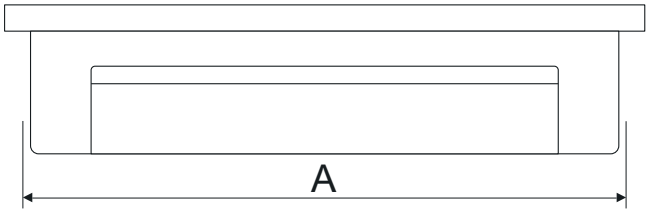
User memory (Flash)

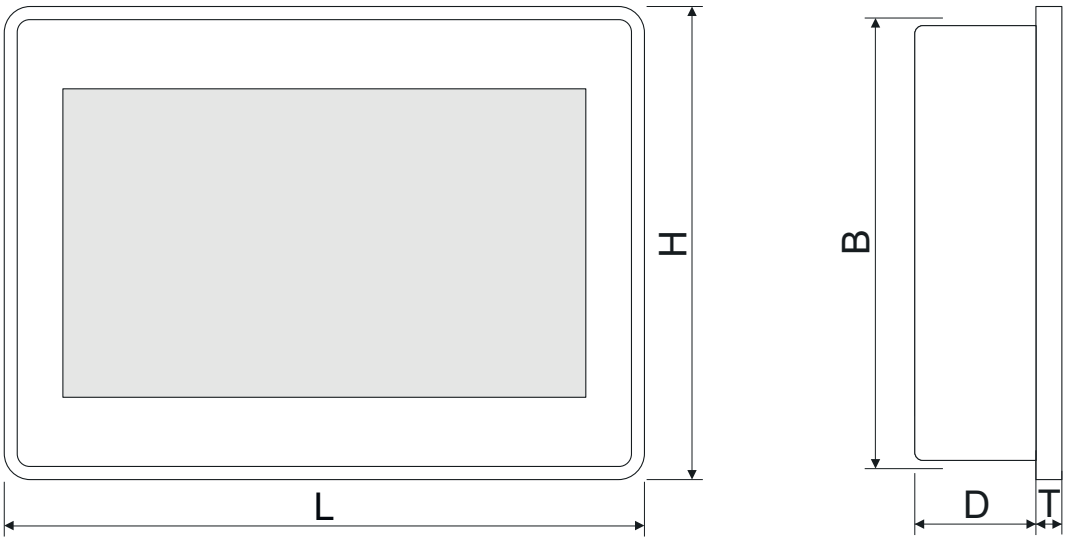
As internal permanent storage medium the smartPanel has a flash memory with a size of 4GB.

USB storage media (USB 2.0)

The connection of USB sticks and USB drives by use of the "Host"-USB-A interface is supported by the smartPanel. After connection the storage media is listed as *USB Hard Disk* under *My Device*.

2.4 Dimensions





Installation dimensions

Front panel (L x H)	187 x 147 mm
Depth (D+T)	29 + 5 mm
Installation cutting (A x B)	176 x 136 mm

The degrees of protection are only guaranteed when the following is observed:

- *Material thickness at the mounting cut-out: 1.5 ... 6mm*
- *The deviation from the plane for the panel cut-out is ≤ 0.5mm. This condition must be fulfilled for the mounted HMI device.*
- *Permissible surface roughness in the area of the seal: ≤ 120µm (friction coefficient 120)*

2.5 General data for the smartPanel

Conformity and approval		
Conformity		
CE	2014/30/EU	EMC Directive
RoHS (EU)	2011/65/EU	Restriction of the use of certain hazardous substances in electrical and electronic equipment
UKCA	2016 No. 1101	Electrical Equipment (Safety) Regulations
	2016 No. 1091	Electromagnetic Compatibility Regulations
RoHS (UK)	2012 No. 3032	Use of Certain Hazardous Substances
Approval		
Certifications	-	Refer to technical data

Protection of persons and device protection		
Type of protection	-	Rear: IP20; Front: IP66, NEMA Type 2 and Type 4x
Electrical isolation		
to the field bus	-	electrically isolated
to the process level	-	electrically isolated
Insulation resistance		-
Insulation voltage to reference earth		
Inputs / outputs	-	AC / DC 50V, test voltage AC 500V
Protective measures	-	against short circuit

Environmental conditions to EN 61131-2		
Climatic		
Storage / transport	EN 60068-2-14	-20…+70°C
Operation		
Horizontal installation	EN 61131-2	0…+40°C
Vertical installation	EN 61131-2	0…+50°C
Air humidity	EN 60068-2-30	RH1 (without condensation, rel. humidity 5…85%)
Pollution	EN 61131-2	Degree of pollution 2
Mechanical		
Oscillation	EN 60068-2-6	1g, 9Hz ... 150Hz
Shock	EN 60068-2-27	15g, 11ms

Mounting conditions		
Mounting place	-	In the control cabinet
Mounting position	-	Horizontal and vertical

EMC	Standard	Comment
Emitted interference	EN 61000-6-4	Class A (Industrial area)
Noise immunity	EN 61000-6-2	Industrial area

EMC	Standard		Comment
zone B		EN 61000-4-2	ESD 8kV at air discharge (degree of severity 3), 4kV at contact discharge (degree of severity 2)
		EN 61000-4-3	HF field immunity (casing) 80MHz … 1000MHz, 10V/m, 80% AM (1kHz) 1.4GHz ... 2.0GHz, 3V/m, 80% AM (1kHz) 2GHz ... 2.7GHz, 1V/m, 80% AM (1kHz)
		EN 61000-4-6	HF conducted 150kHz … 80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-4	Burst
		EN 61000-4-5	Surge[1]

1) Due to the high-energetic single pulses with Surge an appropriate external protective circuit with lightning protection elements like conductors for lightning and overvoltage is necessary.

2.6 Use in difficult operating conditions

Without additional protective measures, the products must not be used in locations with difficult operating conditions; e.g. due to:

- *dust generation*
- *chemically active substances (corrosive vapors or gases)*
- *strong electric or magnetic fields*

2.7 Technical data

Order no.	H71-A1A41-0
Type	smartPanel TP407-SM
Display	
Display size (diagonal)	7 "
Display size (width)	155 mm
Display size (height)	88 mm
Resolution	480 x 800 / 800 x 480
Aspect ratio	16:9
Type of display	TFT color (64K colors)
MTBF Backlights (25°C)	20000 h
System properties	
Processor	Cortex-A8 1GHz
Operating system	Linux 4.14.94
User software	HMI Runtime
Work memory	512 MB
User memory	4 GB
Available memory (user data)	60 MB
SD/MMC Slot	-
CF Card Slot Typ II	-
CFast Slot	-
Time	
Real-time clock buffered	✓
Clock buffered period (min.)	2 w
Type of buffering	Goldcap
Load time for 50% buffering period	5 h
Load time for 100% buffering period	10 h
Accuracy (max. deviation per day)	8 s
Operating controls	
Touchscreen	resistive
Touch function	Single Touch
Keyboard	external via USB
Mouse	external via USB
Interfaces	
MPI, PROFIBUS-DP	-
MPI, PROFIBUS-DP connector	-
Serial, COM1	RS232 / RS422 / RS485
COM1 connector	Sub-D, 9-pin, male
Serial, COM2	-
COM2 connector	-
Number of USB-A interfaces	1
USB-A connector	USB-A (host)
Number of USB-B interfaces	-
USB-B connector	-
Number of ethernet interfaces	1
Ethernet	Ethernet 10/100 MBit
Ethernet connector	RJ45
Integrated ethernet switch	-

Order no.	H71-A1A41-0
Video connectors	-
Audio connections	-
Technical data power supply	
Power supply (rated value)	DC 24 V
Power supply (permitted range)	10 - 32 VDC
Reverse polarity protection	✓
Current consumption (no-load operation)	0.1 A
Current consumption (rated value)	0.3 A
Inrush current	49 A
I^2t	0.7 A^2s
Power loss	7 W
Status information, alarms, diagnostics	
Status display	none
Supply voltage display	none
Mechanical data	
Housing / Protection class	
Material	PC + ABS
Mounting	mounting clips
Protection class IP front side	IP 66
Protection class IP back side	IP 20
Protection class NEMA front side	Type 2, 4X
Protection class NEMA back side	-
Dimensions	
Front panel	187 mm x 147 mm x 5 mm
Rear panel	172 mm x 133 mm x 29 mm
Installation cut-out	
Width	176 mm
Height	136 mm
Minimum	1.5 mm
Maximum front panel thickness	6 mm
Net weight	531 g
Weight including accessories	584 g
Gross weight	860 g
Environmental conditions	
Operating temperature	0 °C to 50 °C
Storage temperature	-20 °C to 70 °C
Certifications	
UL certification	yes
KC certification	-
UKCA certification	yes
ChinaRoHS certification	yes
DNV certification	yes
EU MR certification	yes

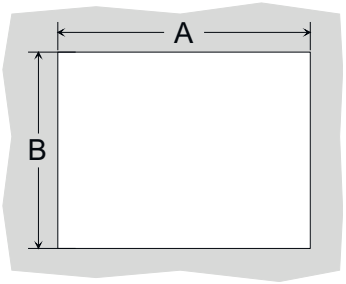
3 Deployment

3.1 Installation

Overview

The smartPanel is suitable for the installation in operating tables and control cabinet fronts. The installation happens via the backside. The smartPanel is provided with a fixing technique that allows an easy connection with a crosstip screwdriver. A fast and easy device change is possible.

Installation cutting



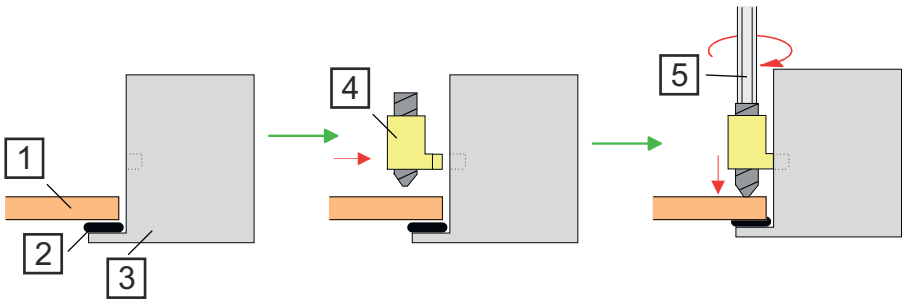
For the installation into a operating tableau and control cabinet fronts, the smartPanel requires the following front plate cutting:

smartPanel	A x B in mm
H71-A1A41-0	176 x 136 mm

Mounting

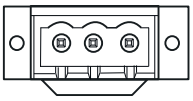
To fix the smartPanel mounting clips are included. A small crosstip screwdriver is required for mounting.

1. Insert your smartPanel [3] from the front through the front panel cut-out [1] until it rests on the seal [2] .
2. Now place the mounting clips [4] into the openings provided on all four sides of the smartPanel so that the tip of the screw points towards the front panel.
3. Use the crosstip screwdriver [5] to tighten the screws.

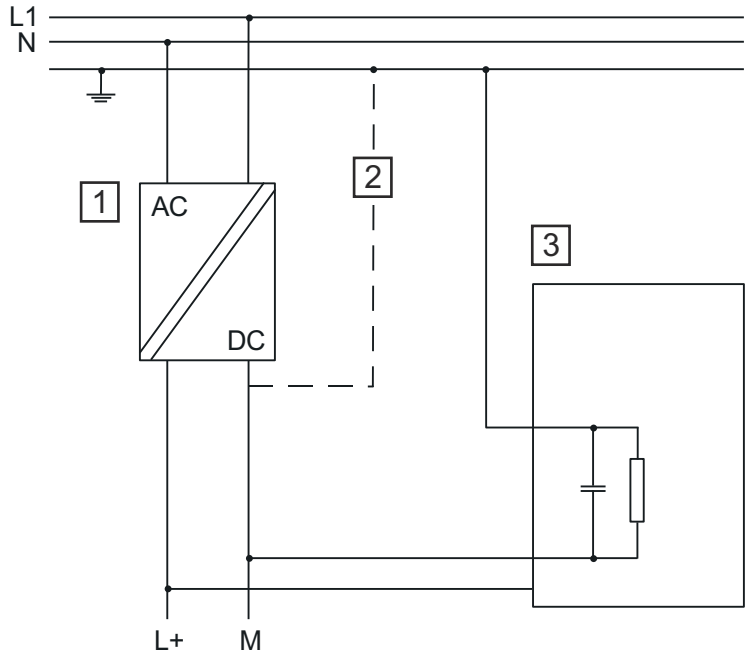


[1] Front panel cut-out
[2] Seal
[3] smartPanel
[4] Mounting clip
[5] Crosstip screwdriver

Connecting the power supply



- For wiring the DC 24V power supply (10 ... 32 VDC), a 3-fold connector with screw contacts is used, which is included in the scope of delivery. The corresponding label is located on the back of the smartPanel.
- The smartPanel must always be connected to the ground. This reduces the effects of electromagnetic interference.
- Use the terminal on the power supply unit labelled ⏚ for earthing.
- The wiring to the power supply can be floating or earthed.
  - With floating wiring, it should be noted that the smartPanel has an internal connection between the power supply and earth via a 1MΩ resistor in parallel with a 4.7nF capacitor.
  - For earthing, connect the power supply to earth as shown in the figure at 2.



1 Power supply
2 With an earthed circuit of the power supply
3 smartPanel

3.2 Commissioning

CAUTION

- Before commissioning the device must be brought to room temperature.
- At condensation the device must be absolutely dry before connected to power.
- Avoid using in direct sunlight.
- After opening the control cabinet or desk, there are parts with possible dangerous voltage available.
- For all signal connections only screened cables are permitted.
- Signal cables must not be let within the same cable shaft as high voltage cables.

IP address

On delivery the smartPanel has the following IP address:

- 192.168.1.100

> *You get valid IP address parameters from your system administrator. These can be specified in the 'System Settings' via Network.* ➦ *'Network'...page 24*

Project transfer

The smartPanel can only be configured with the HMI Designer. Here, the data are transferred via Ethernet to the smartPanel using the IP address. More information can be found in the documentation of the HMI Designer.

1. Mount and wire your smartPanel.
   ➦ *'Installation'...page 20*
2. Establish an Ethernet connection to your smartPanel and switch it on.
3. Start the HMI Designer with your project and open the dialog for the project transfer.
4. Enter the IP Address of the smartPanel or let the system search for it.
5. Transfer your project to the smartPanel.
   ➧ After the transfer, the smartPanel starts with your project.

Runtime

The smartPanel is delivered without a runtime environment, in the following called "runtime". The smartPanel can only be configured with the HMI Designer. As soon as you transfer a project from the HMI Designer to the smartPanel, the corresponding runtime is automatically installed.

Start menu

If no project was transferred yet, the smartPanel shows the *start menu* with access to:

- System Settings
- Startup Sequence

You can also use the "Tap-Tap" method to open the *'Start menu'* during start-up.

➦ *'Tap-Tap Menu'...page 28*

Access data

Please note that the submenu items within the start menu are protected by access data. During initial operation, a password must be assigned as soon as a submenu item is accessed. The following requirements apply:

- At least 8 characters
- At least 1 capital letter (A...Z)
- At least 1 lower-case letter (a...z)
- At least 1 digit (0...9)
- At least 1 special character such as # ! @ ?

After you have assigned a password, the start menu is shown. With your password and the user name *admin* you now have access to the submenu items.

3.3 System Settings

3.3.1 Overview

Submenu

The submenu is protected by access data.

➦ *'Access data'...page 22*

After requesting the access data, you can access the basic settings of smartPanel via the following submenu items:

- Localisation
- System
- Logs
- Date & Time
- Network
- Security
- Applications
- Services
- Management
- Display
- Fonts
- Authentication
- Restart

Navigation

The following navigation elements are located in the header of a submenu:

- jumps back to the overview of the System Settings.
- opens the editing dialog, if available. Within the dialog, you can apply your changes with Safe or close the dialog without saving with Cancel .
- refreshes the view.
- jumps back to the Start menu.

3.3.2 Localisation

Language

The interface language for the smartPanel can be set here

Country Code

This parameter is not relevant for this smartPanel and should remain at *'00...'*.

System Keyboard Layout

The layout of the system keyboard can be set here

3.3.3 System

Info

Here you will find information on the operating system, the serial and article number, the available working memory (RAM) of the smartPanel and have access to the license information package.

- The smartPanel works with a Linux operating system.
- Via the button *'Get license info package'* licence information on the individual Linux packages can be retrieved.
- Any open source software used in the product is subject to the respective licence terms, which are not affected by the Yaskawa Software Licence Terms (SLT) for the product.
- The licensee can change the respective open source software in accordance with the applicable license terms.

Status

Here you get information about the current device status such as free working memory, operating time since PowerON and average CPU load at various time intervals.

Timers

The total running time of the system and the backlight is shown here.

3.3.4 Logs

Persistent log

When enabled, the log data are saved permanently and is still available after a PowerON. With *'Safe'* the log file can be downloaded to a connected PC.

3.3.5 Date & Time

Date and time of the smartPanel can be changed here. For this go to *Edit* .

Provided *'Automatic update (NTP)'* is disabled, date and time can be set here.

If *'Automatic update (NTP)'* is enabled, the smartPanel gets the time and date from the NTP server to be specified here.

By enabling *'Slow time adjustment … '* the time is adjusted by no more than 1 minute per day.

Is *'Accept NTP requests'* is enabled, the smartPanel serves as a time server and responds to external NTP requests.

3.3.6 Network

The network settings of smartPanel can be changed here. For this go to *Edit* .

General settings

A device name for the smartPanel can be assigned here.

Network interface

If *'DHCP'* is disabled, the network parameters such as IP address, network mask and gateway can be set here.

If DHCP is enabled, these parameters are automatically retrieved from the DHCP server.

DNS

A DNS server for hostname resolution or a DNS domain for search can be specified here. Typically, a DNS server is provided by the DHCP server.

Restore

This will reset all network, firewall and router settings to their delivery state!

3.3.7 Security

Credentials

This function can only be accessed by a registered administrator.

The security area contains passwords and certificates that are required for your applications. They can be created, deleted, imported and exported.

3.3.8 Applications

Via the [App Management] button the application programmes of the smartPanel can be managed here.

If *'Autostart'* is enabled, the corresponding application will be started when the smartPanel is switched on.

Via Bootsequence the order in which the applications are started is defined.

3.3.9 Services

This function can only be accessed by a registered administrator.

Autorun scripts from external storage

When enabled, a script file "autoexec.sh" can be executed from a connected USB stick. Disable this service if you want to prevent unauthorized access via the USB interface.

Avahi Daemon

Avahi is a system that enables programs to serve and recognise services and hosts in a local network. When enabled, the smartPanel can also be accessed via the host name of the device (as an alternative to the IP address).

Cloud / VPN Service

Remote maintenance can be configured here for devices that are connected to a central server via gateways.

Further details can be found in the online help of the HMI Designer.

DHCP Server

The settings for the DHCP server can be configured here.

Enable device restore via Tap Tap option

When enabled, the *'Tap-Tap Menu'* can be used to reset the device to factory settings if, for example, the administrator password is not known.

➦ *'Tap-Tap Menu'...page 28*

Enable device restore via USB

When enabled, the USB stick can be used to restore factory settings if, for example, the administrator password is not known. For this, create an empty file without an extension with the name *'device-factory-restore'* in the root directory. After the boot process, this file is detected on the USB stick and a reset to the factory settings is applied.

Firewall Service

The firewall can be configured here by blocking connections or defining rules for them.

Further details can be found in the online help of the HMI Designer.

Router / NAT / Port forwarding

The IP/port forwarding and network address translations can be configured here.

Further details can be found in the online help of the HMI Designer.

Show loading bar during boot

When enabled, a loading bar is shown during the boot phase.

SNMP Server

When enabled, the SNMP manager can retrieve information from smartPanel by means of the SNMP protocol. SNMP is a network protocol that can be used to manage network infrastructures. It is often used to monitor network devices such as switches, routers, etc. that are connected to a LAN network.

Further details can be found in the online help of the HMI Designer.

SSH Server

When enabled, login can be done by means of the Secure Shell protocol.

Further details can be found in the online help of the HMI Designer.

VNC Service

When enabled the smartPanel can be remotely accessed by means of a VNC client.

➥ *'VNC server'...page 32*

Further details can be found in the online help of the HMI Designer.

Web Server

The parameters for the web server can be set here.

➥ *'Web server'...page 32*

Further details can be found in the online help of the HMI Designer.

3.3.10 Management

This function can only be accessed by a registered administrator.

In this area, the individual components of the Linux operating system can be managed. This includes the individual operating system components and the *'Splash Screen'*. Information on usage and size of the respective component is also listed here.

CAUTION

Please note that working in the Management area is a critical process. If this is not properly executed, it can lead to product damage that requires product maintenance.

Further details can be found in the online help of the HMI Designer.

3.3.11 Display

Here a slider can be used to adjust the brightness of the display and the time until the automatic backlight turns off. After the set time elapses, the backlight is switched off and is activated again by touching the display.

The *'Orientation'* option allows you to adjust the panel alignment to the built-in alignment. Here you can choose between 90°, 180°, 270° or 360°.

The [Touch calibration] button can be used to access the calibration for the touch display. For calibration, follow the instructions on the display.

3.3.12 Fonts

The fonts can be managed here and additional fonts installed if required.

3.3.13 Authentication

Users

Click on *Edit* to change the corresponding passwords. The following user data are available for the smartPanel:

- Administrator
  - User name: admin
  - The password must be defined during commissioning.
- Standard user (default: disabled)
  - User name: user
  - Password: user

x.509 Certificate

A generated certificate is used in the smartPanel to encrypt Internet communication via the HTTPS protocol. The certificate can be personalised with your company's details and verified by a certification authority.

Further details can be found in the online help of the HMI Designer.

3.3.14 Restart

You can restart the smartPanel here. For this, select *'Main OS'* and confirm the security prompt.

3.4 Startup Sequence

The submenu is protected by access data.

➥ *'Access data'...page 22*

Via the [App Management] button the application programmes of the smartPanel can be managed here.

If *'Autostart'* is enabled, the corresponding application will be started when the smartPanel is switched on.

Via Bootsequence the order in which the applications are started is defined.

3.5 Tap-Tap Menu

Accessing the Tap-Tap Menu

The *Tap-Tap Menu* can be accessed by quickly touching the screen in a certain order during the start-up of the smartPanel.

1. Switch on the smartPanel and wait until *'Yaskawa'* is shown.
2. Tap the screen several times in quick succession.
   ➡ You receive the message `TAP-TAP DETECTED` and find yourself in the Tap-Tap Menu.

   After a countdown of 5s, the following menu items are shown for selection:

   - System Settings
   - Touchscreen Calibration
   - Device Restore

   A menu item is selected by pressing any point on the touch screen and holding it for at least 5 seconds.

"TAP-TAP DETECTED 5"
RESTART CONFIG OS
>> SYSTEM SETTINGS

Accessing the System Settings

1. Open the Tap-Tap Menu as shown above.
2. It is not necessary to press the touchscreen to access the System Settings. Wait until the Tap-Tap Menu disapears and the Start menu is shown. From here the *'System Settings'* can be accessed.

"TAP-TAP DETECTED 5"
RESTART CONFIG OS
>> SYSTEM SETTINGS

Accessing the touch screen calibration

1. Open the Tap-Tap Menu as shown above.
2. Wait until *'TOUCHSCREEN CALIBRATION'* is listed. To access the touchscreen calibration, press any point on the touchscreen within 5 seconds and hold it for at least 5 seconds.
   ➡ *'>>'* switches to TOUCHSCREEN CALIBRATION and the counter behind 'TAP-TAP DETECTED' starts a countdown of 5s.
3. Release the touch after the countdown has finished.
   ➡ The touchscreen calibration opens.
4. For calibration, follow the instructions on the display.

"TAP-TAP DETECTED 5"
>> DEFAULT MODE
TOUCHSCREEN CALIBRATION

Device restore

If enabled in ➡ *'System Settings'...page 23* at *'Services'*, this function can be used to reset the device to its factory settings.

1. Open the Tap-Tap Menu as shown above.
2. Wait until *'DEVICE RESTORE'* is listed. To reset to factory settings, press any point on the touchscreen within 5 seconds and hold it for at least 5 seconds.
   ➡ *'>>'* switches to DEVICE RESTORE and the counter behind 'TAP-TAP DETECTED' starts a countdown of 5s.
3. Release the touch after the countdown has finished.
   ➡ The device resets to factory settings and restarts.

"TAP-TAP DETECTED 5"
>> DEFAULT MODE
DEVICE RESTORE



Please note that when resetting to factory settings, all applications will be removed and all settings will be changed to the respective default value!

3.6 Firmware update

Overview

- The latest firmware versions can be found in the *'Download Center'* of www.yaskawa.eu.com at *'Firmware H71-A1A41-0'*.
- The *'Autorun scripts from external storage'* service must be enabled in the *'System Settings'*.
- An empty USB stick with at least 1GB in FAT32 format is required for the firmware update.
- The identification of a firmware file on the memory card takes place by means of a defined naming convention.
- The update starts automatically.

Retrieve firmware version

Via *'System'* of the *'System Settings'* information about the firmware version can be retrieved.

➦ *'System Settings'...page 23*

Update the firmware



CAUTION

When installing a new firmware you have to be extremely careful. In certain circumstances, your smartPanel may become unusable if, for example, the power supply is interrupted during transmission or the firmware file is faulty. In this case, please contact our hotline!

1. Go to the *'Download Center'* of www.yaskawa.eu.com.
2. At *'Firmware H71-A1A41-0'*, download the appropriate zip file for your smartPanel to your PC.
3. Unzip the zip file and copy the files to the root directory of your USB stick. The USB stick should have at least 1GB and be previously formatted in FAT32 format.
4. To ensure the H71-A1A41-0 can access the USB stick automatically, open the *'System Settings'* of the H71-A1A41-0, enable at *'Services'* the parameter *'Autorun scripts from external storage'* and save your settings.

   ➦ *'System Settings'...page 23*
5. Switch off the H71-A1A41-0.
6. Insert the USB stick.
7. Switch on the H71-A1A41-0.

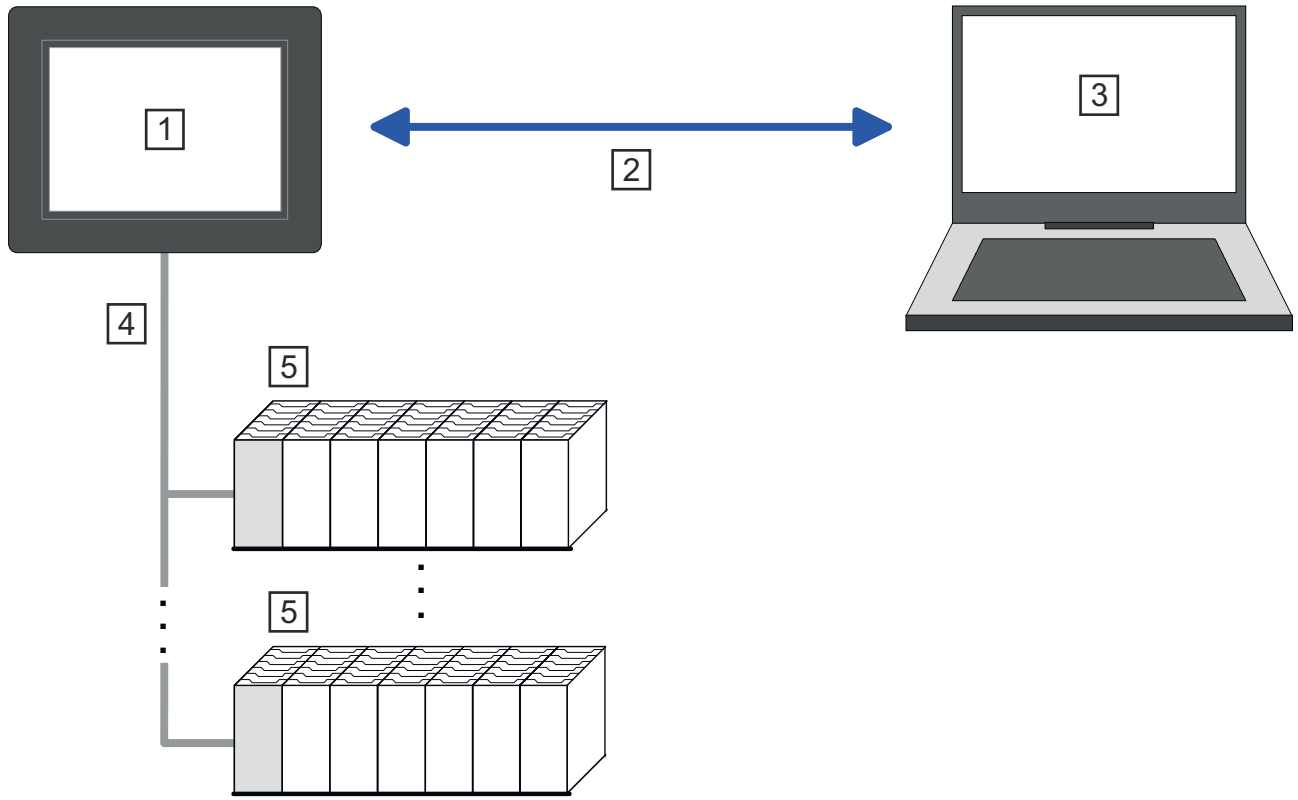
   ➥ After the boot process, the firmware package on the USB stick is recognized, the firmware update is started automatically and shown accordingly on the display.
8. As soon as you get the message that the firmware update is completed, switch the H71-A1A41-0 off, remove the USB stick and switch the H71-A1A41-0 on again.
9. If necessary, disable the parameter *'Autorun scripts from external storage'*.

   ➥ After the start-up, the H71-A1A41-0 is ready for operation with the new firmware.

3.7 Connection to a PLC system

Overview

- To integrate it into your PLC system, the HMI Designer is to be used, which is to be installed on a PC. Here the project can be created and simulated if necessary and transferred to the smartPanel via Ethernet or a USB stick. The runtime version installed on your smartPanel will enable your project to run on the smartPanel.
- The corresponding communication drivers provide connectivity of the smartPanel to your PLC over Ethernet.
- During operation, the smartPanel communicates with the corresponding control system and reacts to programme sequences in the PLC based on the configured specifications. Process values can be graphically displayed, changed and evaluated using previously configured dialogs.



1 smartPanel with VNC / FTP / web server
2 Ethernet connection
3 PC with HMI Designer
4 PLC connection via Ethernet
5 PLC

3.8 Integrated server

Overview

The following servers are integrated in the smartPanel, which enable remote maintenance via Ethernet:

- FTP server - Default: enabled
- VNC server - Default: disabled
- Web server - cannot be disabled

Terms used to describe the servers:

- Client
  - A *client* is an application that uses the service of a server in a network. For example, a web browser is a client because it sends a request to a web server each time a web page is accessed and then receives a response from the server.
- Server
  - A *server* is a programme that waits for a client programme to establish contact and exchanges messages with it after contact has been established. This type of communication is called client-server communication.
- Host
  - A *host* is a device within a network on which at least one server is operated.
- Download
  - Data transfer server >>> client
- Upload
  - Data transfer server <<< client

3.8.1 FTP server

The smartPanel has a built-in FTP server. FTP means **F**ile **T**ransfer **P**rotocol and is used to transfer files via Ethernet between client and server.

Here via your PC files and directories can be copied, deleted or created at the smartPanel. For access, user data must be created at the smartPanel and a corresponding FTP client must be installed on the PC.

Further details can be found in the online help of the HMI Designer.

3.8.2 VNC server

The smartPanel has a built-in VNC server. VNC means **V**irtual **N**etwork **C**ontrol and offers full control of the smartPanel via the connected Ethernet by a PC. Mouse actions and keystrokes are sent to the smartPanel, the screen contents are transferred to the PC and shown in a window. For access, the VNC server must be enabled on the smartPanel and a corresponding VNC viewer must be installed on the PC.

Since all security settings can be bypassed with the VNC server, you should only use it for tests and commissioning! For security reasons, this is disabled on delivery.

Please also note that we cannot offer support for VNC functionality of the Yaskawa. Further information can be found at the manufacturer of the VNC viewer, which is also available as open source.

Establishing a VNC connection

1. Start your smartPanel and open the ➦ *'System Settings'...page 23*.
2. Enable at *'Services'* the service *'VNC Service'* and save the settings.
   ➡ The VNC server on the smartPanel is started.
3. Install a VNC viewer such as TightVNC Viewer on your PC and open it.
4. Enter the IP address *'Remote Host'* of your smartPanel and click [Connect].
   ➡ A connection to the smartPanel is established and the screen content is shown in a window. Mouse actions and keystrokes are sent to the smartPanel.
5. After commissioning, you should always disable the VNC server via the *'System Settings'*.

3.8.3 Web server

The smartPanel has an integrated web server that allows the administration of the smartPanel or web pages of the smartPanel, depending on the access. Administrative access to the web server via Ethernet from the PC is done by entering the IP address of the smartPanel.

Access to the web page is protected by access data that can be assigned during commissioning or in the System Settings.

➦ *'Commissioning'...page 21*

➦ *'System Settings'...page 23*

Further details can be found in the online help of the HMI Designer.

Please note that the integrated web server cannot be disabled. Further settings are available via 'Services' in ➦ *'System Settings'...page 23* *at 'Web Server'.*

4 Industrial security and installation guidelines

4.1 Industrial security in information technology

Latest version

This chapter can also be found as a guide *'Industrial IT Security'* in the *'Download Center'* of www.yaskawa.eu.com

Hazards

The topic of data security and access protection has become increasingly important in the industrial environment. The increased networking of entire industrial systems to the network levels within the company together with the functions of remote maintenance have all served to increase vulnerability. Hazards can arise from:

- Internal manipulation such as technical errors, operating and program errors and deliberate program or data manipulation.
- External manipulation such as software viruses, worms and trojans.
- Human carelessness such as password phishing.

Precautions

The most important precautions to prevent manipulation and loss of data security in the industrial environment are:

- Encrypting the data traffic by means of certificates.
- Filtering and inspection of the traffic by means of VPN - "Virtual Private Networks".
- Identification of the user by "Authentication" via save channels.
- Segmenting in protected automation cells, so that only devices in the same group can exchange data.
- Deactivation of unnecessary hardware and software.

Further Information

You can find more information about the measures on the following websites:

- Federal Office for Information Technology ➦ *www.bsi.bund.de*
- Cybersecurity & Infrastructure Security Agency ➦ *us-cert.cisa.gov*
- VDI / VDE Society for Measurement and Automation Technology ➦ *www.vdi.de*

4.1.1 Protection of hardware and applications

Precautions

- Do not integrate any components or systems into public networks.
  - Use VPN "Virtual Private Networks" for use in public networks. This allows you to control and filter the data traffic accordingly.
- Always keep your system up-to-date.
  - Always use the latest firmware version for all devices.
  - Update your user software regularly.
- Protect your systems with a firewall.
  - The firewall protects your infrastructure internally and externally.
  - This allows you to segment your network and isolate entire areas.
- Secure access to your plants via user accounts.
  - If possible, use a central user management system.
  - Create a user account for each user for whom authorization is essential.
  - Always keep user accounts up-to-date and deactivate unused user accounts.
- Secure access to your plants via secure passwords.
  - Change the password of a standard login after the first start.
  - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
  - Change the passwords according to the rules and guidelines that apply to your application.
- Deactivate inactive communication ports respectively protocols.
  - Only the communication ports that are used for communication should be activated.
  - Only the communication protocols that are used for communication should be activated.
- Consider possible defence strategies when planning and securing the system.
  - The isolation of components alone is not sufficient for comprehensive protection. An overall concept is to be drawn up here, which also provides defensive measures in the event of a cyber attack.
  - Periodically carry out threat assessments. Among others, a comparison is made here between the protective measures taken and those required.
- Limit the use of external storage media.
  - Via external storage media such as USB memory sticks or SD memory cards, malware can get directly into a system while bypassing a firewall.
  - External storage media or their slots must be protected against unauthorized physical access, e.g. by using a lockable control cabinet.
  - Make sure that only authorized persons have access.
  - When disposing of storage media, make sure that they are safely destroyed.
- Use secure access paths such as HTTPS or VPN for remote access to your plant.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.

4.1.2 Protection of PC-based software

Precautions

Since PC-based software is used for programming, configuration and monitoring, it can also be used to manipulate entire systems or individual components. Particular caution is required here!

- Use user accounts on your PC systems.
  - If possible, use a central user management system.
  - Create a user account for each user for whom authorization is essential.
  - Always keep user accounts up-to-date and deactivate unused user accounts.
- Protect your PC systems with secure passwords.
  - Change the password of a standard login after the first start.
  - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
  - Change the passwords according to the rules and guidelines that apply to your application.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.
- Protect your PC systems by security software.
  - Install virus scanners on your PC systems to identify viruses, trojans and other malware.
  - Install software that can detect phishing attacks and actively prevent them.
- Always keep your software up-to-date.
  - Update your operating system regularly.
  - Update your software regularly.
- Make regular backups and store the media at a safe place.
- Regularly restart your PC systems. Only boot from storage media that are protected against manipulation.
- Use encryption systems on your storage media.
- Perform security assessments regularly to reduce the risk of manipulation.
- Use only data and software from approved sources.
- Uninstall software which is not used.
- Disable unused services.
- Activate a password-protected screen lock on your PC systems.
- Always lock your PC systems as soon as you leave your PC workstation.
- Do not click any links that come from unknown sources. If necessary ask, e.g. on e-mails.
- Use secure access paths such as HTTPS or VPN for remote access to your PC system.

4.2 Installation guidelines

General

The installation guidelines contain information about the interference free deployment of a PLC system. There is the description of the ways, interference may occur in your PLC, how you can make sure the electromagnetic compatibility (EMC), and how you manage the isolation.

What does EMC mean?

Electromagnetic compatibility (EMC) means the ability of an electrical device, to function error free in an electromagnetic environment without being interfered respectively without interfering the environment.

The components are developed for the deployment in industrial environments and meets high demands on the EMC. Nevertheless you should project an EMC planning before installing the components and take conceivable interference causes into account.

Possible interference causes

Electromagnetic interferences may interfere your control via different ways:

- Electromagnetic fields (RF coupling)
- Magnetic fields with power frequency
- Bus system
- Power supply
- Protected ground conductor

Depending on the spreading medium (lead bound or lead free) and the distance to the interference cause, interferences to your control occur by means of different coupling mechanisms.

There are:

- galvanic coupling
- capacitive coupling
- inductive coupling
- radiant coupling

Basic rules for EMC

In the most times it is enough to take care of some elementary rules to guarantee the EMC. Please regard the following basic rules when installing your PLC.

- Take care of a correct area-wide grounding of the inactive metal parts when installing your components.
  - Connect all inactive metal extensive and impedance-low.
  - Please try not to use aluminium parts. Aluminium is easily oxidizing and is therefore less suitable for grounding.
- When cabling, take care of the correct line routing.
  - Organize your cabling in line groups (high voltage, current supply, signal and data lines).
  - Always lay your high voltage lines and signal respectively data lines in separate channels or bundles.
  - Route the signal and data lines as near as possible beside ground areas (e.g. suspension bars, metal rails, tin cabinet).
- Proof the correct fixing of the lead isolation.
  - Data lines must be shielded.
  - Analog lines must be shielded. When transmitting signals with small amplitudes the one sided laying of the isolation may be favourable.
  - Cables for frequency inverters, servo and stepper motors must be shielded.
  - Lay the line isolation extensively on an isolation/protected ground conductor rail directly after the cabinet entry and fix the isolation with cable clamps.
  - Make sure that the isolation/protected ground conductor rail is connected impedance-low with the cabinet.
  - Use metallic or metallised plug cases for isolated data lines.
- In special use cases you should appoint special EMC actions.
  - Consider to wire all inductivities with erase links.
  - Please consider luminescent lamps can influence signal lines.
- Create a homogeneous reference potential and ground all electrical operating supplies when possible.
  - Please take care for the targeted employment of the grounding actions. The grounding of the PLC serves for protection and functionality activity.
  - Connect installation parts and cabinets with your PLC in star topology with the isolation/protected ground conductor system. So you avoid ground loops.
  - If there are potential differences between installation parts and cabinets, lay sufficiently dimensioned potential compensation lines.

Isolation of conductors

Electrical, magnetically and electromagnetic interference fields are weakened by means of an isolation, one talks of absorption. Via the isolation rail, that is connected conductive with the rack, interference currents are shunt via cable isolation to the ground. Here you have to make sure, that the connection to the protected ground conductor is impedance-low, because otherwise the interference currents may appear as interference cause.

When isolating cables you have to regard the following:

- If possible, use only cables with isolation tangle.
- The hiding power of the isolation should be higher than 80%.
- Normally you should always lay the isolation of cables on both sides. Only by means of the both-sided connection of the isolation you achieve high quality interference suppression in the higher frequency area. Only as exception you may also lay the isolation one-sided. Then you only achieve the absorption of the lower frequencies. A one-sided isolation connection may be convenient, if:
  - the conduction of a potential compensating line is not possible.
  - analog signals (some mV respectively µA) are transferred.
  - foil isolations (static isolations) are used.
- With data lines always use metallic or metallised plugs for serial couplings. Fix the isolation of the data line at the plug rack. Do not lay the isolation on the PIN 1 of the plug bar!
- At stationary operation it is convenient to strip the insulated cable interruption free and lay it on the isolation/protected ground conductor line.
- To fix the isolation tangles use cable clamps out of metal. The clamps must clasp the isolation extensively and have well contact.
- Lay the isolation on an isolation rail directly after the entry of the cable in the cabinet.



CAUTION

Please regard at installation!

At potential differences between the grounding points, there may be a compensation current via the isolation connected at both sides.

Remedy: Potential compensation line