SIEMENS

SIMATIC HMI

Industrial Thin Clients ITC V3, ITC V3 PRO

Operating Instructions

View HTML5 version

Preface

Overview 1

Safety instructions 2

Installing and connecting the device 3

Operating the device 4

ITC Operating mode 5

SINUMERIK operating mode 6

Device maintenance and repair 7

Technical specifications 8

Technical Support A

Markings and symbols B

Abbreviations C

Firmware version V3.3

03/2026

A5E42761061-AH

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the application described in the catalog and the associated usage information. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Ⓟ 03/2026 Subject to change

Copyright © Siemens 2026.
All rights reserved

Preface

Purpose of the operating instructions

These operating instructions provide information based on the requirements defined by mechanical engineering documentation for manuals. This information relates to the place of use, transport, storage, mounting, use and maintenance.

These operating instructions are intended for the following user groups:

- Operators
  The following chapters are of relevance:
  - Overview (Page 13)
  - Operating the device (Page 71)
- Administrator
  The following chapters are of relevance:
  - Overview (Page 13)
  - Assigning device parameters (Page 81)
  - Configuring the server (Page 110)
- Commissioning engineers
  The following chapters are of relevance:
  - Overview (Page 13)
  - Installing and connecting the device (Page 42)
  - Configuring the server (Page 110)
- Maintenance personnel
  The following chapters are of relevance:
  - Overview (Page 13)
  - Device maintenance and repair (Page 165)

Chapter Safety instructions (Page 35) must be particularly observed by all user groups.

Basic knowledge required

General knowledge of automation technology and process communication is needed to understand the operating instructions.

Specialist knowledge of SINUMERIK systems are required for the "SINUMERIK" operating mode.

It is also assumed that those using the manual have experience in using personal computers and knowledge of Microsoft operating systems.

Scope of the operating instructions

These operating instructions apply to the following Industrial Thin Client ITC V3 devices in conjunction with firmware version V3.3:

ITC V3 devices 12"

Designation	Type	Display / resolution	Article number, device with Siemens logo	Article number, device without Siemens logo
ITC1200 V3	Built-in unit	12" HD	6AV6646-1BA12-0AA1	6AV6646-1BA12-0NA1
ITC1200 V3 PRO	PRO device for pedestal (extendable, flange bottom)	12" HD	6AV6646-1BB12-0AA1	6AV6646-1BB12-0NA1
ITC1200 V3 PRO	PRO device for support arm (not extendable, flange top)	12" HD	6AV6646-1BC12-0AA1	6AV6646-1BC12-0NA1
ITC1200 V3 PRO	PRO device for support arm (extendable, round tube)	12" HD	6AV6646-1BD12-0AA1	6AV6646-1BD12-0NA1

ITC V3 devices 15"

Designation	Type	Display / resolution	Article number, device with Siemens logo	Article number, device without Siemens logo
ITC1500 V3	Built-in unit	15" HD	6AV6646-1BA15-0AA0	6AV6646-1BA15-0NA0
		15" HD	6AV6646-1BA15-0AA1	6AV6646-1BA15-0NA1
		15" Full HD	6AV6646-1BA16-0AA1	6AV6646-1BA16-0NA1
ITC1500 V3 PRO	PRO device for pedestal (extendable, flange bottom)	15" HD	6AV6646-1BB15-0AA0	6AV6646-1BB15-0NA0
		15" HD	6AV6646-1BB15-0AA1	6AV6646-1BB15-0NA1
		15" Full HD	6AV6646-1BB16-0AA1	6AV6646-1BB16-0NA1
ITC1500 V3 PRO	PRO device for support arm (not extendable, flange top)	15" HD	6AV6646-1BC15-0AA0	6AV6646-1BC15-0NA0
		15" HD	6AV6646-1BC15-0AA1	6AV6646-1BC15-0NA1
		15" Full HD	6AV6646-1BC16-0AA1	6AV6646-1BC16-0NA1
ITC1500 V3 PRO	PRO device for support arm (extendable, round tube)	15" HD	6AV6646-1BD15-0AA0	6AV6646-1BD15-0NA0
		15" HD	6AV6646-1BD15-0AA1	6AV6646-1BD15-0NA1
		15" Full HD	6AV6646-1BD16-0AA1	6AV6646-1BD16-0NA1

ITC V3 devices 19"

Designation	Type	Display / resolution	Article number, device with Siemens logo	Article number, device without Siemens logo
ITC1900 V3	Built-in unit	19" HD	6AV6646-1BA18-0AA0	6AV6646-1BA18-0NA0
		19" HD	6AV6646-1BA18-0AA1	6AV6646-1BA18-0NA1
		19" Full HD	6AV6646-1BA20-0AA1	6AV6646-1BA20-0NA1
ITC1900 V3 PRO	PRO device for pedestal (extendable, flange bottom)	19" HD	6AV6646-1BB18-0AA0	6AV6646-1BB18-0NA0
		19" HD	6AV6646-1BB18-0AA1	6AV6646-1BB18-0NA1
		19" Full HD	6AV6646-1BB20-0AA1	6AV6646-1BB20-0NA1
ITC1900 V3 PRO	PRO device for support arm (not extendable, flange top)	19" HD	6AV6646-1BC18-0AA0	6AV6646-1BC18-0NA0
		19" HD	6AV6646-1BC18-0AA1	6AV6646-1BC18-0NA1
		19" Full HD	6AV6646-1BC20-0AA1	6AV6646-1BC20-0NA1
ITC1900 V3 PRO	PRO device for support arm (extendable, round tube)	19" HD	6AV6646-1BD18-0AA0	6AV6646-1BD18-0NA0
		19" HD	6AV6646-1BD18-0AA1	6AV6646-1BD18-0NA1
		19" Full HD	6AV6646-1BD20-0AA1	6AV6646-1BD20-0NA1

ITC V3 devices 22"

Designation	Type	Display / resolution	Article number, device with Siemens logo	Article number, device without Siemens logo
ITC2200 V3	Built-in unit	22" Full HD	6AV6646-1BA22-1AA0	6AV6646-1BA22-1NA0
		22" Full HD	6AV6646-1BA22-1AA1	6AV6646-1BA22-1NA1
ITC2200 V3 PRO	PRO device for pedestal (extendable, flange bottom)	22" Full HD	6AV6646-1BB22-1AA0	6AV6646-1BB22-1NA0
		22" Full HD	6AV6646-1BB22-1AA1	6AV6646-1BB22-1NA1
ITC2200 V3 PRO	PRO device for support arm (not extendable, flange top)	22" Full HD	6AV6646-1BC22-1AA0	6AV6646-1BC22-1NA0
		22" Full HD	6AV6646-1BC22-1AA1	6AV6646-1BC22-1NA1
ITC2200 V3 PRO	PRO device for support arm (extendable, round tube)	22" Full HD	6AV6646-1BD22-1AA0	6AV6646-1BD22-1NA0
		22" Full HD	6AV6646-1BD22-1AA1	6AV6646-1BD22-1NA1

ITC V3 devices 24"

Designation	Type	Display / resolution	Article number, device with Siemens logo	Article number, device without Siemens logo
ITC2400 V3	Built-in unit	24" Full HD	6AV6646-1BA24-0AA1	6AV6646-1BA24-0NA1
ITC2400 V3 PRO	PRO device for pedestal (extendable, flange bottom)	24" Full HD	6AV6646-1BB24-0AA1	6AV6646-1BB24-0NA1
ITC2400 V3 PRO	PRO device for support arm (not extendable, flange top)	24" Full HD	6AV6646-1BC24-0AA1	6AV6646-1BC24-0NA1
ITC2400 V3 PRO	PRO device for support arm (extendable, round tube)	24" Full HD	6AV6646-1BD24-0AA1	6AV6646-1BD24-0NA1

ID Link for the digital type plate

The ID Link is a unique identifier in accordance with IEC 61406, which you will find in future as a QR code on your product and the product packaging.

You can recognize the ID Link from the frame, which has a black corner at the bottom right. The ID Link takes you to the digital type plate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, a bar code scanner or a Read app. Call the relevant link.

In the digital type plate, you will find product data, manuals, Declarations of Conformity, certificates and other helpful information on your product.

Keeping this documentation

NOTICE
Manual belongs to the HMI device This manual belongs to the HMI device and is also required for recommissioning. Store all supplied and supplementary documentation for the entire service life of the HMI device. Provide all stored documents to subsequent owners of the HMI device.

For digitally attached documentation:

1. After you receive your product, download the relevant documentation, at a time no later than the first assembly/commissioning. Use the following options for the download:
   - Technical Support (https://support.industry.siemens.com):
     The documentation is assigned to the product via the article number. The article number can be found on the product and on the packaging label. Products with new, incompatible functions are given a new article number and documentation.
   - ID Link:
     If your product carries an ID Link, you can recognize it as a QR code having a frame with a black corner at the bottom right. The ID Link takes you to the digital type plate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera or a bar code scanner. Call the relevant ID Link.
2. Keep this version of the documentation.

Brands

The following designations marked with the symbol ® are registered trademarks of Siemens Aktiengesellschaft:

- HMI®
- SIMATIC®
- SINUMERIK®
- WinCC®

Style conventions

The following text notation will facilitate reading this manual:

Text markup	Example	Meaning
Text in quotation marks: "*Text*"	"Add screen"	• Terminology that appears in the user interface, for example dialog names, tabs, buttons, menu commands • Required input, for example, limits, tag values. • Path information
Texts in quotation marks, separated by a greater-than sign: "*Text* > *Text*"	"File > Edit"	Operating sequences, for example, menu commands, shortcut menu commands.
Texts in square brackets: <*Text*>	<F1>, <Alt+P>	Keyboard operation

Please observe notes labeled as follows:

Note

Notes contain important information concerning the product, its use or a specific section of the documentation to which you should pay particular attention.

Naming conventions

Term	Applies to
Device, HMI device, Industrial Thin Client, Panel, TCU	All ITC V3 devices
Built-in unit	All ITC V3 built-in units
PRO device	All ITC V3 PRO devices
HD device	ITC V3 device with HD display
Full HD device	ITC V3 device with Full HD display

The information as to which devices are equipped with HD display or Full HD display can be found in the tables in the section "Scope (Page 3)".

Figures

This manual contains illustrations of the described devices. The figures can deviate from the particularities of the delivered device.

Picture parts are marked with black position numbers on a white background: ①, ②, ③, ...

Work steps within the figures are marked with white process numbers on a black background according to the sequence to be followed: ❶, ❷, ❸, ...

Table of contents

Preface ... **3**

1 Overview ... **13**

1.1 Product description ... 13

1.2 Product package ... 16

1.3 Layout of the devices ... 17
1.3.1 ITC V3 built-in units ... 17
1.3.2 ITC V3 PRO devices ... 19
1.3.2.1 Overview ... 19
1.3.2.2 PRO devices for support arm (not extendable, flange top) ... 20
1.3.2.3 PRO devices for pedestal (extendable, flange bottom) ... 21
1.3.2.4 PRO devices for support arm (extendable, round tube) ... 23
1.3.3 Interfaces ... 24

1.4 System components and accessories ... 25
1.4.1 System components for PRO devices ... 25
1.4.2 Accessories ... 33

2 Safety instructions ... **35**

2.1 General safety instructions ... 35

2.2 Security management for HMI devices ... 37

2.3 Data protection ... 37

2.4 ITC data ... 38

2.5 Notes about usage ... 39

2.6 Use in hazardous areas ... 41

3 Installing and connecting the device ... **42**

3.1 Preparing for installation ... 42
3.1.1 Checking delivery ... 42
3.1.2 Checking the operating conditions ... 43
3.1.3 Built-in units ... 43
3.1.3.1 Permitted mounting positions ... 43
3.1.3.2 Checking clearances ... 44
3.1.3.3 Preparing the mounting cutout ... 45
3.1.3.4 Installing a strain relief ... 46
3.1.4 PRO devices ... 47
3.1.4.1 Permitted mounting positions ... 47
3.1.4.2 Installing a strain relief ... 48

3.2 Installing the built-in unit ... 49
3.2.1 Notes on installation ... 49
3.2.2 Positions of the mounting clips ... 49
3.2.3 Fastening the device with mounting clips ... 51

3.3 Installing a PRO device ... 53
3.3.1 Notes on mounting ... 53
3.3.2 PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom) ... 54
3.3.3 PRO devices for support arm (extendable, round tube) ... 56

3.4 Connecting the device ... 59
3.4.1 Notes on connection ... 59
3.4.2 Equipotential bonding ... 61
3.4.3 Connecting the power supply ... 63
3.4.4 Connecting device to the server ... 65
3.4.5 Connecting a USB device ... 65
3.4.6 Switching the device on, testing it and switching it off ... 67
3.4.7 Securing cables ... 68
3.4.8 Securing cables for use in hazardous areas ... 68

3.5 Removing the device ... 69
3.5.1 Removing the built-in unit ... 69
3.5.2 Removing a PRO device ... 70

4 Operating the device ... 71

4.1 Overview ... 71

4.2 Notes on the capacitive touch screen ... 72
4.2.1 General information ... 72
4.2.2 Operating a device with capacitive multi-touch screen ... 73

5 ITC Operating mode ... 75

5.1 System requirements ... 75

5.2 Typical applications ... 76

5.3 ITC commissioning ... 79

5.4 Interrupting and restoring a connection ... 80

5.5 Assigning device parameters ... 81
5.5.1 Possible applications ... 81
5.5.2 Opening the configuration ... 81
5.5.3 The "All" menu ... 83
5.5.4 The "Information" submenu ... 84
5.5.5 The "System" submenu ... 85
5.5.6 The "Network" submenu ... 91
5.5.7 The "Connections" submenu ... 94
5.5.7.1 Setting up client-server connections ... 95
5.5.7.2 Connection settings ... 96
5.5.7.3 Setting up startup connection ... 100
5.5.7.4 PROFINET basic functions ... 100
5.5.8 The "Passwords" submenu ... 101
5.5.9 The "Desktop" submenu ... 104
5.5.10 The "Programs" submenu ... 106
5.5.11 Remote configuration ... 109

5.6 Configuring the server ... 110
5.6.1 RDP ... 110
5.6.1.1 RDP overview ... 110
5.6.1.2 Administration on the server ... 111
5.6.2 Citrix ... 112
5.6.2.1 Citrix overview ... 112
5.6.2.2 Connecting to a Citrix application or a desktop ... 113
5.6.2.3 Restrictions ... 114
5.6.3 VNC ... 115
5.6.4 Sm@rtServer ... 115
5.6.5 WinCC OA ... 116

5.7 Operating ITC ... 117
5.7.1 Notes on Sm@rtServer access ... 117
5.7.2 Operating the taskbar ... 117
5.7.2.1 Structure and functions of the taskbar ... 117
5.7.2.2 Starting a connection ... 119
5.7.2.3 Changing from one connection to another ... 120
5.7.2.4 Terminating a connection ... 120
5.7.3 Operating the on-screen keyboard ... 121
5.7.4 Use USB memory devices ... 123
5.7.5 Using a USB reader ... 124

6 SINUMERIK operating mode ... 125

6.1 SINUMERIK commissioning ... 125

6.2 Networking ... 127
6.2.1 System settings ... 127
6.2.1.1 Thin Client Unit (TCU) ... 127
6.2.1.2 Settings for SINUMERIK solution line ... 128
6.2.1.3 System boot with system network ... 129
6.2.1.4 Factory default settings ... 130
6.2.2 Commissioning TCU ... 133
6.2.2.1 Key assignment ... 133
6.2.2.2 Settings in the "TCU.ini" file ... 134
6.2.2.3 Displacement mechanism for TCUs ... 135
6.2.2.4 Disable switchover between TCU via PLC ... 136
6.2.2.5 Example: How to select the behavior of the TCUs during boot up ... 138
6.2.3 Network configuration ... 139
6.2.3.1 Permissible network topologies ... 139
6.2.3.2 Networks without connection to the company network ... 140
6.2.3.3 Networks with NCU connection to the company network ... 141
6.2.3.4 Example: Configuring a VNC connection to a PC ... 143
6.2.4 Service and diagnostics ... 145
6.2.4.1 Using the TCU's main menu ... 145
6.2.4.2 Operating the TCU menu "Service sessions" ... 148
6.2.4.3 Operating the TCU menu "Service menu" ... 150
6.2.4.4 Operating the TCU menu "Modify settings" ... 153
6.2.4.5 Operating the menu for a new TCU or spare part TCU ... 155
6.2.4.6 How to register a TCU on the system network ... 160
6.2.4.7 This is how you register a spare part TCU ... 162
6.2.4.8 Booting of the TCU ... 163

7 Device maintenance and repair ... 165

7.1 General information on maintenance and servicing ... 165

7.2 Cleaning the device ... 165

7.3 Spare parts and repairs ... 166

7.4 Recycling and disposal ... 166

8 Technical specifications ... 167

8.1 Labels, certificates and approvals ... 167

8.2 Electromagnetic compatibility ... 175

8.3 Mechanical environmental conditions ... 176
8.3.1 Storage conditions ... 176
8.3.2 Operating conditions ... 177

8.4 Climatic ambient conditions ... 177
8.4.1 Transport and storage conditions ... 177
8.4.2 Operating Conditions ... 178

8.5 Information on insulation tests, protection class and degree of protection ... 178

8.6 Dimensional drawings ... 180
8.6.1 ITC1200 V3 ... 180
8.6.2 ITC1500 V3 ... 181
8.6.3 ITC1900 V3 ... 182
8.6.4 ITC2200 V3 ... 183
8.6.5 ITC2400 V3 ... 184
8.6.6 ITC1200 V3 PRO ... 185
8.6.7 ITC1500 V3 PRO ... 188
8.6.8 ITC1900 V3 PRO ... 191
8.6.9 ITC2200 V3 PRO ... 194
8.6.10 ITC2400 V3 PRO ... 197

8.7 Technical specifications ... 200
8.7.1 ITC1200/1500 V3 (PRO) ... 200
8.7.2 ITC1900/2200/2400 V3 (PRO) ... 202

8.8 Description of the ports ... 204
8.8.1 Power supply ... 204
8.8.2 PROFINET (LAN), LAN - 10/100/1000 MBit ... 204
8.8.3 USB ... 205

8.9 Performance data ... 205

A Technical Support ... 206

A.1 Service and support ... 206

A.2 Application examples and FAQs ... 207

B Markings and symbols ... 208

B.1 Safety-relevant symbols ... 208

C Abbreviations ... 210

Glossary ... 212

Overview

1

1.1 Product description

SIMATIC ITC - the high-performance local thin client solution

Industrial Thin Clients are low-cost HMI terminals that provide local HMI functionality in plants spread over large areas. In this way, Industrial Thin Clients contribute to an improved overview, operability, and productivity of plants. In addition, the Industrial Thin Clients also reduce the total cost of ownership (TCO) by virtue of their extremely easy commissioning, efficient Ethernet networking, reduced software costs, and minimal service costs.

The Industrial Thin Client itself requires no installation and no licenses to operate. You can also bridge greater distances via Ethernet.

The Industrial Thin Client offers the following operating modes. The operating mode is defined as part of first commissioning.

- ITC Operating mode
- SINUMERIK operating mode

ITC Operating mode

In the ITC operating mode, the Industrial Thin Client always communicates with a host, such as an HMI device, industrial PC, or server, via the following connection types:

- Web browser functionality
- SIMATIC WinCC Sm@rtServer
- Standard RDP (Remote Desktop Protocol) from Microsoft
- VNC (Virtual Network Computing)
- On-demand application service from Citrix
- WinCC OA

You can do the following from the Industrial Thin Client:

- Display and run web-based content from a web server available on the network (e.g., S7 controller, Intranet/Internet) via the integrated web browser.
- Run WinCC projects on other HMI devices or industrial PCs via Sm@rtServer.
- Run HMI applications (e.g., WinCC), Office applications (e.g., Excel), or SAP directly at the machine via RDP.
- Operate a PC remotely with VNC (similar to RDP).
- Access a Citrix server as Citrix client.
- Access a WinCC OA server as client.

You will find the description of the ITC operating mode in Section "ITC Operating mode (Page 75)".

SINUMERIK operating mode

In SINUMERIK operating mode, the Industrial Thin Client behaves like a SINUMERIK operator panel face with built in Thin Client Unit TCU.

You will find the description of the SINUMERIK operating mode in Section "SINUMERIK operating mode (Page 125)".

Features

Installation compatibility

The Industrial Thin Client built-in units are compatible with SIMATIC Industrial PCs, Industrial Flat Panels, HMI devices and SINUMERIK TOP Panels of the same series.

Front

- Integrated glass front, anti-reflective coating, resistant to scratches and chemicals
- Brilliant 12"-, 15"-, 19"-, 22"- or 24" TFT display with 16 million colors

Touch screen

- Capacitive touch screen
- Suitable for operation with glove, pen and finger
- Detection of accidental contact

IP65 fully-enclosed

The Thin Client PRO with an IP65 protection class housing features all-round dust- and hose water protection. The ready-to-use HMI device can be mounted either from the top or the bottom to a support arm system or to a pedestal.

A basic adapter and adapter sets that can be ordered separately support mounting systems from various manufacturers (including VESA standard for flat screens). The rear panel can be easily opened. The interfaces of the HMI device can therefore be reached without problem. Special cables or plugs are not required.

The Thin Client PRO is impressive not only on account of its ease of servicing but also due to its sophisticated design and slimline device depth.

Easy commissioning

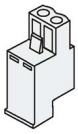
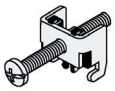
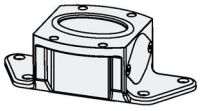
The Industrial Thin Client merely requires an IP address. For fast on-site commissioning and diagnostics, the SIMATIC ITC is equipped with a Setup Wizard optimized for touch operation. Local software installation on the device is not necessary. The display and user interface of the application are provided by the host.

High robustness

As a remote operator terminal without any rotating media (hard drive or fan), you can operate the Industrial Thin Client on machines having stringent requirements for mechanical robustness.

1.2 Product package

The following components are included in the scope of delivery of the device:

Designation	Figure		Quantity
HMI device			1
Installation instructions (Quick Installation Guide)			1
Power supply connector			1
Mounting clips with screw		Steel mounting clip, captive For built-in units	12
Strain relief bracket		For built-in units	1
		For PRO devices	1
Basic adapter		Only for PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom)	1
Cover for mechanical interface including screw kit		Only for PRO devices for support arm (extendable, round tube)	1

Some components of the product package are also available separately, see section "System components and accessories (Page 25)".

1.3 Layout of the devices

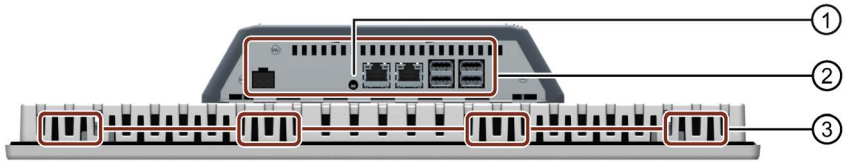
1.3.1 ITC V3 built-in units

The following figures show the structure of the Industrial Thin Clients using an example of the SIMATIC ITC1900 V3 built-in units with Siemens logo.

Front view and side view

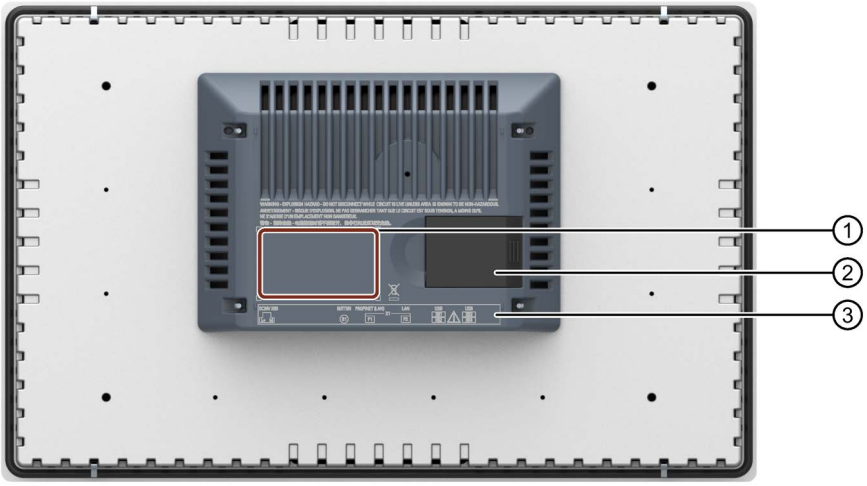
① Capacitive touch screen
② Recesses for mounting clips
③ Mounting seal

Bottom view



① "Factory settings" button
② Interfaces
③ Recesses for mounting clips

Rear view



① Rating plate
② Cover
③ Interface designation

1.3.2 ITC V3 PRO devices

1.3.2.1 Overview

The PRO devices are available in the following variants. The figures show examples.

- **PRO devices for support arm (not extendable, flange top)**

  These devices are designed for mounting on a support arm without extensions such as Extension Units. If required, the PRO Option handles can be used between the support arm and the device.

- **PRO devices for pedestal (extendable, flange bottom)**

  These devices are designed for mounting on a pedestal with extensions such as Extension Units. If required, the PRO Option handles can be used between the pedestal and the device.

- **PRO devices for support arm (extendable, round tube)**

  These devices are designed for mounting on a support arm with extensions such as Extension Units or PRO Options (e.g. handles, keyboard tray).

Additional information on the PRO Options as well as adapters and other system components can be found in the section "System components for PRO devices (Page 25)".

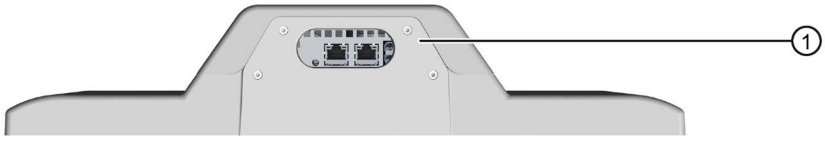
1.3.2.2 PRO devices for support arm (not extendable, flange top)

The following figures show the structure of the devices using the example of the ITC2200 V3 PRO for support arm (not extendable, flange top) with Siemens logo.

Front view and side view

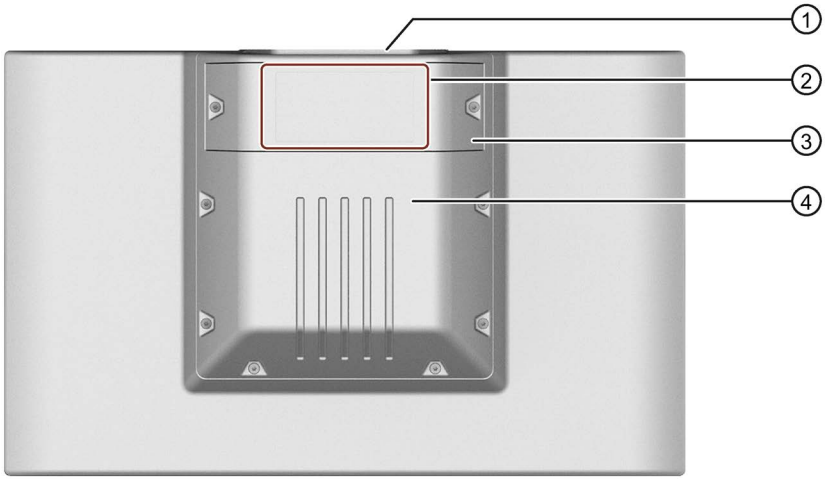
① Display with touch screen
② Enclosure
③ Backplane cover

Top view



① Mechanical interface for fastening

Rear view



① Mechanical interface for fastening
② Rating plate
③ Terminal compartment cover
④ Backplane cover

1.3.2.3 PRO devices for pedestal (extendable, flange bottom)

The following figures show the structure of the devices using the example of the ITC2200 V3 PRO for pedestal (extendable, flange bottom) with Siemens logo.

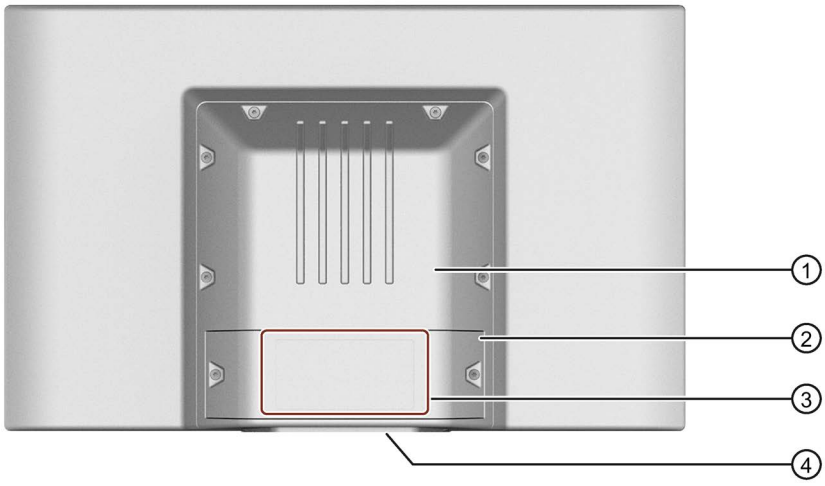
Front view and side view

① Display with touch screen
② Enclosure
③ Backplane cover

Bottom view

① Mechanical interface for fastening

Rear view



① Backplane cover
② Terminal compartment cover
③ Rating plate
④ Mechanical interface for fastening

1.3.2.4 PRO devices for support arm (extendable, round tube)

The following figures show the structure of the devices using the example of the ITC1500 V3 PRO for support arm (extendable, round tube) with Siemens logo.

Front view and side view

① Display with touch screen
② Enclosure
③ Mechanical interface for fastening (round tube)
④ Terminal compartment cover
⑤ Mechanical interface below

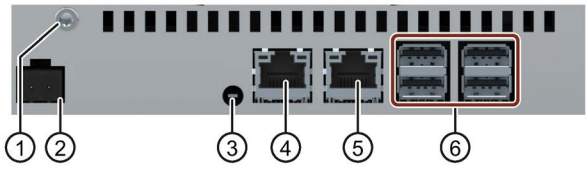
Rear view

① Mechanical interface for fastening (round tube)
② Terminal compartment cover
③ Rating plate
④ Mechanical interface below
⑤ Lower cover, included in the product package

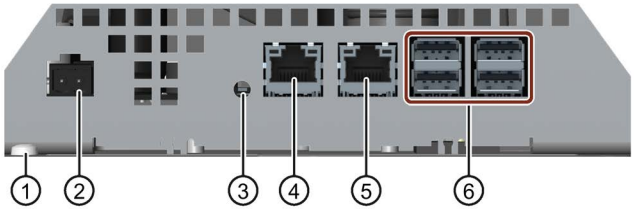
1.3.3 Interfaces

The following figures show the interfaces of the ITC V3 devices.

Built-in units



PRO devices



① Functional grounding connection
② X80 power supply connector
③ B1 "Factory settings" button
④ X1 P1 PROFINET (LAN), 10/100/1000 MBit
⑤ X1 P2 LAN, 10/100/1000 MBit
⑥ X61 ... X64 USB Type A

1.4 System components and accessories

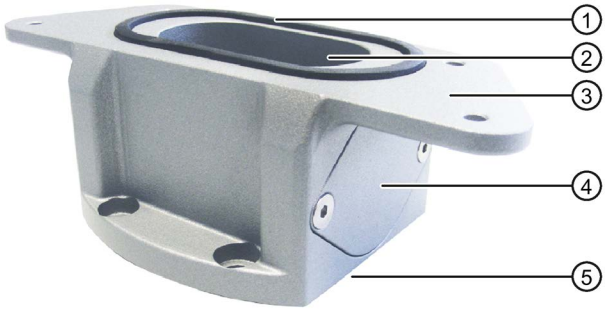
System components are products that have been developed for a specific system and can not be used in general, for example, like the base adapter. System components are always directly related to a core product.

Accessories can typically be used for multiple devices from the same or different device families, for example, batteries, touch pens or protective membranes.

1.4.1 System components for PRO devices

Base adapter

Using the base adapter, mount PRO devices for support arm (not extendable, flange top) or for pedestal (extendable, flange bottom) on the support arm or pedestal. A base adapter is included in the scope of delivery for the corresponding PRO device. The base adapter can also be ordered separately.



① Seal
② Channel cable
③ Mechanical interface to the PRO device
④ Cover
⑤ Mechanical interface to the support arm or pedestal including seal

Article number: 6AV7674-1KA00-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/32109730).

Adapter sets and couplings

For mounting a PRO device for support arm (not extendable, flange top) or for pedestal (extendable, flange bottom) using the base adapter, the following adapter sets are available additionally:

- Adapter set VESA75 for VESA75-compatible systems, article number 6AV7674-0KE00-0AA0

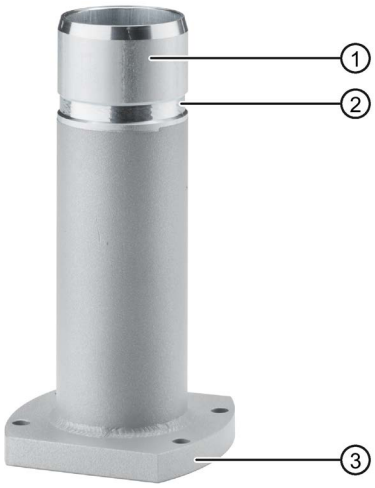
- Adapter set VESA100 for VESA100-compatible systems, article number 6AV7674-0KD00-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/32109730).

In addition, other manufacturers are offering support arm or pedestal systems with mechanical interface or adapter for Siemens PRO devices, for example, RITTAL, ROLEC, BERNSTEIN, HASEKE, ROSE. Observe the technical specifications of the respective manufacturer.

Flange mount adapter

A flange mount adapter is available for mounting a PRO device for support arm (extendable, round tube).



① Flange mount adapter
② Ring groove for fastening on PRO device with setscrews
③ Mechanical interface to support arm

Article number: 6AV7674-1KF00-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/32109730).

Round tube plug

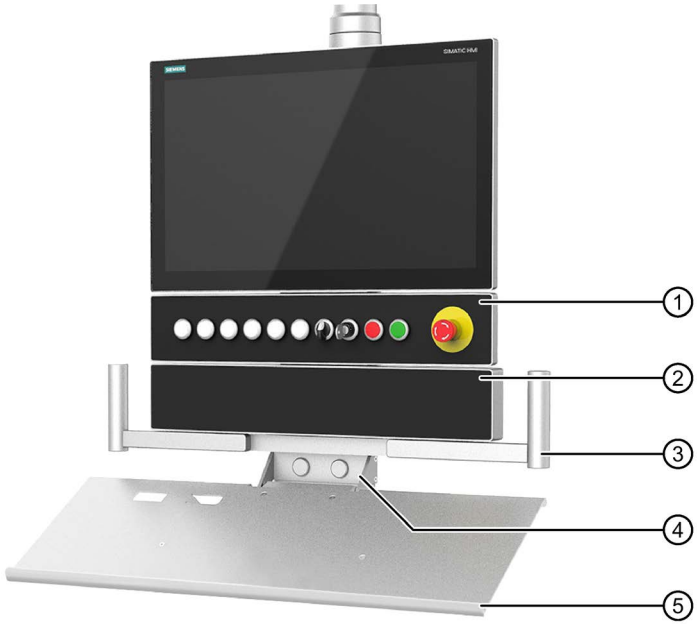
If you do not need the mechanical interface of a PRO device for support arm (extendable, round tube) you can install the round tube plug into the mechanical interface. With the round tube plug, the degree of protection IP65 is maintained all around for the PRO device.

Article number: 6AV7674-1LB40-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109769784).

Extensions for PRO devices

The following example shows a PRO device for a support arm (extendable, round tube) with Extension Unit, Extension Unit box as well as the PRO Options Handles and Keyboard tray with Keyboard tray plate.



① **Extension Unit**, example of an Extension Unit 22" with eight operator controls and emergency stop button

② **Extension Unit box**, deep empty enclosure, example Extension Unit box 22" without operator controls

③ **Handles**, set matching the 22" device

④ **Keyboard tray** for mounting the keyboard tray plate or installing a suitable keyboard

⑤ **Keyboard tray plate**

Mounting options

The handles can be mounted above a PRO device of type "not extendable" or below a PRO device of type "extendable".

Extension Units and keyboard tray can only be mounted below a PRO device of the "extendable" type.

Note

A maximum of two Extension Units is permitted

A maximum of two Extension Units are permitted below a PRO device for pedestal (extendable, flange bottom) or for support arm (extendable, round tube) and can be configured in TIA Portal.

Extension Unit

The Extension Unit is used to install additional operator controls below a SIMATIC PRO device for pedestal (extendable, flange bottom) or for support arm (extendable, round tube).

The Extension Unit can be customized and is supplied without operator controls. The front of the Extension Unit has pre-perforated slots for operator controls. The Extension Unit is available in four sizes:

- Extension Unit 12", article number 6AV7674-1LA3x-0AA0
- Extension Unit 15", article number 6AV7674-1LA4x-0AA0
- Extension Unit 19", article number 6AV7674-1LA5x-0AA0
- Extension Unit 22", article number 6AV7674-1LA6x-0AA0
- Extension Unit 24", article number 6AV7674-1LA7x-0AA0

In each size, you have the flexibility to choose between the following Extension Unit interface variants (x) for connection to the plant:

- Hardwired (x=1)
- PROFINET (x=2)
- PROFIsafe (x=3)

In addition, different operator controls, such as Emergency Stop pushbutton, selector switch, illuminated pushbutton, keyswitch or indicator light are available.

Note

Only operator controls with Siemens approval may be installed in the Extension Unit.

You can find detailed information in the corresponding operating instructions on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742323).

Extension Unit Advanced

The Extension Unit Advanced can be ordered pre-configured or customer-specific in numerous variants and is mounted below a SIMATIC PRO device for pedestal (extendable, flange bottom) or for support arm (extendable, round tube).

The Extension Unit Advanced for PROFINET or PROFIsafe connections is available with one or more KP12 keypads. Free slots can be equipped with Standard/Advanced and Safety operator controls.

Note

Only operator controls with Siemens approval may be installed in the Extension Unit.

Extension Units Advanced minimum configuration with 1 x KP12 for PROFINET:

- Extension Unit 12" KP12 PN, article number 6AV2185-8CE01-0AA0
- Extension Unit 15" KP12 PN, article number 6AV2185-8DE01-0AA0
- Extension Unit 19" KP12 PN, article number 6AV2185-8EE01-0AA0
- Extension Unit 22" KP12 PN, article number 6AV2185-8FE01-0AA0

Extension Units Advanced maximum configuration with several KP12 for PROFINET:

- Extension Unit 12" KP24 PN, 2 x KP12, article number 6AV2185-8CE08-0AA0
- Extension Unit 15" KP36 PN, 3 x KP12. article number 6AV2185-8DE08-0AA0
- Extension Unit 19" KP36 PN, 3 x KP12, article number 6AV2185-8EE08-0AA0
- Extension Unit 22" KP48 PN, 4 x KP12, article number 6AV2185-8FE08-0AA0

Extension Units Advanced with 1 x KP12 for PROFINET/PROFIsafe:

- Extension Unit 12" KP12F PN, article number 6AV2185-8CF01-0AA0
- Extension Unit 15" KP12F PN, article number 6AV2185-8DF01-0AA0
- Extension Unit 19" KP12F PN, article number 6AV2185-8EF01-0AA0
- Extension Unit 22" KP12F PN, article number 6AV2185-8FF01-0AA0

In addition, customer-specific Extension Units Advanced can be ordered in various pre-configured expansion stages with operator controls.

You can find detailed information in the corresponding operating instructions on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109756068).

Extension Unit box

The Extension Unit box offers an empty enclosure for installation of larger customer-specific components below a 16:9 SIMATIC PRO device for pedestal (extendable, flange bottom) or for support arm (extendable, round tube).

The Extension Unit is supplied without operator controls; the front has not been prepared for installation of operator controls. The Extension Unit box is available in four sizes:

- Extension Unit box 12", article number 6AV7674-1LA30-0AA0
- Extension Unit box 15", article number 6AV7674-1LA40-0AA0
- Extension Unit box 19", article number 6AV7674-1LA50-0AA0
- Extension Unit box 22", article number 6AV7674-1LA60-0AA0
- Extension Unit box 24", article number 6AV7674-1LA70-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109761025).

Handles

The width of the handles can be adjusted so that the entire device can be aligned or positioned without having to touch the display of the PRO device.

Article number: 6AV7674-1LB10-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109761024).

Keyboard tray

You can mount the keyboard tray plate or a matching keyboard to the keyboard tray. In addition, the keyboard tray has two openings for USB interfaces on the front and two openings for cable glands in the rear.

Article number: 6AV7674-1NF01-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109761024).

Keyboard tray plate

The keyboard tray plate has sufficient space for the keyboard and the mouse.

Article number: 6AV7674-1NG00-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109761024).

Replacement adapter

The Replacement adapter simplifies the dismantling and mounting of a Extension Unit, that are mounted below a SIMATIC PRO device of the "extendable" type .

Article number: 6AV7674-1LB50-0AA0

You can find the associated documentation on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109769845).

Additional information

You can find additional information on system components for fully-enclosed IP65 and Type 4X/12 protected devices on the Internet (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10268745).

1.4.2 Accessories

An accessory kit with the necessary accessories is included with the HMI device.

Note

This section includes a selection of accessories suited to your operator control. You can find additional versions of this selection and the full range of accessories for HMI devices in the Industry Mall on the Internet (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10144445). Details such as the delivery quantity and technical specifications of accessories can be found in the Industry Mall under the respective article numbers.

You can find an overview of the status and compatibility of the accessories portfolio in the "Cross-List" on the Internet (https://support.industry.siemens.com/cs/ww/en/view/40466415).

HMI I/O components

Designation	Article number
Plug for the power supply of the HMI device, 2-pole, screw terminals	6AV6671-8XA00-....
Plug for the power supply of the HMI device, 2x2-pole, spring-type terminals	6ES7193-4JB00-....

"...." stands for the variant key of the article number.

Protective films

Designation	Article number
Protective film 12" front, for built-in units *	6AV6881-0MJ22-....
Protective film 15" front, for built-in units and PRO devices	6AV6881-0QJ22-....
Protective film 19" front, for built-in units and PRO devices	6AV6881-0UJ22-....
Protective film 22" front, for built-in units and PRO devices	6AV6881-0VJ22-....
Protective film 24" front, for built-in units and PRO devices	6AV6881-0WJ22-....

* Protective film requires trimming for use with 12" PRO device
"...." stands for the variant key of the article number.

Storage media

Use only the following storage media for the HMI device.

Designation	Article number
SIMATIC HMI USB stick	6AV6881-0AS42-....

"...." stands for the variant key of the article number.

Fasteners

Designation	Article number
Set with steel mounting clips	6AV6881-6AD10-0AA0

Adapter frames

Designation	Article number
Adapter frame widescreen 15"	6AV6881-6QD41-....
Adapter frame widescreen 19"	6AV6881-6UD41-....
Adapter frame widescreen 22"	6AV6881-6VD41-....

"...." stands for the variant key of the article number.

Input help

Designation	Article number
Touch pen systems ELO and V2A	6AV6881-0AV2.-....

"...." stands for the variant key of the article number.

INOX frame systems

In combination with an INOX frame and a protective film, the degree of protection of the built-in unit can be increased to IP69. With the INOX frame and an antibacterial protective film, which at the same time offers conditional splinter protection, you can use the HMI device in some areas of the food and beverage industry or the pharmaceutical industry, for example.

You can find more information and important tips on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109806812).

Other accessories

Additional USB accessories can be found on the Internet in the following entry:
FAQ 19188460 (https://support.industry.siemens.com/cs/ww/en/view/19188460).

Safety instructions 2

2.1 General safety instructions

The device is designed for use in the industrial sector for operating and monitoring plant processes.

Observe the safety and accident prevention instructions applicable to your application in addition to the safety information given in the device documentation.

Safety of the plant or system

NOTICE
The planner is responsible for the safety. The safety of the plant or system into which the device is integrated is the responsibility of the plant or system planner.

Safety instructions for built-in units

⚠ WARNING
The rear of the device constitutes open equipment. The rear of the device constitutes open equipment. This means that the device may only be installed in an enclosure or cabinet which provides front access for operating the device. The enclosure or the cabinet must provide protection against electric shock and the spread of fire. The enclosure or the cabinet must meet the requirements for mechanical strength and the degree of protection for the relevant application. Access to the enclosure or cabinet in which the device is installed should only be possible by means of a key or tool and for trained and authorized personnel. **Electrocution risk when control cabinet is open** When you open the control cabinet, there may be a dangerous voltage at certain areas or components. If you touch these areas or components, you may be killed by electric shock. Disconnect the cabinet from the mains before opening it. Do **not** plug in or pull out the system component during operation.

Safety instructions for PRO devices

WARNING

The device must be mounted on a suitable support arm or pedestal

If the device is not mounted, mounted improperly or mounted on an unsuitable support arm system or pedestal system, liquids, dust or gases can enter the device. This can result in malfunctions which could cause death or serious injuries.

The device is only considered enclosed equipment and only fulfils the specified degree of protection or Enclosure Type when it is connected in line with the stipulations in this document to a suitable support arm system or pedestal system which also fulfils the required degree of protection or Enclosure Type.

Operation of the device is only permitted when the device is secured to a suitable support arm system or pedestal system in line with the stipulations in these operating instructions. All connection cables of the HMI panel must be routed through the support arm or pedestal.

If the device is extended by optional system components, then the system components must also meet the required degree of protection or enclosure type. Observe the technical specifications of the system components.

ESD

An electrostatically sensitive device is equipped with electronic components. Due to their design, electronic components are sensitive to overvoltage and thus to the discharge of static electricity. Note the corresponding regulations when handling ESD.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (https://www.siemens.com/cert).

Disclaimer for third-party software updates

This product includes third-party software. Siemens Aktiengesellschaft only provides a warranty for updates/patches of the third-party software if these have been distributed as part of a Siemens Software Update Service contract or officially released by Siemens Aktiengesellschaft. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (https://support.industry.siemens.com/cs/ww/en/view/109759444).

Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

2.2 Security management for HMI devices

You can find additional information on security management of HMI devices on the Internet at the following address:

Panel Security Guidelines (https://support.industry.siemens.com/cs/de/en/view/109481300)

2.3 Data protection

Siemens observes the data protection guidelines, especially the requirements regarding data minimization (privacy by design). This means the following for this SIMATIC product: The product does not process / save any personal information, but only technical functional data (e.g. time stamps). If the user links this data to other data (e.g. shift plans) or if the user saves personal information on the same medium (e.g. hard disk) and therefore creates a personal reference in the process, the user has to ensure meeting the guidelines regarding data protection.

Remote maintenance is not recommended for production and should be disabled before production is started.

The remote maintenance settings are disabled by default. If you enable them for maintenance purposes, disable the remote maintenance settings once again for production in the start menu "Configuration > System", "Remote maintenance" (see configuration settings, section "The "System" submenu (Page 85)").

2.4 ITC data

The EU Data Act, a key component of the European data strategy, went into effect on January 11, 2024.

The following information provides you with an overview of the data that an Industrial Thin Client can generate and the information you need to keep in mind.

Type, format and estimated scope of the data

Type of data	Formats	Estimated scope	Storage location		Storage duration
Configuration settings	Text format	Approx. 100 KB	SSD	Internal	Permanent
			USB storage medium	External medium	Permanent

Continuous and real-time data generation

An Industrial Thin Client is not able to generate data continuously and in real time.

Remote data storage

The Industrial Thin Client **does not** store the generated data on another device or another remote server.

Accessing/retrieving the data

The following table shows how the users can access and retrieve the data. Depending on the type of data, the access takes place on the device

Type of data	Access/retrieval via	Terms of use	Quality of service
Configuration settings	Start menu	Authentication	Direct access to the device, password

Deleting data

To delete all data on the Industrial Thin Client, reset the device to the factory settings; see section "The "System" submenu (Page 85)".

2.5 Notes about usage

NOTICE
The HMI device is approved for indoor use only The HMI device may be damaged if it is operated outdoors. Operate the HMI device only indoors ("Indoor use only").

Note

Operate the device only in a normal atmospheric environment

The technical characteristics of the device described in the operating instructions are guaranteed if you operate the device in normal ambient air conditions with usual air composition.

Note

The device is intended for operation on a SELV/PELV circuit according to IEC/EN 61131-2 or IEC/EN UL 61010-2-201 in a dry environment. For the different device types, this means:

- Built-in units: A dry environment at the rear of the device
- PRO devices: A dry environment inside the enclosure

You can find additional information in the section "Operating Conditions (Page 178)".

Industrial applications

The HMI device is designed for industrial applications. It conforms to the following standards:

- Requirements for interference emission EN 61000-6-4:2019
- Requirements for interference immunity EN 61000-6-2:2019

Use in mixed-use zone

Under certain circumstances, you can use the HMI device in a mixed-use zone. A mixed-use zone is used for housing and commercial operations that do not have a significant impact on residents.

When you use the HMI device in a mixed-use zone, you must ensure that the limits of the generic standard EN 61000-6-3 regarding emission of radio frequency interference are observed. Suitable measures for achieving these limits for use in a mixed-use zone include:

- Installation of the HMI device in grounded control cabinets
- Use of filters in electrical supply lines

Individual acceptance is required.

Use in residential areas

Note

HMI device not intended for use in residential area

The HMI device is not intended for use in residential areas. Operation of an HMI device in residential areas can have a negative influence on radio or TV reception.

Use with additional measures

The HMI device should not be used at the following locations unless additional measures are taken:

- In locations with a high degree of ionizing radiation
- In locations with severe operating conditions, for example, due to:
  - Corrosive vapors, gases, oils or chemicals
  - Strong electrical or magnetic fields of high intensity
- In systems that require special monitoring, for example, in:
  - Elevators
  - Systems in especially hazardous rooms

TFT displays

NOTICE

Burn-in effect

A permanently displayed picture of two or more colors can result in a burn-in effect, i.e. the image remains slightly visible for a certain time even on a blank screen. The longer the image has been burned in, the longer the image remains. In an extreme case, the image is displayed permanently.

The ghost image usually disappears by itself if the screen remains off for a long period or the screen content changes, for example, when the screen saver is activated. Screen savers for the backlit active black mode reduce the burn-in effect.

- Activate a screen saver on the server.

Backlighting

The brightness of the backlighting decreases incrementally during its operating period. You can extend the life of the display and backlight by taking the following measures:

- Reduce the backlighting, see section "The "System" submenu (Page 85)".
- Observe the operating period of the backlighting, see section "Technical specifications (Page 200)".

2.6 Use in hazardous areas

The following warnings apply to operating a device with Ex approval in hazardous areas.

WARNING

Do not plug or pull connectors in potentially explosive atmospheres

If you plug in or pull out connecting plugs during operation, there is a risk of sparkover. An explosion can be triggered in the hazardous area due to sparkover, and death or serious physical injury can occur.

Plugging or pulling connecting plugs, such as a 24 V DC power supply plug, is **prohibited** in a potentially explosive atmosphere.

Only plug or pull a connecting plug when one of the following two conditions is met: The area is no longer hazardous or the device and its plug-in connections are de-energized.

To switch off the device, close all open programs or the current project, and switch off the power to the device.

WARNING

USB devices

USB interfaces are not permitted to connect with USB devices except for equipment with USB cable connection.

Note for using the HMI device within the scope of UL approval:

WARNING

Explosion Hazard

Do not disconnect while circuit is live unless area is known to be non-hazardous. Substitution of components may impair suitability for Class I, II, III, Division 2, or Zone 2/22.

Risque d'Explosion

Ne pas déconnecter pendant que le circuit est sous tension, sauf si la zone est non-dangereuse. Le remplacement de composants peut compromettre leur capacité à satisfaire à la Classe I, II, III, Division 2, ou Zone 2/22.

Also read the enclosed documentation for use in potentially explosive atmospheres and the information in the section "Labels, certificates and approvals (Page 167)".

Installing and connecting the device 3

3.1 Preparing for installation

Points to observe when selecting the mounting location:

- Position the HMI device so that it is not subjected to direct sunlight.
- Position the HMI device such that it is ergonomically accessible for the operator. Choose a suitable mounting height.
- Note the permissible mounting positions.

3.1.1 Checking delivery

Check the package content for visible signs of transport damage and for completeness.

Note

Damaged parts

A damaged part will cause the HMI device to malfunction.

Do not install parts damaged during shipment. In the case of damaged parts, contact your Siemens representative.

Check the scope of supply of the HMI device (see Product package (Page 16)).

Additional documents may be included in the delivery.

The documentation is part of the HMI device and is required for subsequent commissioning. Keep all enclosed documentation for the entire service life of the HMI device. You must pass along the enclosed documentation to any subsequent owner or user of the HMI device. Make sure that every supplement to the documentation that you receive is stored together with the operating instructions.

3.1.2 Checking the operating conditions

Note the following aspects before installing the HMI device:

1. Familiarize yourself with the standards, approvals, EMC parameters and technical specifications for operation of the HMI device. This information is available in the following sections:
   - Labels, certificates and approvals (Page 167)
   - Electromagnetic compatibility (Page 175)
2. Check the mechanical and climatic ambient conditions for operation of the HMI device:
   - Mechanical environmental conditions (Page 176)
   - Climatic ambient conditions (Page 177)

3.1.3 Built-in units

3.1.3.1 Permitted mounting positions

Mounting position

The device is suitable for installation in:

- Mounting cabinets
- Control cabinets
- Switchboards
- Consoles

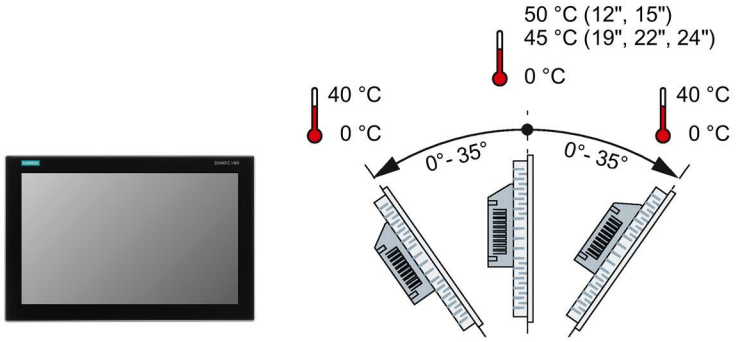
In the following, all of these mounting options are referred to by the general term "control cabinet".

The device is self-ventilated and may be installed up to an angle of +/-35° to the vertical.

NOTICE
Damage due to overheating An inclined installation reduces the convection by the device and therefore the maximum permitted ambient temperature for operation. If there is sufficient convection from forced ventilation, the HMI device can also be operated in the inclined mounting position up to the maximum permitted ambient temperature for vertical installation. The HMI device may otherwise be damaged and its certifications and warranty will be void. The operating temperature ranges specified in this section apply to the rear and front of the HMI device.

For detailed information regarding the permitted ambient temperatures, refer to section "Climatic ambient conditions (Page 177)".

Mounting in landscape format

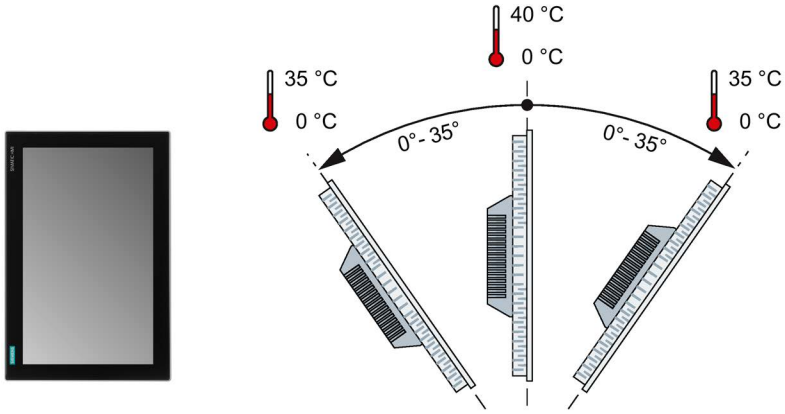


Mounting in portrait format

Note

Portrait format must also be supported by the software

Only install the HMI device in portrait format when the software used supports portrait format.



3.1.3.2 Checking clearances

The following clearances around the device are required:

- Above and below the mounting cutout for ventilation purposes: 50 mm each
- Keep 15 mm free to the right and left of the mounting cutout for inserting the mounting clips.
- At least 10 mm behind the rear panel of the device. The device depth in the control cabinet is 73.1 mm.

Note

Ensure compliance with the permissible ambient temperature when the device is installed in a cabinet and especially in a closed enclosure.

3.1.3.3 Preparing the mounting cutout

Note

Stability of the mounting cutout

The material in the area of the mounting cutout must provide sufficient strength to guarantee the enduring and safe mounting of the HMI device.

The force of the mounting clips or operation of the device may not lead to deformation of the material in order to achieve the degrees of protection described below.

Degrees of protection and installation area

The degrees of protection of the HMI device can only be guaranteed if the following requirements are met:

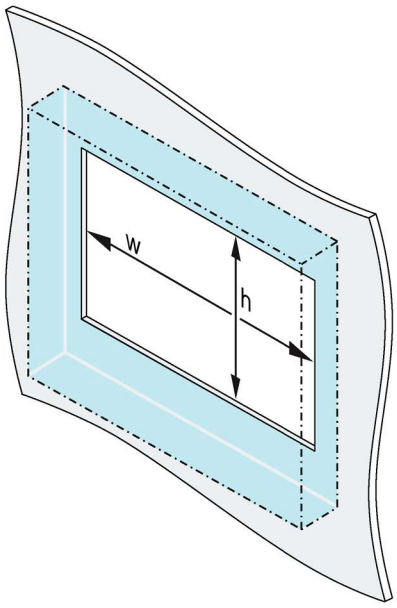
- Material thickness at the mounting cutout for degree of protection IP65 or Type 4X/12 (indoor use only, front face only): 2 mm to 6 mm
- Permitted deviation from plane at the mounting cutout: ≤ 0.5 mm
  This condition must also be fulfilled for the mounted HMI device.
- Permitted surface roughness in the area of the mounting gasket: ≤ 120 µm (R_z 120)
- The installation area is dry and free from contamination such as dust or lubricant.

Compatibility of the mounting cutout to other HMI devices

The Industrial Thin Client built-in units are compatible with SIMATIC Industrial PCs, Industrial Flat Panels, HMI devices and SINUMERIK TOP Panels of the same series with corresponding display size.

Note that despite the same dimensions for the mounting cut-out, the device depth of ITC V3 devices can differ from the device depth of the compatible devices.

Dimensions of the mounting cutout



	w^{+1}_{0}		h^{+1}_{0}
ITC1200 V3	310	x	221 mm
ITC1500 V3	382	x	241 mm
ITC1900 V3	448	x	278 mm
ITC2200 V3	513	x	315 mm
ITC2400 V3	569	x	347 mm

The width and height values must be reversed accordingly for mounting in portrait format.

3.1.3.4 Installing a strain relief

Requirement

For the assembly of the strain relief bracket you require:

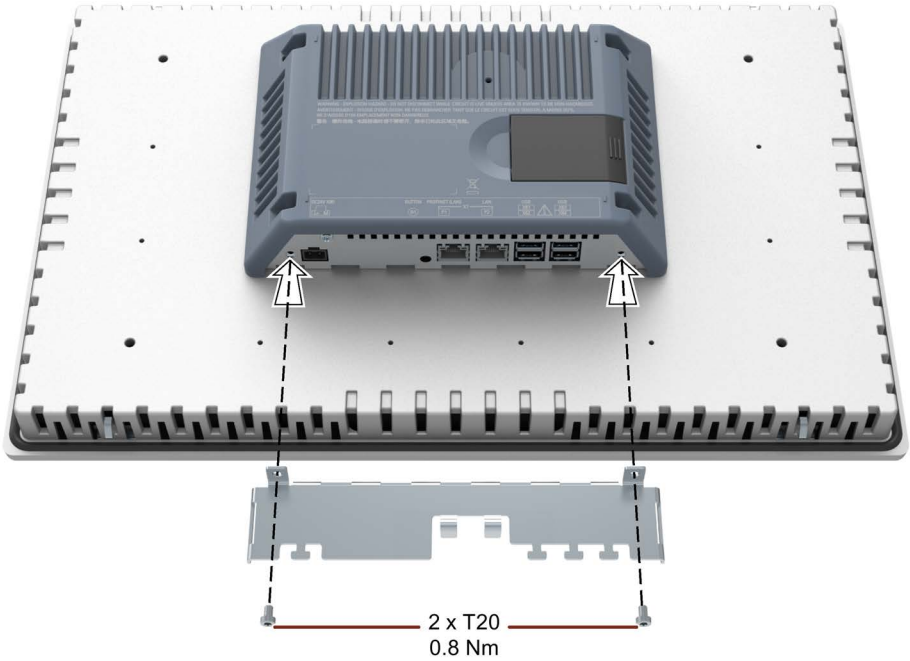
- The strain relief bracket from the scope of delivery
- A torque screwdriver with a T20 bit

Procedure

Fasten the strain-relief with the screws intended for this purpose, torque 0.8 Nm.

The screws are already inserted in the device in the delivery state.

The figure below shows an example.



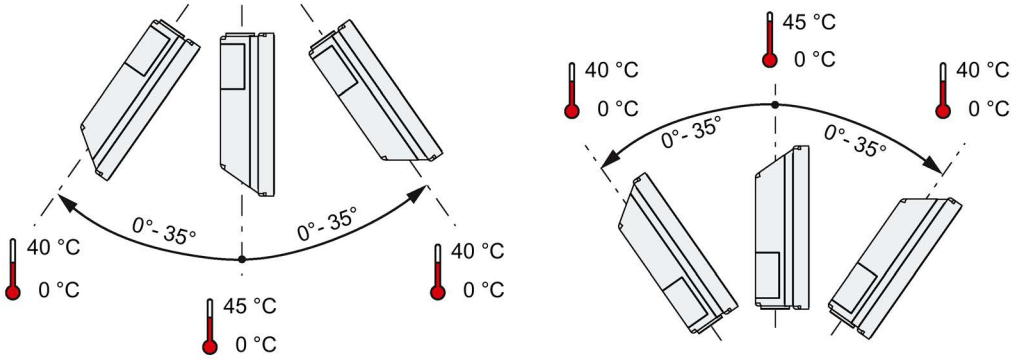
3.1.4 PRO devices

3.1.4.1 Permitted mounting positions

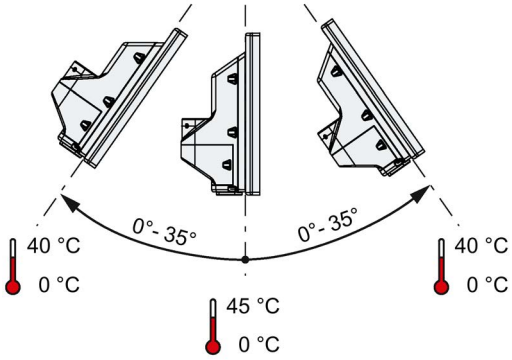
The device is intended for mounting on a support arm or stand.

The following figures show the permissible mounting positions of the different PRO devices.

PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom)



PRO devices for support arm (extendable, round tube)



Note

Mounting a PRO device in portrait format is **not** permitted.

See also

Climatic ambient conditions (Page 177)

3.1.4.2 Installing a strain relief

Requirement

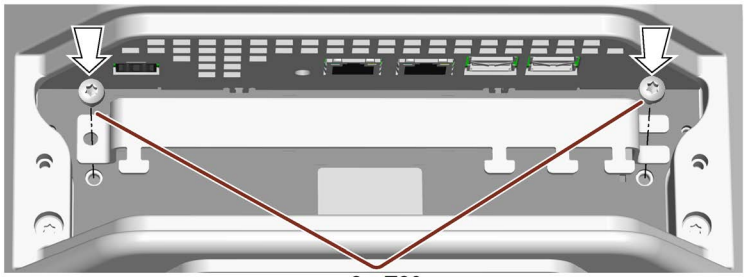
For the assembly of the strain relief bracket you require:

- The strain relief bracket from the scope of delivery
- A torque screwdriver with a T20 bit

Procedure

Mount the strain relief plate as follows:

1. Loosen the two screws of the terminal compartment cover and remove the terminal compartment cover.
2. Fasten the strain-relief with the screws intended for this purpose, torque 0.8 Nm.
   The screws are already inserted in the device in the delivery state.
   The figure below shows an example.



   For PRO devices for support arm (not extendable, flange top), the strain relief plate must be installed rotated by 180°.
3. If you do not install the device to a support arm or a pedestal immediately afterwards, close the terminal compartment. Fasten the terminal compartment cover with the two associated screws, torque 1.5 Nm. Check that the seal is sitting correctly.

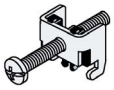
3.2 Installing the built-in unit

3.2.1 Notes on installation

NOTICE
Use according to IEC 61010-2-201 requires an appropriate enclosure The rear of the built-in device is classified as "Open Equipment" according to IEC 61010-2-201 for use in industrial control equipment. For approval and operation according to IEC 61010-2-201, the device must be installed in an enclosure or integrated in a cabinet. The enclosure or the cabinet must provide protection against electric shock and the spread of fire. The enclosure or the cabinet must meet the requirements for mechanical strength and the degree of protection for the relevant application.

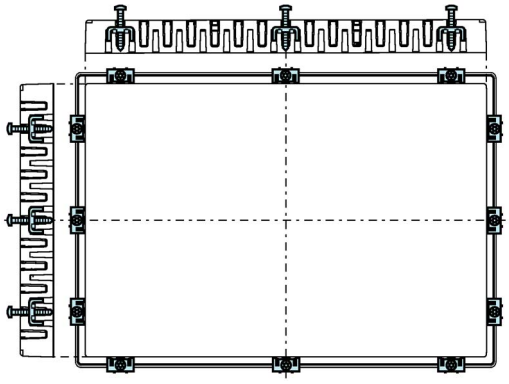
3.2.2 Positions of the mounting clips

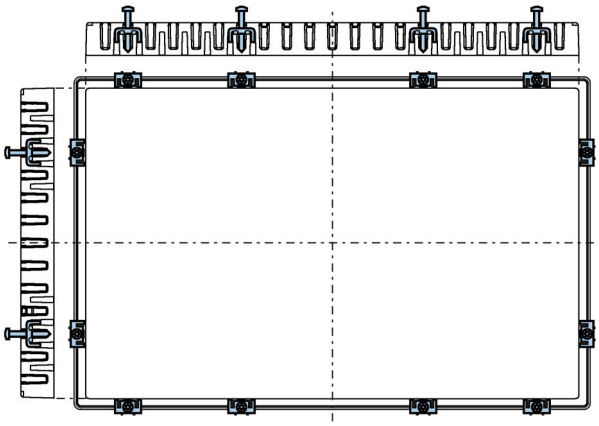
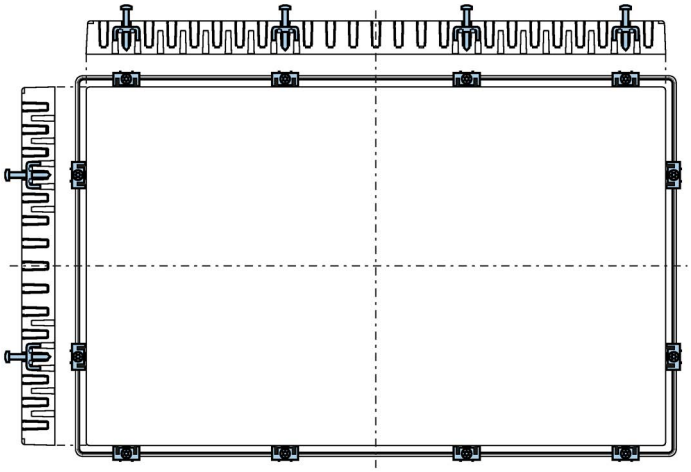
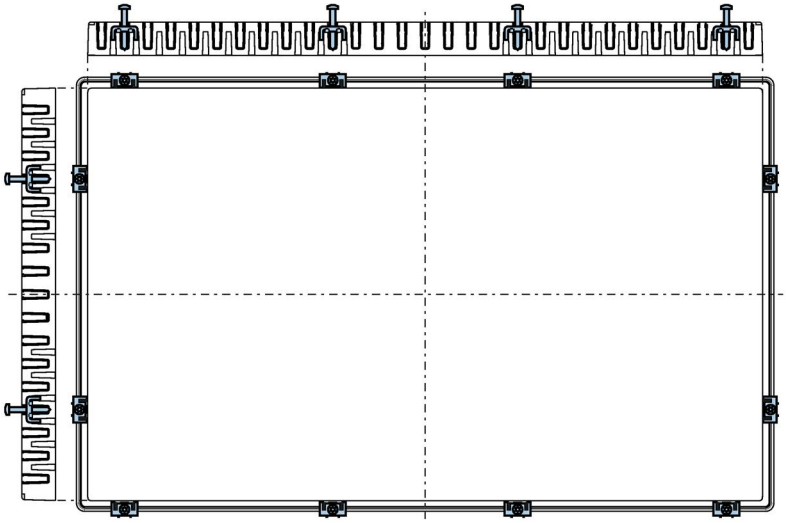
You attach the device with 12 mounting clips from the accessory kit, which are also available as an accessory.

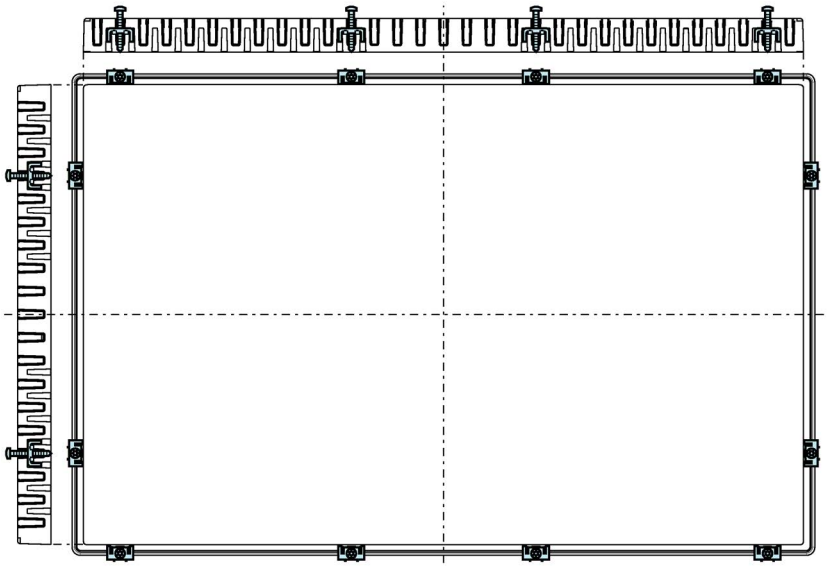


See also section "Accessories (Page 33)".

In order to achieve an IP65 degree of protection for the device, mounting clips must be installed in the following positions.

Device	Positions of the mounting clips
ITC1200 V3	

Device	Positions of the mounting clips
ITC1500 V3	
ITC1900 V3	
ITC2200 V3	

Device	Positions of the mounting clips
ITC2400 V3	

3.2.3 Fastening the device with mounting clips

Requirement

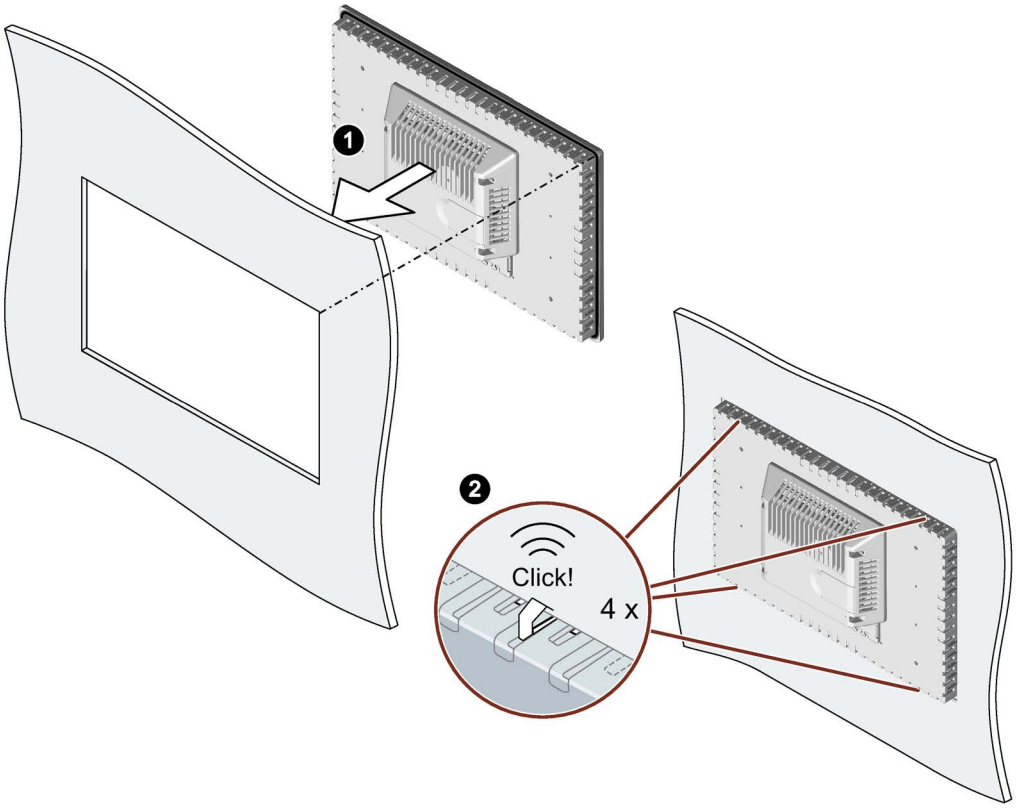
- All packaging components and protective films have been removed from the device.
- The following material and tools are available:
  - The mounting clips from the accessory kit
  - One torque screwdriver with cross-tip insert, size 2

Procedure

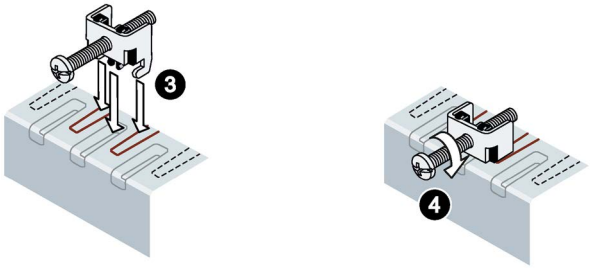
Note

If the mounting seal is damaged, the degree of protection is not guaranteed.

1. Insert the device into the mounting cutout from the front.



2. Make sure that all four spring locks on the top and bottom of the device fully engage. If necessary, gently press the device into the recess if it is not fully engaged.
3. Insert a mounting clip into the cutout provided on the device. Make sure it is in the correct position; see the section "Positions of the mounting clips (Page 49)".



4. To secure the mounting clip, tighten the grub screw with the screwdriver, torque 0.5 Nm.
5. Repeat step 3 and 4 for all mounting clamps until all clamps are fastened.
6. Check the fit of the mounting seal.

3.3 Installing a PRO device

3.3.1 Notes on mounting

WARNING

The device must be mounted securely.

Inadequately dimensioned fasteners may cause the device to fall down. Serious physical injury may result.

Make sure that fasteners are adequately dimensioned during installation. Make sure to consider the weight of the device and the forces acting on the device when dimensioning. This applies in particular to dynamic load of the device. All fasteners including mounting surfaces, support arm systems, and fastening elements such as screws must be able to carry at least four times the weight of the device.

Observe any further statutory specifications applying at the location of use of the device and further applicable regulations with regard to fastening the device.

Pay attention to the torque specifications in the following sections.

NOTICE

Degree of protection for overall device

If you are using a support arm system or a pedestal system that does not have IP65 degree of protection or Enclosure Type 4X/12 (indoor use only), IP65 degree of protection or Enclosure Type 4X/12 (indoor use only) are lost for the entire device. Spray and water jets as well as penetrating substances can then damage the device.

Use a suitable support arm system or pedestal system with IP65 degree of protection or Enclosure Type 4X/12 (indoor use only) for your application.

Note

Liability disclaimer

The device is mounted to a pedestal or a support arm via the mechanical interface with screws. Siemens assumes no liability for the consequences of incorrect installation.

Warranty at risk

If you do not install the HMI device in accordance with the specifications in these operating instructions, the warranty for the device is voided.

- Always install the device according to these operating instructions.
- If the seal on the backplane cover is damaged, it can be repaired. For a repair scenario, following the instructions in the section "Spare parts and repairs (Page 166)".

IP65 degree of protection and Enclosure Type 4X/12 (indoor use only) at risk

If there are no seals on the mechanical interfaces or if they are damaged, IP65 degree of protection and Enclosure Type 4X/12 (indoor use only) is at risk. Check the condition and proper seating of the seals.

NOTICE
Damaging the seal when opening If the device has not been opened for a long time, the backplane cover or terminal compartment cover may stick to the seal of the enclosure. Opening the device with excessive force or with tools will destroy the seal. Spray and water jets as well as penetrating substances can then damage the device. Open the terminal compartment cover gently, without too much pressure.

3.3.2 PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom)

Note

Mounting with and without a base adapter

The SIMATIC PRO devices are designed for mounting with the base adapter. If you install the device without a base adapter, you must adjust the mechanical interface between the support arm or pedestal and the unit accordingly, including placement of an appropriate seal on the mechanical interface.

Requirement

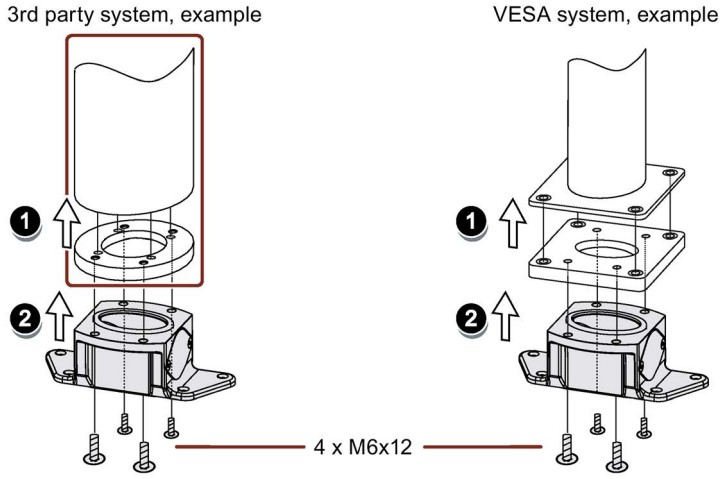
- All packaging components and protective films have been removed.
- Siemens base adapter with screws, included in the product package of a PRO device for support arm (not extendable, flange top) or for pedestal (extendable, flange bottom).
- One of the following support arms or pedestal systems:
  - Support arm or pedestal with mechanical VESA interface and the corresponding Siemens adapter set
  - Support arm or pedestal with mechanical interface for the Siemens base adapter
    The type of mechanical interface differs depending on the type of support arm or pedestal.

  See also section "System components for PRO devices (Page 25)".
- The following cables are fed through the pedestal or the support arm to which the device is mounted:
  - Cables for the power supply
  - Equipotential bonding cable
  - Data cables, e.g. PROFINET/Ethernet or USB cable

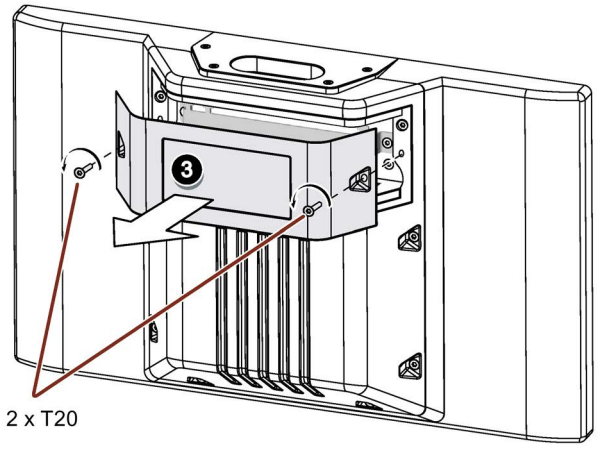
Procedure

This section describes the mounting of the device to a support arm system using example figures. Installation on a pedestal is carried out in the same way. For PRO devices for support arm (not extendable, flange top), the base adapter is screwed on from the top of the device. For PRO devices for pedestal (extendable, flange bottom) the base adapter is screwed on from the bottom of the device. A PRO device for support arm system cannot be used on a pedestal and vice versa.

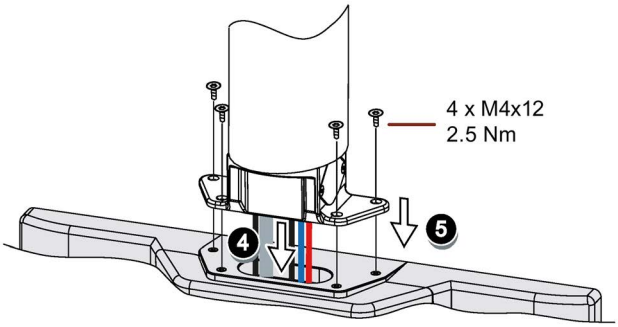
1. If an adapter plate for the Siemens base adapter is included in your support arm system, attach the adapter plate to the support arm with 4 M6x12 screws. Pay attention to the torque that is specified for the support arm.



2. Attach the base adapter with 4 M6x12 screws to the mechanical interface of the support arm from below. Pay attention to the torque that is specified for the support arm.
3. Loosen the 2 screws of the terminal compartment cover and remove the terminal compartment cover.



4. Insert all connection cables through the opening of the PRO device. Make sure that the connection cables are not damaged.



5. Attach the device with 4 M4x12 screws to the base adapter from the top, torque 2.5 Nm. Make sure that the connection cables are not crushed.
6. Connect all cables according to the description in the section below.
7. Fasten the terminal compartment cover to the device with the 2 screws, torque 1.5 Nm. Check that the seal is sitting correctly.

3.3.3 PRO devices for support arm (extendable, round tube)

Requirement

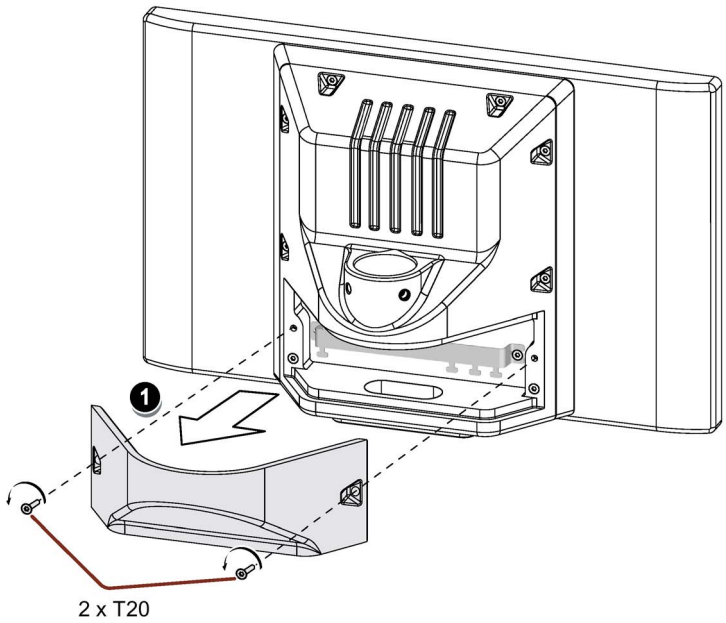
- One of the following support arm systems:
  - Support arm with round tube end with outside diameter 48.3 mm, appropriate for the opening of the PRO device
    When selecting the round tube, ensure that its inside diameter is large enough so that all needed cables and their connectors can fit through.
  - Support arm with mechanical interface, suitable for the flange of the flange mount adapter, and Siemens flange mount adapter (not included in product package)
  - Support arm with mechanical VESA interface, the corresponding Siemens adapter set and the Siemens flange mount adapter (not included in product package)

  See also section "System components for PRO devices (Page 25)".
- The PRO device, all packaging components and protective films have been removed
- The lower cover of the PRO device from the accessory kit
- The following cables are fed through the support arm to which the device is mounted:
  - Cables for the power supply
  - Equipotential bonding cable
  - Data cables, e.g. PROFINET/Ethernet or USB cable

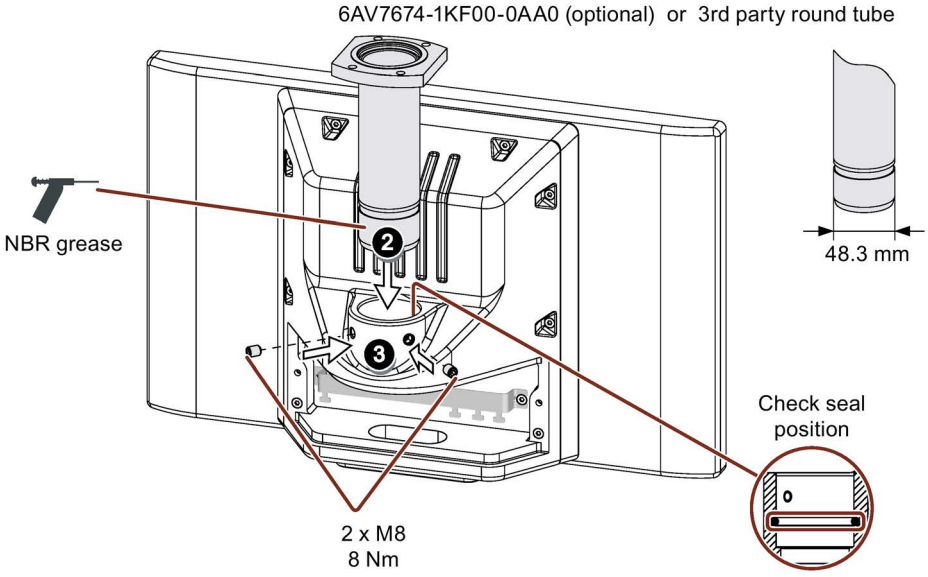
Procedure

The following figures show an example of how to attach the PRO device to a support arm system using the optionally available Siemens flange mount adapter. The same approach is used to mount the PRO device to a 48.3 mm round tube.

1. Loosen the 2 screws of the terminal compartment cover and remove the terminal compartment cover.



2. Ensure that the NBR seal is correctly seated on the inside of the mechanical interface to the flange mount adapter, see figure below. Grease the flange mount adapter or 48.3 mm round tube with grease suitable for NBR seals, and insert the flange mount adapter or 48.3 mm round tube into the corresponding opening of the PRO device.

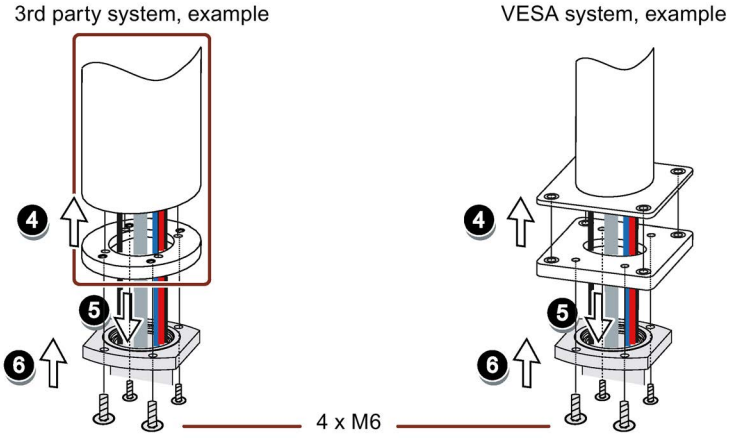


3. Attach the flange mount adapter or the 48.3 mm round tube with the two M8 threaded pins. Observe the appropriate torque:
   - Siemens flange mount adapter: 8 Nm
   - 48.3 mm steel round tube 8 Nm
   - 48.3 mm aluminum round tube: 5 Nm

4. If you use an adapter plate from a Siemens VESA adapter set, attach the adapter plate to the support arm with four M6x12 screws.

   If you use an adapter plate suitable for the Siemens flange mount adapter, attach the adapter plate to the support arm using the appropriate mounting hardware.

   When tightening the screws, adhere to the torque that is specified for the support arm.



5. Insert all connection cables through the opening of the flange mount adapter or 48.3 mm round tube into the connection compartment of the PRO device. Make sure that the connection cables are not damaged.
6. If you use an adapter plate from a Siemens VESA adapter set, attach the flange mount adapter to the support arm from the bottom with four M6 screws, 16 mm to 20 mm in length.

   If you do not use an adapter plate or use a differnt one, attach the flange mount adapter to the support arm from the bottom with four M6 screws. The length of the screws depends on the specifications for the support arm and must be at least 16 mm to ensure secure fastening of the flange mount adapter.

   The screws are not included in the product package of the PRO device. Pay attention to the torque that is specified for the support arm. Make sure that the connection cables are not crushed.
7. Connect all cables according to the description in the section below.
8. Fasten the terminal compartment cover to the device with the 2 associated screws, torque 1.5 Nm. Check that the seal is sitting correctly.
9. Attach the lower cover from the product package to the PRO device with 4 M4x12 screws, torque 1.5 Nm. Alternatively, you can extend the PRO device by adding an Extension Unit at the bottom. Observe the associated documentation.

See also

System components for PRO devices (Page 25)

3.4 Connecting the device

3.4.1 Notes on connection

Connecting cables

Use only shielded standard cables as data connection cables. You can find order information on the Internet (https://mall.industry.siemens.com).

Note

Disconnect SELV/PELV circuits from other circuits or insulate the cables

The wiring of the SELV/PELV circuits must be disconnected from other circuits that are not SELV/PELV or the insulation of all conductors must be rated for the higher voltage. Alternatively, a grounded shielding or additional insulation must be arranged around the wiring for SELV/PELV circuits or other circuits based on IEC 60364-4-41.

Note for using the HMI device in the geographical scope of the UL approval:

CAUTION

Use copper cables at connectors with terminal connections

Use copper (Cu) cables for all supply lines that are connected to the device with terminals, e.g. 24 V DC power supply cables to the 24 V DC power supply connectors.

Utiliser des câbles en cuivre sur les connexions à bornes

Utilisez des câbles en cuivre (Cu) pour tous les câbles d'alimentation qui sont raccordés à l'appareil par des bornes, par exemple les câbles d'alimentation 24 V CC sur le connecteur d'alimentation 24 V CC.

Connection sequence

NOTICE
Damage to the HMI device If you do not keep to the connection sequence you could damage the HMI device. Be sure to connect the HMI device in the following sequence.

1. Equipotential bonding
2. Power supply
3. PROFINET/Ethernet
4. USB devices

Disconnect the HMI device by completing the above steps in reverse order.

Connecting the cables

NOTICE
Adhere to the local installation regulations When connecting the cables, observe the local regulations and the local installation conditions, such as protective circuits for power supply lines.

NOTICE
Temperature resistance and insulation of the cables Use cables with a maximum permissible operating temperature that is at least 20 °C more than the maximum ambient temperature. The insulation of the cables must be suitable for the operating voltage.

NOTICE
Short-circuit and overload protection Various measures as protection against short-circuits and overloads are required for setting up a full installation. The types of components and the degree to which the protective measures are mandatory depend on the regulation that applies to your system setup.

- When connecting the cables, make sure that you do not bend the contact pins.
- Secure the cable connectors by fastening the connector to the socket with screws.
- Provide adequate strain relief for all cables.
- The pin assignment of the interfaces is described in the technical specifications.

3.4.2 Equipotential bonding

Differences in electrical potential

Differences in electrical potential can develop between spatially separate plant components. Such electrical potential differences can lead to high equalizing currents across the data cables and therefore to the destruction of their interfaces. Equalizing currents can develop if the cable shielding is terminated at both ends and grounded to different plant components.

Differences in potential may develop when a system is connected to different mains supplies.

General requirements for equipotential bonding

Differences in potential must be reduced by means of equipotential bonding in order to ensure trouble-free operation of the relevant components of the electronic system. The following must therefore be observed when installing the equipotential bonding circuit:

- The effectiveness of equipotential bonding increases as the impedance of the equipotential bonding conductor decreases or as its cross-section increases.
- If two plant components are interconnected by means of shielded data cables and their shielding is bonded at both ends to the grounding/protective conductor, the impedance of the additionally installed equipotential bonding cable must not exceed 10% of the shielding impedance.
- The cross-section of an equipotential bonding conductor must be capable of handling the maximum equalizing current. Equipotential-bonding cables are required between two control cabinets with a minimum conductor cross-section of 16 mm^2.
- Use equipotential bonding conductors made of copper or galvanized steel. Establish a large surface contact between the equipotential bonding conductors and the grounding/protective conductor and protect them from corrosion.
- Clamp the shield of the data cable from the HMI device flush at the equipotential bonding rail using suitable cable clamps. The equipotential bonding rail should be as close to the HMI device as possible.
- Route the equipotential bonding conductor and data cables in parallel and with minimum clearance in between.

Note

Equipotential bonding cable

Cable shields are not suitable for equipotential bonding. Always use the prescribed equipotential bonding conductors for this. An equipotential bonding conductor between control cabinets must have a minimum cross-section of 16 mm^2. The cable between the ground bar and HMI device must have a minimum cross-section of 4 mm^2.

Connection diagram

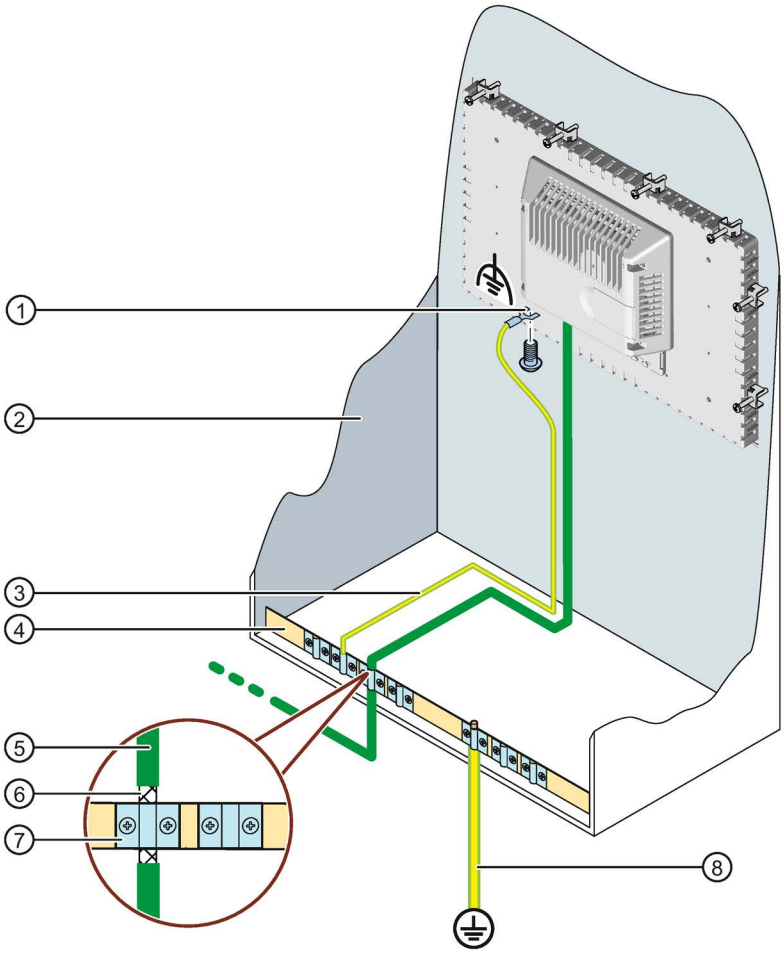
The following figure shows the connection of the functional grounding for equipotential bonding using the SIMATIC ITC1900 V3 as an example and applies in the same way to the other built-in devices.

Note

Cable routing for the PRO devices

Since the PRO device is mounted on a pedestal or a support arm instead of in a control cabinet, the connecting cables must be routed through the support arm or pedestal. The cross-sections specified for the built-in units are also valid for the PRO devices.

Follow the corresponding connection diagrams in the Quick Install Guide, which is enclosed with your PRO device.



① Connection for functional grounding, use a fork cable lug or ring cable lug, size M4
② Control cabinet
③ Equipotential bonding cable, 4 mm ^{2}
④ Equipotential busbar for equipotential bonding cables, grounding connection and shield support of the data cables
⑤ PROFINET data cable
⑥ Shield of the PROFINET data cable, connected to the equipotential busbar
⑦ Cable clip
⑧ Ground bar, 16 mm ^{2}

3.4.3 Connecting the power supply

NOTICE
Safe electrical isolation For the 24 V DC supply, use only power supply units with safe electrical isolation (SELV/PELV) in accordance with IEC 61010-2-201 or IEC 62368-1. The supply voltage must be within the specified voltage range. Malfunctions in the HMI device may otherwise result. For non-isolated plant design: Connect the connection for GND 24 V from the 24 V power supply output to equipotential bonding for uniform reference potential. Select a central termination point as far as possible.

Connecting cables for the power supply connector

The power supply plug is included in the accessory kit.

For the power supply connector, use flexible cables with end sleeves according to the specification in the following table.

Cables for the 24 V DC power supply connector		Specification
Cable type		Flexible cable (Cu), with end sleeve
Connectable cable cross-sections		0.5 ... 1.5 mm^2
		AWG*: 20 ... 16
Number of cables per connection		1
Stripped length of the cables		7 ... 8 mm
End sleeves according to DIN 46228	Without plastic sleeve	Form A, 7 mm long
	With plastic sleeve 0.5 ... 1.5 mm^2	Form A, 7 mm long
Tool		Screwdriver, tapered, 3 ... 3.5 mm
Connection system		Screw terminal
Tightening torque		0.5 ... 0.6 Nm

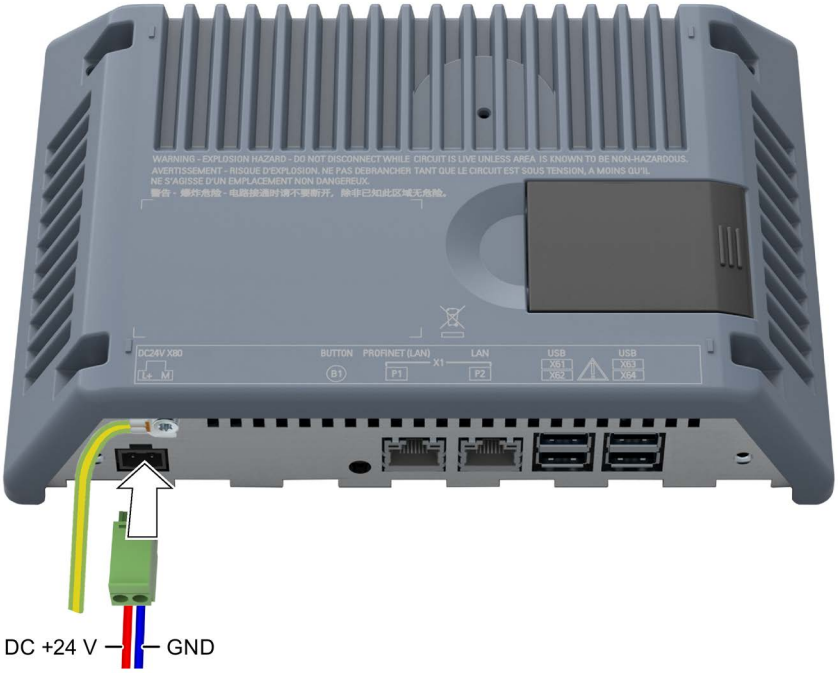
* American Wire Gauge

Additional information on the power supply connector supplied and other permissible power supply connectors can be found in the section "Accessories (Page 33)".

Connecting the power supply

NOTICE
Do not damage the socket Do not tighten the screws of the power supply connector if it is plugged into the HMI device. The pressure from the screwdriver may otherwise damage the HMI device socket. Connect the power cables when the power supply is disconnected from the HMI device.

1. Switch off the power supply.
2. Connect the power supply cables to the power supply connector as shown by way of example in the following figure. Observe the cable specification in the table above.



3. Connect the power supply connector to the corresponding socket of the HMI device. Check for correct polarity of the cables by referring to the interface labeling on the back of the HMI device.

Reverse polarity protection

The device is equipped with reverse polarity protection.

See also

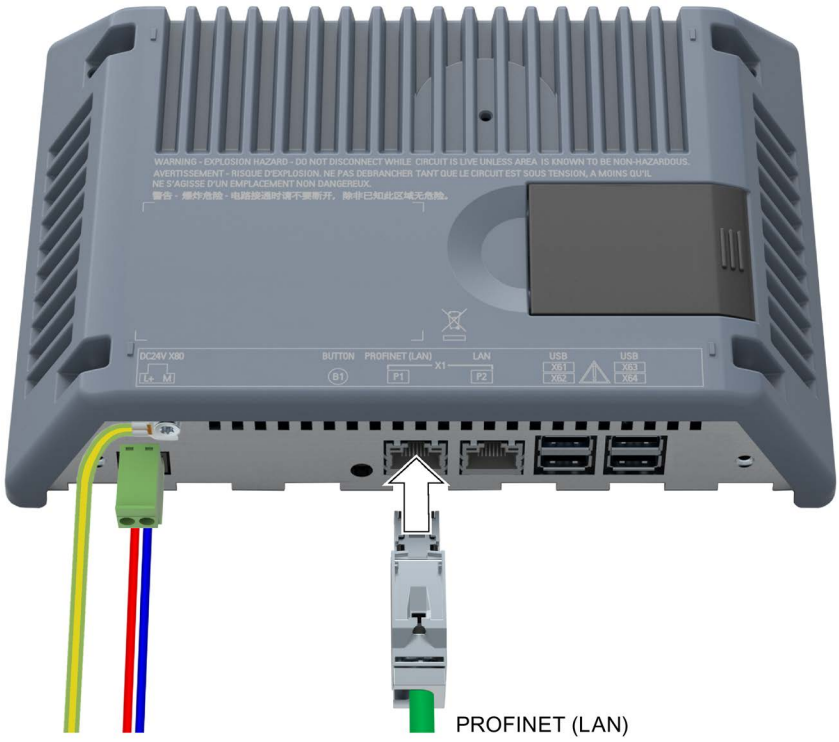
Interfaces (Page 24)

Power supply (Page 204)

3.4.4 Connecting device to the server

Connection diagram

The following figure shows the connection between the device and the server via PROFINET/Ethernet.



For PROFINET communication, use interface X1 P1 "PROFINET (LAN)", e.g. to use topology detection.

Procedure

1. Connect the PROFINET/Ethernet cable to the PROFINET (LAN) interface on the device.
2. Connect the PROFINET/Ethernet cable to the network or server.

See also

Interfaces (Page 24)

PROFINET (LAN), LAN - 10/100/1000 MBit (Page 204)

3.4.5 Connecting a USB device

You can connect the following industrial grade devices to the USB port:

- Mouse
- Keyboard
- Industrial USB Hub 4

- USB devices

  The Industrial Thin Client supports USB storage devices formatted with the FAT16/32, exFAT or NTFS file system.

  In addition, the following USB readers are supported for the connection type "RDP":

  – SIMATIC MV32x optical handheld readers
  – SIMATIC RF10xxR readers, which can be used, for example, in conjunction with the PM-LOGON or SIMATIC Logon software.

  Please note the detailed information on the use of USB devices in the following chapters:

  – Use USB memory devices (Page 123)
  – Using a USB reader (Page 124)

  Note

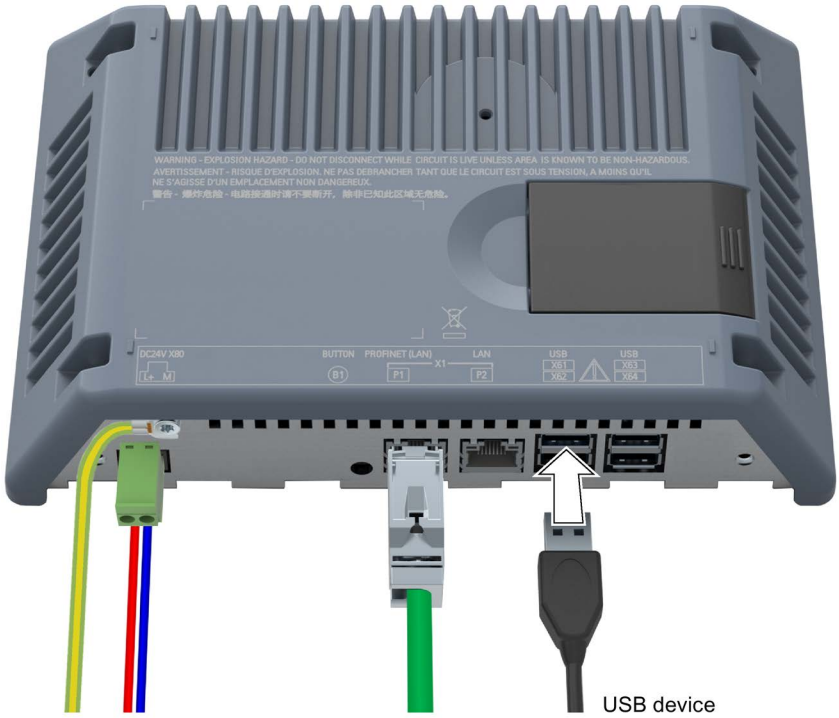
  Malfunction of the USB port

  If you wish to connect a USB device with its own power supply to the USB port, ensure that the USB ground connection of the external device is connected to the ground.

You can find additional information in section "Accessories (Page 33)".

Connection diagram

The figure below shows an how to connect a USB device.



See also

Interfaces (Page 24)

USB (Page 205)

3.4.6 Switching the device on, testing it and switching it off

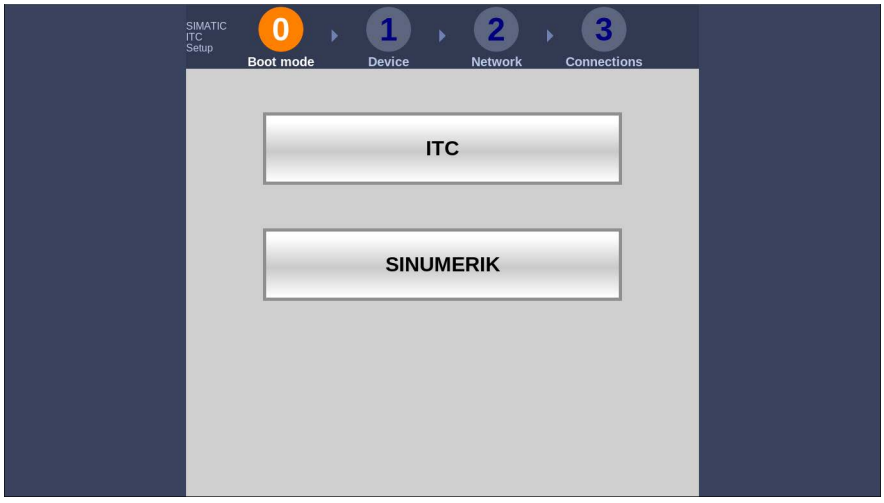
Execute a function test after connecting.

Function test

1. Switch on the power supply of the HMI device.

   If the device fails to start, you might have crossed the wires on the power plug. Check the connected cables and change their polarity.

   If the HMI device is properly connected, then you will see in the first commissioning dialog:



2. Switch the operator control off or perform the commissioning depending on the desired operating mode according to the following sections:
   - ITC commissioning (Page 79)
   - SINUMERIK commissioning (Page 125)

Shutdown the device

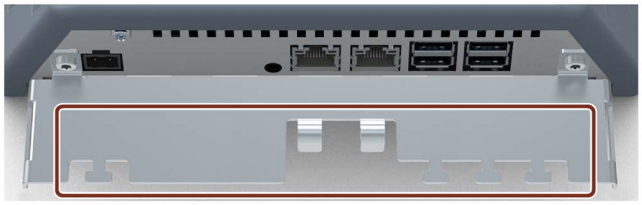
Proceed as follows:

1. Exit all open programs and ITC or SINUMERIK connections with the HMI device.
2. Turn off the power supply to the HMI device.

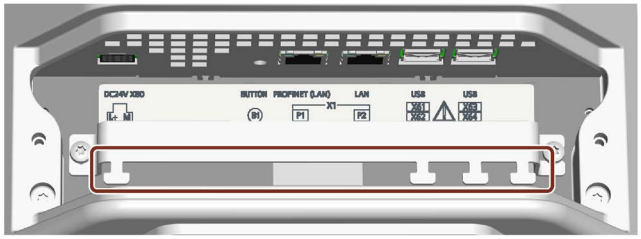
3.4.7 Securing cables

After connecting the cables, secure the cables with cable ties on the marked fastening elements.

Built-in units



PRO devices



See also

Installing a strain relief (Page 46)

3.4.8 Securing cables for use in hazardous areas

When devices with Ex approval are used in hazardous areas, note that the connectors must be secured in a captive manner at the interfaces.

⚠ WARNING

Explosion hazard from sparks when connectors come loose

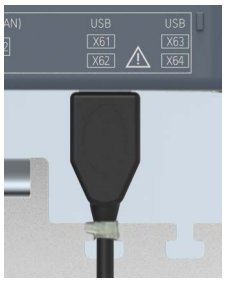
If a plug connector comes loose from the associated device interface during operation in a hazardous area, a spark over at the interface may cause an explosion. Death or serious physical injury as well as property damage may result.

For use in hazardous areas, it must be ensured that the plug connectors of the cables are fully connected to the respective interface and cannot come loose from the interfaces in any case. With SIMATIC HMI Industrial Thin Clients, this danger only exists at the USB interfaces.

Secure all connected USB cables directly at the transition between plug and cable to the nearest mounting element using a cable tie. Tighten up all cable ties in such a way that they fully wrap around the respective cable but do not damage the cable.

Use the appropriate mounting elements to secure the connected USB cables, as described in the previous chapter.

The following figure shows an example of how to captively secure a USB plug.



3.5 Removing the device

3.5.1 Removing the built-in unit

The HMI device is removed again in reverse order of its installation and connection.

Procedure

Proceed as follows:

1. Exit all open programs and ITC or SINUMERIK connections with the HMI device.
2. Switch off power to the HMI device.
3. If you use the HMI device in a hazardous area, ensure that both of the following conditions are met: The area is no longer hazardous or the operator control and its plug-in connections are de-energized.
4. Remove all cable ties which are located on the operator control to relieve strain from the connection cables.
5. Remove all connector plugs and the equipotential bonding from the operator control.
6. Secure the operator control so that it cannot fall out of the installation slot.
7. Remove the screws from the cover of the mounting clip and remove all mounting clips.
8. Replace the operator control from the installation slot.

See also

Installing the built-in unit (Page 49)

Connecting the device (Page 59)

3.5.2 Removing a PRO device

The HMI deices is generally removed by following the steps taken to install in it but in the reverse order.

Procedure

Proceed as follows:

1. Exit all open programs and ITC or SINUMERIK connections with the HMI device.
2. Switch off power to the HMI device.
3. If you use the HMI device in a hazardous area, ensure that both of the following conditions are met: The area is no longer hazardous or the device and its plug-in connections are de-energized.
4. Open the connection bay by removing the connection bay cover.
5. Remove all cable ties which are located in the connector compartment on the operator control to relieve strain from the connection cables.
6. Remove all connector plugs and the equipotential bonding from the operator control.
7. Replace the operator control from the support arm or pedestal. Make sure that the connection cables are not damaged.
8. Fasten the terminal compartment cover to the device with the 2 screws, torque 1.5 Nm.

See also

Installing a PRO device (Page 53)

Connecting the device (Page 59)

Operating the device

4

4.1 Overview

Introduction

If you are using the device to access a server, the screen display of the server is shown on the device. You operate the server screen from the device.

Operator input options

The following operator input options are available, depending on the peripherals that are connected to your device:

- External keyboard, connected via USB
- External mouse, connected via USB
- Touch screen
  You control operating elements by touching with your finger.
  To double-click, touch an operating element twice in rapid succession. The server can be configured for opening folders and files with a single click.

  Depending on the features of the server to which the Industrial Thin Client is connected, the capacitive touch screen provides single-touch or multi-touch functionality.

⚠ WARNING
Unintentional actions In conjunction with a server configured for single-touch operation, operate only one operating element on the screen at a time. Otherwise, you can trigger unintended reactions.

On-screen display for remote access to a server

The server screen is displayed as a full screen.

4.2 Notes on the capacitive touch screen

4.2.1 General information

The following information applies to all devices with a capacitive touch screen, regardless of whether the touch screen is operated in single-touch or multitouch mode.

WARNING

Personal injury or property damage due to no earth connection

An inadequate earth connection or the lack of one may cause malfunction of the capacitive touch screen. Functions may not work properly. This can result in personal injury or property damage.

- Always connect the device to an earth conductor.
- The earth conductor from the device must be connected directly to earth with low impedance (short connection, minimum cross-section 4 mm^2).

You can find additional information on connecting the ground conductor in the section "Equipotential bonding (Page 61)".

WARNING

Personal injury or property damage due to maloperation

Incorrect operation of devices with a touch screen can occur. This can result in personal injury or property damage.

Take the following precautions:

- Configure the plant so that safety-related functions are not operated with the touch screen.
- Switch off the device for cleaning and maintenance.

NOTICE

Damage to the touch screen

Operation of the touch screen in the following ways will reduce its service life up to and including total failure:

- Touching it with a pointed or sharp object
- Abrupt impact with solid objects

Use only your finger or a touch pen to touch the touch screen.

Note

Do not touch the touch screen during startup

During the startup process, the device automatically calibrates the capacitive multitouch screen. The touch screen is locked during calibration.

Do **not** touch the touch screen during startup. Make sure that you do **not** rest on the touch screen with the palm of your hand during startup.

Make sure that there are **no** conductive liquids on the touch screen during startup.

Security functions in an industrial environment

The touch screen is locked for security reasons when following happens:

- There is a conductive liquid on the touch screen with ground contact via the enclosure or the operator, for example.
- An electromagnetic disturbance has an effect which exceeds the specification in the technical specifications of the device, see section "Electromagnetic compatibility (Page 175)".

Once the interference is over, the touch screen is no longer locked.

4.2.2 Operating a device with capacitive multi-touch screen

You operate the multi-touch screen with one or multiple fingers. You can also operate it using gestures with up to five fingers at a time.

WARNING

Danger of malfunction due to improper execution of gestures on the touch screen

If gestures are executed incorrectly on the touch screen with multi-touch function, these gestures may not be recognized or could be recognized incorrectly. The entries made are then not implemented by the device or are implemented incorrectly or in an unintended manner.

Incorrect execution of multi-touch functions can lead to errors in the operation of the plant and thus to physical injury.

Note the following when operating the touch screen with multi-touch function:

- The touch screen reacts to contact on its surface, not to pressure.
- When using a touch pen: Operate the touch screen only with a touch pen for capacitive touch.
- Avoid unintended multiple touches, for example, with your knuckles.

Before you start to operate the device, make sure you are familiar with the multi-touch functions of the Windows operating system, as well as with the application to be used and its functions. Ensure that the gestures which the user executes on the multi-touch display are recognized by the application. It is possible that certain gestures need to be trained beforehand.

Notes on operation

Note when operating the multi-touch screen:

- Surface contact with a diameter of about 5 to 20 mm is required for an operator action to be detected.
- An operation with gloves with a material thickness of <2 mm is detected in most cases. However, check the usefulness of the gloves you are using.
- To avoid incorrect operation, certain inputs are ignored and blocked from further entry:
  - Simultaneous operation with more than 5 fingers.
  - Surface contact with a diameter of > 3 cm, for example, resting the palm of the hand on the touch screen
  - As soon as the touch screen is no longer touched, input is possible again.

Functions of the multi-touch screen

- Detection of up to 5 finger touches at a time.
- Detection of gestures that are supported by the operating system or the software installed on the device.

Note

Multi-touch operation can provide advanced features or pose limitations depending on the operating system and the software installed on the device. Read the corresponding documentation.

- You do not need to calibrate the touch screen. Some operating systems do offer touch calibration. However, this calibration does not lead to any improvement in accuracy.

ITC Operating mode

5

5.1 System requirements

The following list shows the operating system and software requirements depending on the specific connection type.

- RDP, Sm@rtServer

RDP	Sm@rtServer	
X		Windows Server 2008 R2 (64-bit)
X		Windows Server 2012 R2 (64-bit)
X		Windows Server 2016 (64-bit)
X		Windows Server 2019 (64-bit)
X		Microsoft Windows 7 SP1 (32-bit and 64-bit)
X		Microsoft Windows 10 (32-bit and 64-bit)
X		Microsoft Windows 11 (64 Bit)
	X	As of SIMATIC WinCC V14 (TIA Portal) with the options: • SIMATIC WinCC Sm@rtServer for SIMATIC Panels • SIMATIC WinCC Sm@rtServer for Runtime Advanced

- VNC: The following protocols are supported for the following versions:
  RealVNC 6.0.1, TightVNC 2.8.5 and UltraVNC 1.2.1.0
- WinCC OA: The connection to WinCC OA is supported as of version WinCC OA 3.16. Support with an earlier version can be requested from the WinCC OA team. Additional information can be found on the Internet at the following address:
  SIMATIC WinCC Open Architecture
  (https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-oa/wincc-oa-basic-software.html)
- Citrix: The current Citrix version is supported. The corresponding system requirements apply. Additional information can be found on the Internet at the following address:
  Citrix product page (https://www.citrix.com/products.html)
- Web access via HTML5

See also

Technical support (https://support.industry.siemens.com)

5.2 Typical applications

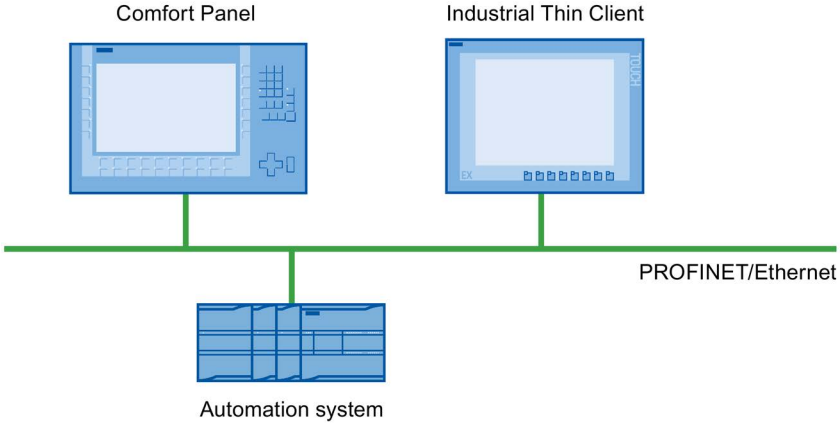
Industrial Thin Clients can be used as operator terminals in different scenarios. With the Industrial Thin Client, for example, you can access an HMI device and hence control a work process. You can also use the Industrial Thin Client to run Office applications on a server, for example, on a PC and modern web applications.

Typical applications are presented in the following.

Access to a Sm@rtServer

The Industrial Thin Client accesses an HMI device or industrial PC as a Sm@rtServer client using the SIMATIC WinCC Sm@rtServer option. You operate and monitor the WinCC project (TIA Portal) of the device on which the Sm@rtServer is activated.

The following figure shows one possible configuration.



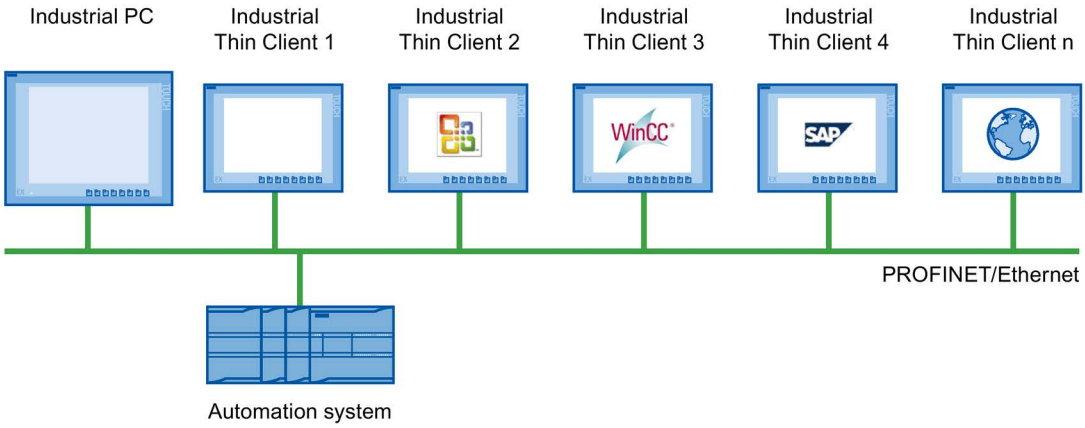
Access to a server via "RDP".

The Industrial Thin Client uses RDP (Remote Desktop Protocol) to access a server, such as an industrial PC or a PC. The following applications are also possible.

- WinCC/Web Navigator

  The Industrial Thin Client uses an Internet browser on the server to access the WinCC Web Navigator as a Web Navigator client. In this case, the Windows Server operating system must be installed on the server. For more information, refer to the documentation for the WinCC/Web Navigator option.
- The Industrial Thin Client accesses an Office application (e.g., MS Excel) or SAP application on the server. In contrast to the Windows Server operating systems, you can only operate one screen with Windows 7. The other monitor is always blocked.
- The Industrial Thin Client accesses an Office application, such as MS Excel, running with the Windows Server operating system or a SAP application on the server.

The following figure shows one possible configuration with the Windows Server operating system on an Industrial PC or a PC.

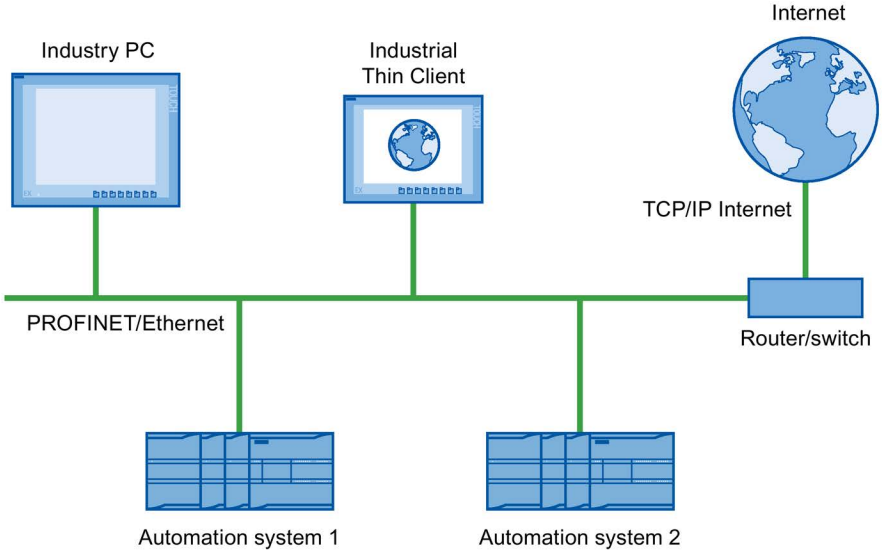


Access to a server via "VNC"

You use VNC in a similar way as RDP to remotely monitor and run a PC and to monitor its screen outputs. In contrast to RDP, all clients display the same server screen.

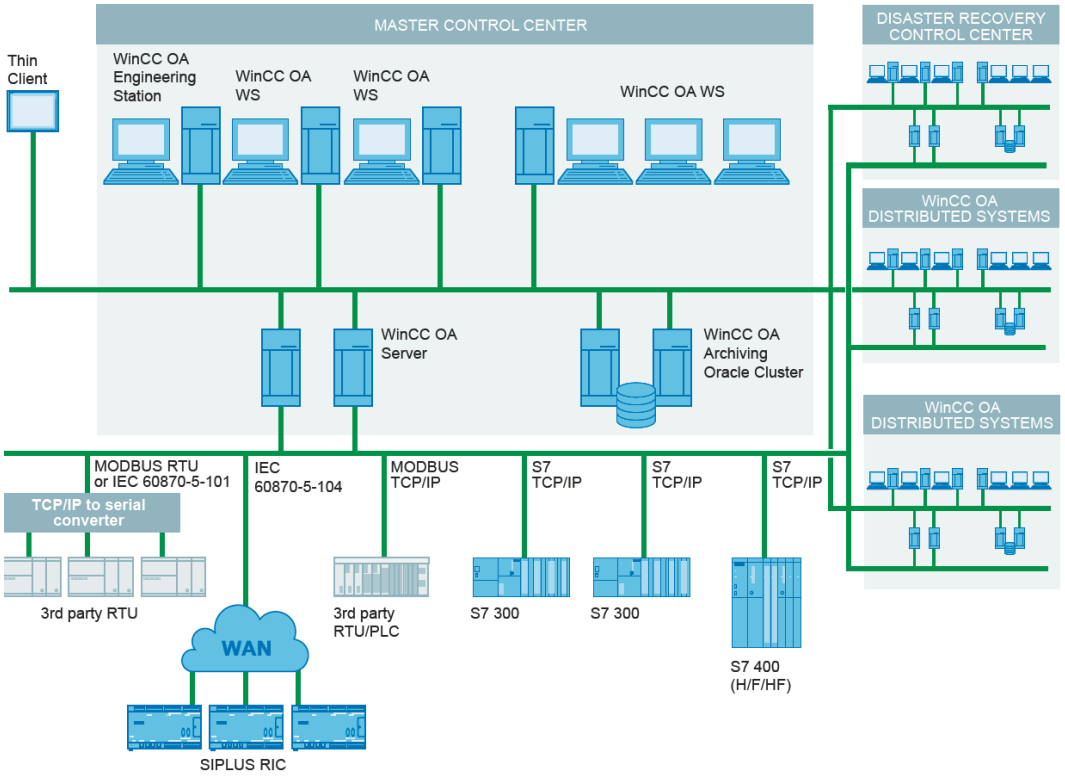
Access to a web server via "Web"

With the integrated web browser functionality, the Industrial Thin Client displays applications and web server contents. Possible web-based contents include diagnostics web pages and user-specific web pages of an S7 controller (PROFINET) and contents from the Internet, an intranet or an IP camera.



Access to a web server via the "WinCC OA"

The Industrial Thin Client operates similarly to a SIMATIC WinCC OA WebClient. The WinCC OA server makes the client component available to the Industrial Thin Client.



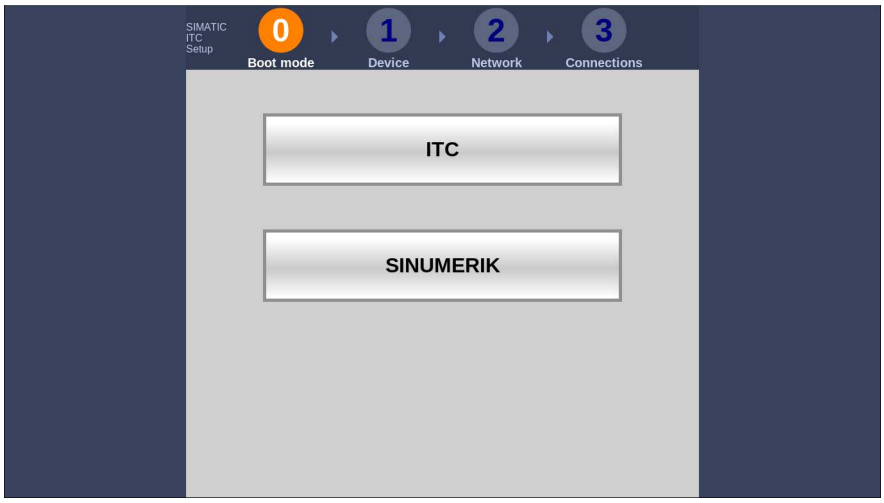
5.3 ITC commissioning

Requirement

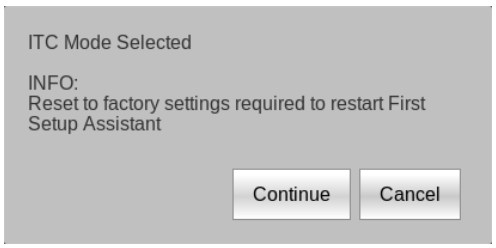
The devices is connected according to the description in these operating instructions to the 24V DC power supply and equipotential bonding is connected.

Procedure

1. Switch on power to the Industrial Thin Client.
   The first commissioning dialog to select the operating mode is displayed.



2. Select the operating mode "ITC".
   The following dialog appears:



3. Confirm the dialog with the "Continue" button.
   The device starts in ITC operating mode. Information regarding the included free software is displayed during startup.
   The Setup Wizard guides you in setup steps 2 through 4 through the configuration of selected device and network data as well as passwords and connection settings.
4. Follow the instructions of the Setup wizard.
   The Setup Wizard remains open until the configuration settings are validated.

The first commissioning was successful if one of the following conditions applies:

- The taskbar is displayed.
- The configured startup connections are established.

Result

The first commissioning has been completed and the operating mode has been defined. In the future, the device starts in ITC operating mode and the first commissioning dialogs are no longer displayed.

To re-commission, you must reset the device to factory settings or update the firmware, see section"The "System" submenu (Page 85)".

5.4 Interrupting and restoring a connection

Introduction

The connection to the server can be interrupted in several ways:

- The server is offline or has not completed its startup sequence.
- The password is incorrect.
- A firewall is blocking server access.
- The server has been shut down, for example, for maintenance purposes.
- The PROFINET/Ethernet network cable has been disconnected.
- A connection problem occurred in the network.
- A client-server connection was started on another device which logs onto the server with the same data. The client-server connection running on your device is then terminated.

Note that there can be multiple client-server connections at one time.

Automatic connection establishment

The device offers the possibility to re-establish an interrupted physical connection automatically. There are two basic standard cases for this:

- Initial start of a connection
  The connection cannot be established because the server is not ready, for example. The device makes continuous attempts to establish the connection to the server.
- Existing connection
  An existing connection to the server is interrupted because the network cable has been removed or the network is faulty, for example. The device attempts to re-establish the connection to the server.

You can find additional information in the section "Connection settings (Page 96)".

5.5 Assigning device parameters

5.5.1 Possible applications

The Industrial Thin Client can fulfill the following functions as an operator terminal:

- Access to an HMI device as a Sm@rtServer client via the WinCC Sm@rtServer option.
- Access as a client via the "RDP" protocol.
- Access as a client via the "VNC" protocol.
- Access a Citrix server as Citrix client.
- Access as a client on a WinCC OA server.
- Access as a web client to a web server, e.g. of an S7 controller or the Intranet.

When the device accesses a server, for example, an HMI device or a PC, as a client, the screen display of the server is shown on the screen of the Industrial Thin Client. The user uses the Industrial Thin Client to access programs or projects on the server.

Note

"Sm@rtServer", "RDP", "VNC", and "Web" are referred to as connection types in this document.

Note

The Industrial Thin Client's browser is based on Chromium version 142.

5.5.2 Opening the configuration

This section describes how you can make configuration settings on the device.

Note

Alternatively, you can edit the configuration settings of the device via remote access from a PC, see section "Remote configuration (Page 109)".

Procedure

1. In the Start menu, press the "Start menu" icon.

2. Select the menu entry "Configuration".
   The configuration settings are opened and are structured as follows:

Menu/Submenu	Content
The "All" menu (Page 83)	All configuration settings in one window
The "Information" submenu (Page 84)	Device and network parameters
The "System" submenu (Page 85)	Parameters for device, screen, firmware, remote maintenance and remote configuration
The "Network" submenu (Page 91)	Settings for the network access
The "Connections" submenu (Page 94)	Parameters for the client-server connection of the ITC
The "Passwords" submenu (Page 101)	Connection password and administrator password
The "Desktop" submenu (Page 104)	Parameters for displaying the ITC desktop
The "Programs" submenu (Page 106)	Parameters for the web browser

3. To edit the configuration, log on as an administrator.

Note

Forced termination of connection

When you change and save the configuration settings, all started client-server connections are terminated without a confirmation prompt and all open programs are closed. The autostart connections are re-established afterwards and the new configuration settings are put into effect.

If you do not log on as administrator, you only have read access to device and network data under "Configuration > Information".

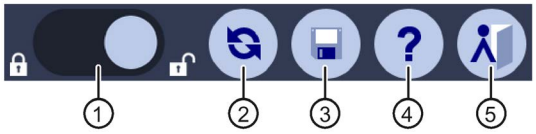
Note

Protection against unauthorized access

To protect the configuration settings from unauthorized access, assign a new administrator password immediately after first commissioning or after restoring the factory settings.

Title bar of the configuration settings

The title bar contains the following icons with the following functions:



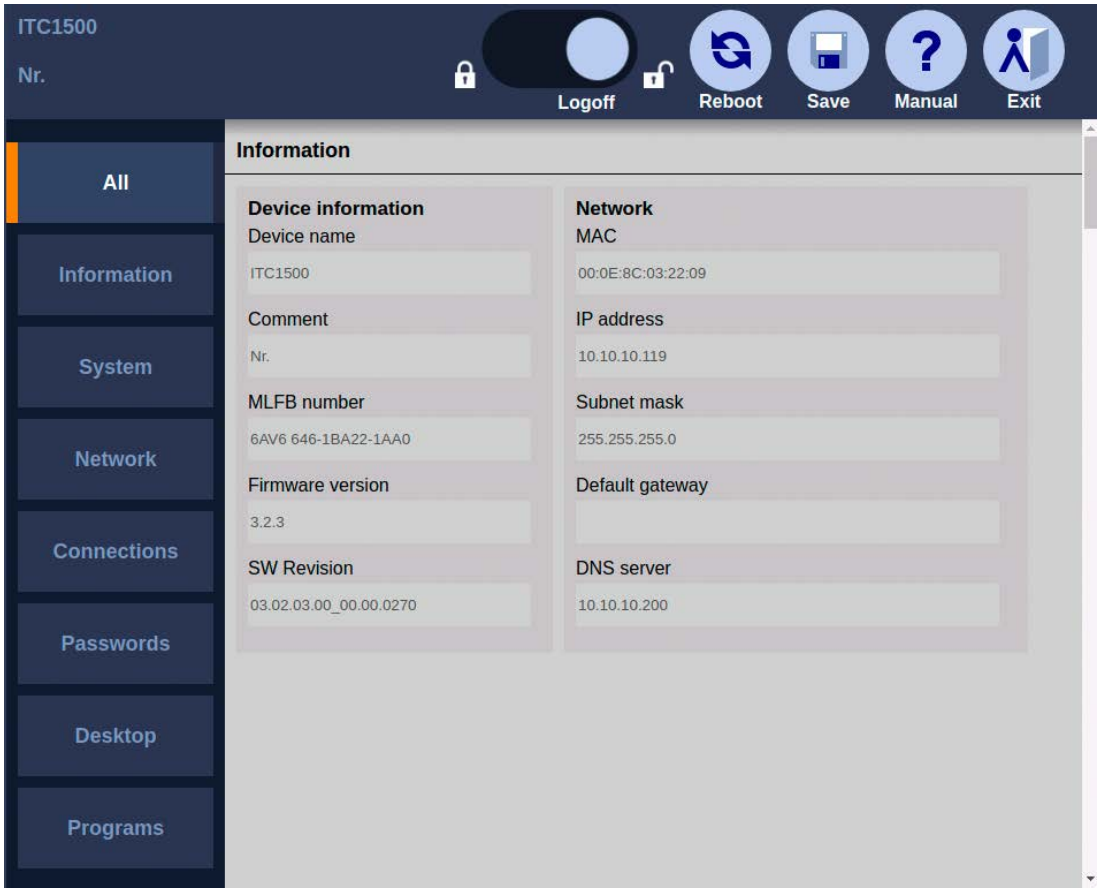
① "Log on" as an administrator and then "log off"
② "Restart" device
③ "Save" configuration settings
④ Call "Help"
⑤ "Exit" configuration

NOTICE
Unintended reactions of the device Two people can edit the configuration settings simultaneously: locally on the device and via remote configuration. The most recently saved settings are the valid settings at any given time (blue "Save" symbol). Organize access to the configuration settings in such a way that only one person can edit the configuration settings at one time.

5.5.3 The "All" menu

Structure

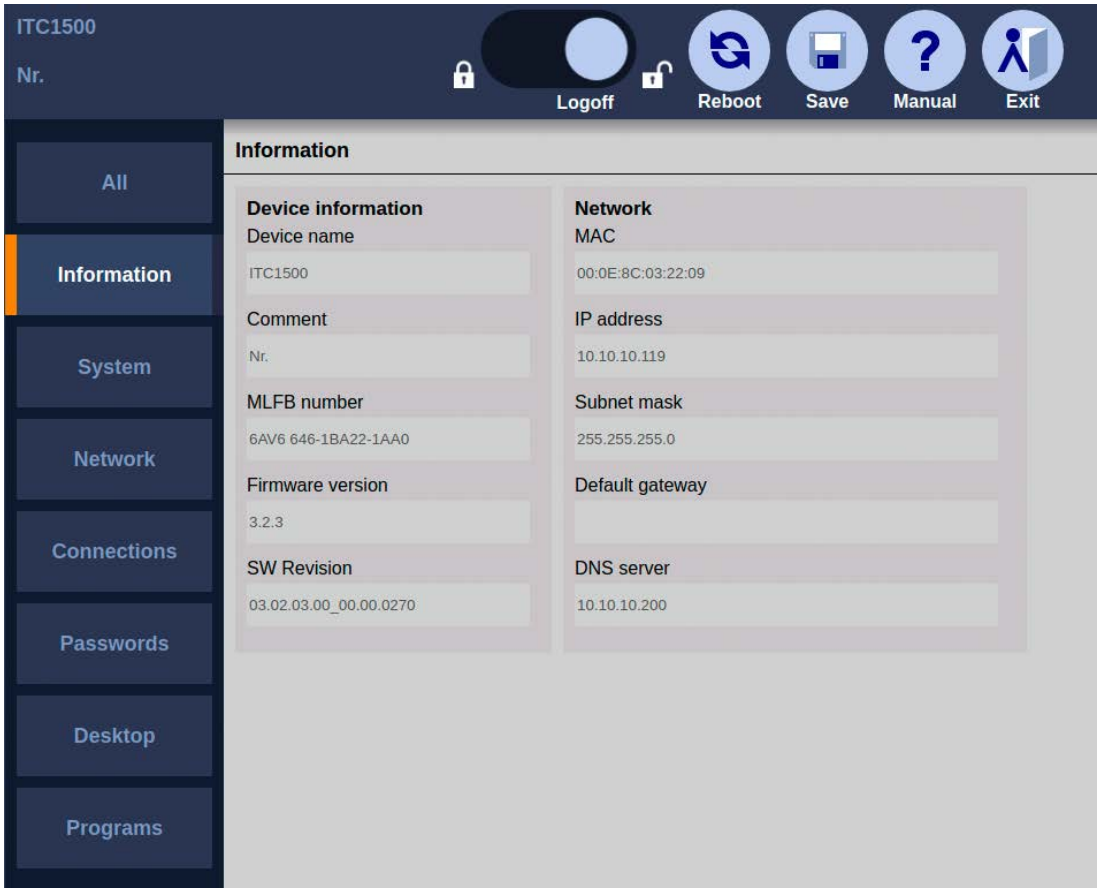
The following figure shows the "All" menu in which all the configuration settings are shown on one page.



If you are logged on as administrator, you have write access, otherwise only read access to the settings.

5.5.4 The "Information" submenu

The following figure shows the device data in the Start menu "Configuration > Information".



The device data identify the device uniquely and are shown here for informational purposes only. You can change the device data via the system settings and the network settings, see sections "The "System" submenu (Page 85)" and "The "Network" submenu (Page 91)". The home page of the web browser also displays device data and network settings.

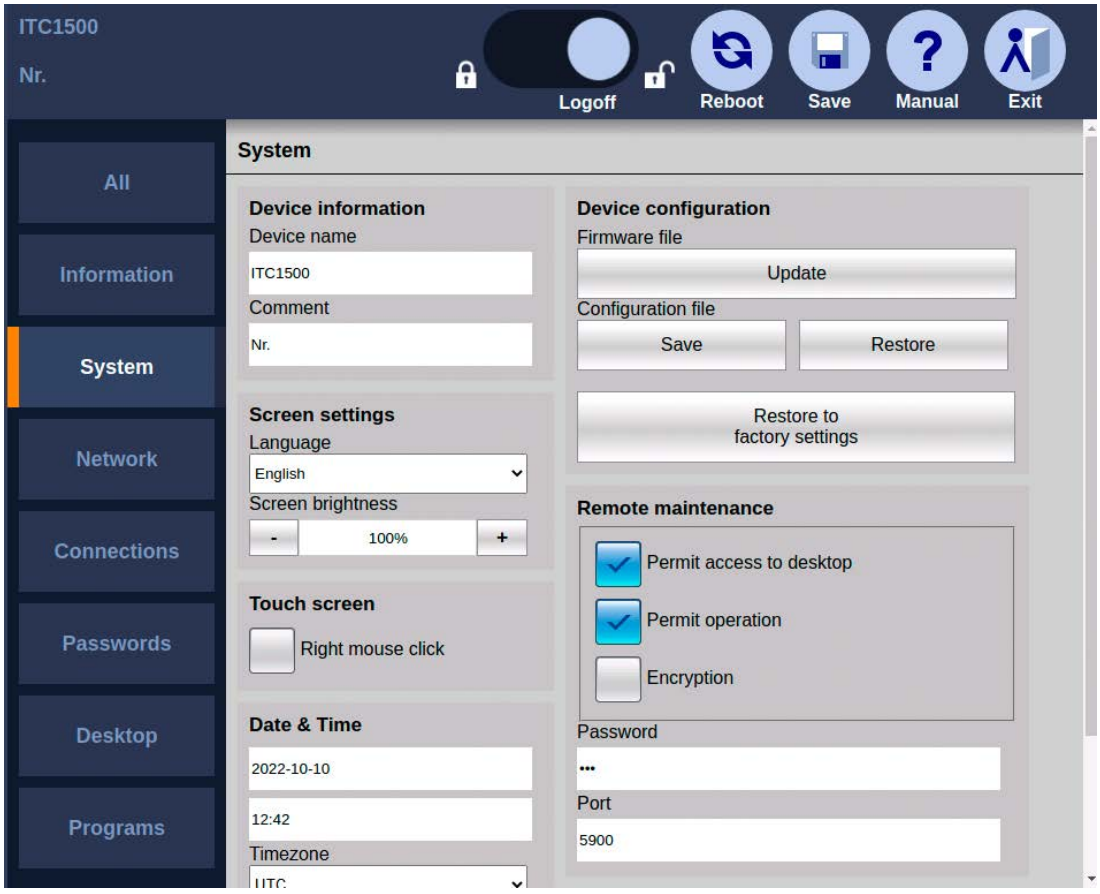
Note

If no administrator is logged on, the configuration settings only show the "Information" submenu.

5.5.5 The "System" submenu

Introduction

The following figure shows the system settings in the Start menu "Configuration > System".



You can perform the following actions:

- Specify device name
- Setting up screen: Language, brightness, right mouse click
- Update firmware
- Save and retrieve the configuration file
- Restore to factory settings
- Setting for remote maintenance via VNC
  Remote maintenance is performed via an encrypted connection. Remote maintenance requires a VNC client that supports the corresponding encryption, for example Tiger VNC.

Specifying device name

In the "Device information" area, specify a name for the Industrial Thin Client in "Device name". This name will allow the administrator to identify the device. The device name will be displayed at the following places:

- In the title bar of the configuration settings
- As the PROFINET station name in SIMATIC Manager

The device name is also the PROFINET station name and must meet the following conditions:

- One or more identifiers separated by a dot.
- Length of identifier: 1-25 characters
- Length of the device name: 1-255 characters, but only up to 26 characters are displayed on the device
- The identifiers contain lower case letters a-z and numbers 0-9.
- The identifiers cannot start or not end with "-".
- The first identifier does not have the form "port-xyz" or "port-xyz-abcde" where a, b, c, d, e, x, y, z = numbers 0 to 9.
- Identifiers do not start with "xn--" if RFC 3490 is applied.
- The device name may not end with "0".
- The device name does not have the n.n.n.n format, where n = 0 to 999.

Devices with more than one Ethernet interface do not need more than one device name.

Only up to 23 characters of the **comment** are displayed on the device (see above).

Setting date, time and time zone

In the "Date & Time" area, you can set the date and time.

NOTICE
Setting the date and time correctly When the date and time are not set correctly, malfunctions may occur in the plant. To prevent malfunctions, set the date and time of the HMI device and all controllers connected to the HMI device to the correct values or use an NTP server for time synchronization. Make sure that the time zone is set correctly depending on the location in which the HMI device is used. Check the correct settings for date and time after every update of the operating system.

NOTICE

Time synchronization required for time-dependent reactions

A malfunction may occur in the plant if the date and time are not synchronized and time-dependent reactions are triggered in the plant via the HMI device. To avoid malfunctions, use automatic time synchronization via one or more NTP servers.

In the input fields under "Date & Time", enter the date in "yyyy-mm-dd" format and the time in 24-hour format.

Alternatively, you can use up to three NTP servers. To do this, activate the option "Use NTP server", select the correct time zone and enter the IP addresses of the desired NTP servers under "NTP Server 1...3". Make sure that the device in question is set up as an NTP server.

Setting up screen

Set the system language that includes the following texts under "Language":

- Start menu and settings
- On-screen keyboard and externally attached USB keyboard
- Messages

CAUTION

Damage to the machine or plant through operating error

The configured system language, English for example, also determines the keyboard language of the externally connected USB keyboard. If you then connect an English keyboard, the keys do not have the same meaning as what is printed on them.

This may result in operating errors at the machine and personal injury or damage to the machine or plant. To connect an English keyboard, set the system language to English under "Language" in the Start menu "Configuration > System".

Under "Screen brightness", adjust the intensity of the backlighting.

If you select the "Right mouse click" option, each contact on the touch screen lasting more than 2 seconds will be interpreted as a right-click.

Example: If you touch the "Workstation" icon in Windows for more than 2 seconds, the operating system or application will respond as though you had right-clicked the icon: the context menu is displayed where you can select the "Properties" item, for example.

Update firmware

You update the device firmware either directly on the device via USB or with remote access from a PC, see section "Remote configuration (Page 109)".

NOTICE

Data loss during firmware update

All configuration settings are lost during a firmware update. The factory settings are restored after the update, which also resets passwords.

Back up the configuration file beforehand and reload it afterward (see below).

NOTICE

Damage to the device

If the power supply or the connection to the device containing the firmware is interrupted during the update process, the device may no longer be functional.

- Ensure that the power supply and the connection to the device are maintained during the entire updating process.
- Make sure that all applications running on the device are closed.
- Before updating the firmware, restart the device to prevent memory problems.

In the "Device configuration" area, use the "Update" button to select an update file "*.upd". The selected file will be transferred to the device. To determine whether the selected file is suitable for the device, the system checks it against the following criteria, for example:

- The selected file is an update file.
- The selected update file is more current than the version installed on the device.
- The selected update file is suitable for this device.

If all the criteria are met, the selected update file will be run on the device. The device and the Setup Wizard restart automatically.

Note

The progress of the update is displayed on the screen.

Back up and restore the configuration file

You back up the configuration file of the device either directly on the device via USB or with remote access from a PC, see section "Remote configuration (Page 109)".

The configuration file contains all device-specific configuration settings with the exception of the background image. You can back up the configuration file of a device and, for example, restore it to several devices:

- Use the "Save" button to back up the configuration file for the device to the connected USB drive. To do this, you select a folder in the file system and close the dialog with "OK". The configuration file is stored in the selected folder.
- Use the "Restore" button to restore the backed up configuration file via a connected USB drive, for example if the current configuration file has been inadvertently overwritten. To do this, you select a configuration file from a file dialog and close the dialog with "OK".

  The syntax within the configuration file is checked. If the syntax is free of errors, the configuration file is transferred to the device and the previous configuration file is overwritten. Otherwise an alarm is output.

Note

Saving the configuration file

Back up the current configuration file before and after each firmware update.

You are prompted to enter a password between 8 and 32 characters in length when saving.

Restoring the configuration file

Only configuration files created on the device or via remote configuration are supported for restoration. Configuration files of older V2.x versions are no longer supported.

When you restore, you are prompted to enter the password you assigned when backing up.

IP address conflicts

Do not restore configuration files with identical IP addresses on different devices. Reassign the IP addresses.

Restore to factory settings

Restoring factory settings has the following effects:

- The default configuration file overwrites the configuration file. All connection data for the network, remote access and web browser is reset. The language and screen brightness, the settings and position of the taskbar and on-screen keyboard, and the background image are reset.

NOTICE
Data loss restoring the factory settings
Back up the configuration file and then reload it (see above).

- The administrator password is deleted and must be reassigned at next restart.

Procedure

- Touch the "Restore to factory settings" button. The "Resetting to factory defaults" message is shown on the touch screen. The device reboots automatically if you confirm this message.

Alternative procedure

1. Switch off power to the device.
2. Press and hold the "Factory settings" button on the device and switch on the power supply of the device again. The device restarts.

   Use a sturdy blunt tool made of non-conductive material with a diameter of approximately 5 mm. The "Factory settings" button is next to the interface X1 P1 PROFINET (LAN).
3. Press and hold the "Factory settings" button until the boot procedure has finished and the first commissioning dialog is displayed.

Service device remotely via VNC

Allows remote access to the device. The device has a VNC server for this purpose. With VNC remote access, you can "Permit access to Desktop" or "Permit operation", in other works, enable operation of the plant or machine from the device. You also set the "port" and the "password" for remote access. Remote access must always be protected by a password, i.e. an entry in the "Password" field is required.

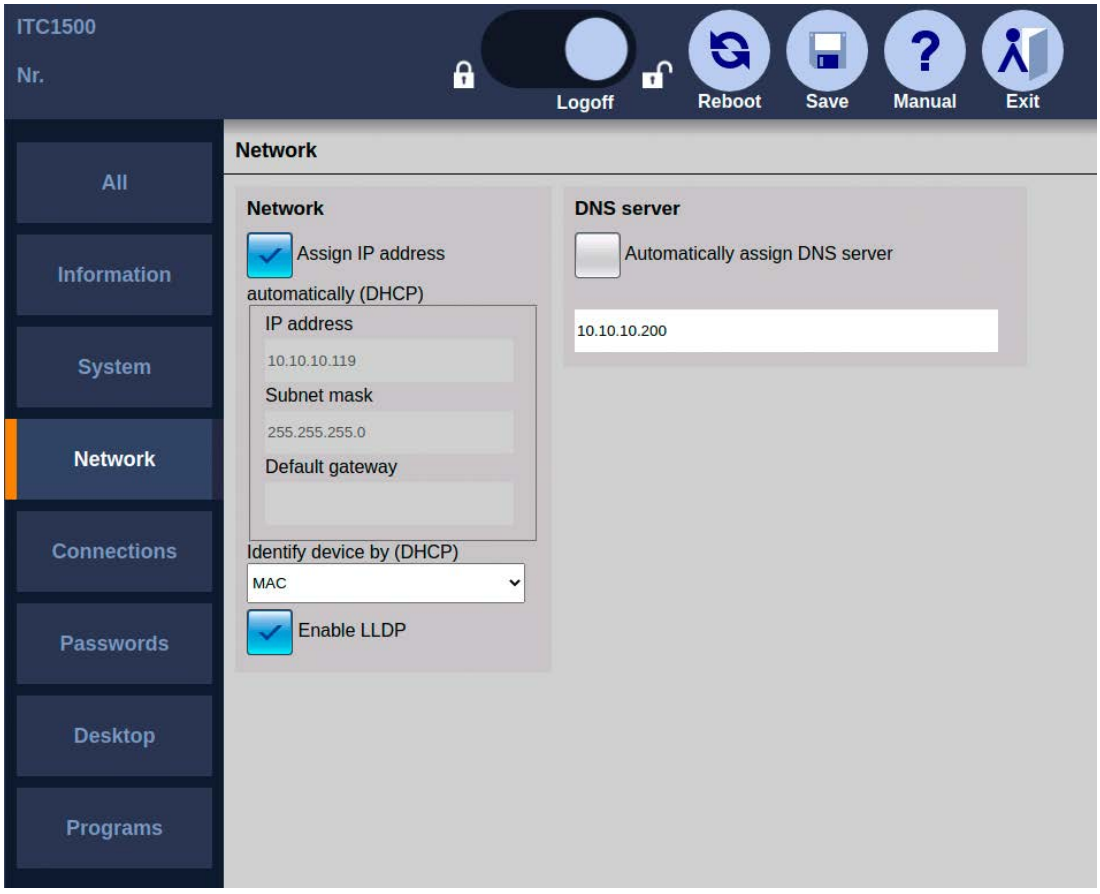
Activating remote configuration

You can use the "Remote configuration" option, "Activate (Web)" to specify whether or not it is allowed to configure the Industrial Thin Client via the Web browser of another device. The configuration settings of the Industrial Thin Client are accessed via an encrypted connection in HTML5 format, which means access must be made with a Web browser that supports HTML5 and encrypted connections (https).

5.5.6 The "Network" submenu

Introduction

The following figure shows the network settings in the Start menu "Configuration > Network".



You can perform the following actions:

- Specify network parameters
- Assign network parameters dynamically
- Use DNS server
- Check valid settings

Specify network parameters

You assign the network parameters either statically or dynamically:

- If "Assign IP address automatically (DHCP)" is not selected, assign a valid static IP address, subnet mask, and default gateway.
- You can also use the "Assign IP address automatically (DHCP)" option to specify that the network parameters will be assigned dynamically by the DHCP server and are therefore not available for assignment (grayed out).

Note

IP address conflicts

Before an IP address is assigned, a check is made to determine whether a device with this IP address already exists in the network. If so, an error message is appears and the address is not assigned. Assign an individual IP address to each device.

The subnet mask specifies the maximum number of nodes, e.g., "255.255.255.0".

Note

Invalid subnet mask

If a subnet mask is invalid, an error message appears and the subnet mask is not assigned. Assign a valid subnet mask.

Activate a PROFINET service under "Enable LLDP" (Link Layer Discovery Protocol) that identifies the Industrial Thin Client in the network as such. If other network components also make their identity known, the management station, such as STEP7, can then detect the network topology automatically.

Assign network parameters dynamically

The following applies only if the "Assign IP address automatically (DHCP)" option is selected.

The device has two features that identify it uniquely. Under "Device identification (DHCP)", you specify the identification feature that the DHCP server uses to identify the device:

- If you select "Device name", the DHCP server identifies the device based on the name stored in the "Device name" field of the system settings, see section "The "System" submenu (Page 85)". If configured correspondingly, the DHCP server searches for the device name in its configuration file and transfers the network settings stored there to the Industrial Thin Client.
- If you select the most common identification parameter "MAC address", the DHCP server identifies the device on the basis of its MAC address.

Use DNS server

You can manually enter the IP address of the DNS server under "DNS server". If you select the "Automatically assign DNS server" option, the manual IP address is overwritten by an IP address assigned by the DHCP server. This requires that the "Assign IP address automatically (DHCP)" option is also selected.

Note

No connection between client and server

If you edit the configuration settings from an external PC, take the following into account: The connection can be interrupted as soon as you enter a different IP address in "IP address" or select the "Assign IP address automatically (DHCP)" option.

If you edit the configuration settings locally on the device, the connection to the configuration settings will be maintained even if you change the IP address in the configuration settings.

If the "Assign IP address automatically (DHCP)" option is selected and no DHCP server is available, no IP address will be assigned to the device. Communication between the server and device is not possible.

- Start the configuration settings locally on the device, and assign an IP address to the device that is not already used in the network.

Alternatively, you can select the "Assign IP address automatically (DHCP)" option with "Device name".

Note

A maximum of 240 characters is permitted. For connections via RDP, the device name will be automatically truncated to the first 15 characters at logon.

Check valid settings

In the Start menu "Configuration > Information", the network settings that are currently valid are always shown, regardless of whether they were assigned statically or dynamically. Use this approach to check whether the change in the network settings was accepted or not.

See also

PROFINET basic functions (Page 100)

5.5.7 The "Connections" submenu

Introduction

Users can connect from the Thin Client to different servers. Example:

- RDP Server 1: Access to office planning documents
- VNC Server 2: Access to Office spreadsheets
- Sm@rtServer 3: Access to WinCC messages at the plant
- WinCC OA-Server 4: Access to WinCC OA workstations
- Web-Server 5: Access to web-based content, for example, of an S7 controller (PROFINET) or Intranet/Internet using the integrated web browser.

Note

Web connection and web browser

You can configure a Web connection, for example, the server address, via the connection settings, see section "Connection settings (Page 96)". You configure the Web browser itself and its proxy settings in the application settings, see section "The "Programs" submenu (Page 106)".

You can establish up to 5 such client-server connections at the same time. These connections are specified mainly by the following parameters:

- Connection type, e.g., "Sm@rtServer" or "RDP"
- IP address of the server
- Port of the server

The Industrial Thin Client then displays the server screen as a full screen.

This section shows how you configure client-server connections. The connection settings can be found in the configuration settings in the Start menu "Configuration > Connections".

Displaying client-server connections in the taskbar

The "Display connection (favorites)" option is enabled by default so that the client-server connection appears in the start bar (under "Favorites") and can be started from there. The favorites contain a maximum of 10 client-server connections.

It makes sense to disable the "Show connection (Favorites)" option, for example, when the associated server must be serviced at regular intervals.

Factory default settings

- "Obtain IP address automatically (DHCP)"

Note

Unauthorized access

To prevent unauthorized persons from logging on and gaining free access to the configuration settings and client-server connections, you should immediately assign a new administrator password after first commissioning or restoring of factory settings.

Note

Avoiding malfunctions

The factory default is that the IP address is assigned dynamically (DHCP). If you disable the "Obtain IP address automatically (DHCP)" option, there is no static IP address ("0.0.0.0"). Therefore, assign an individual IP address to each device.

Some client-server connections have already been created as examples. Set up client-server connections with valid IP addresses.

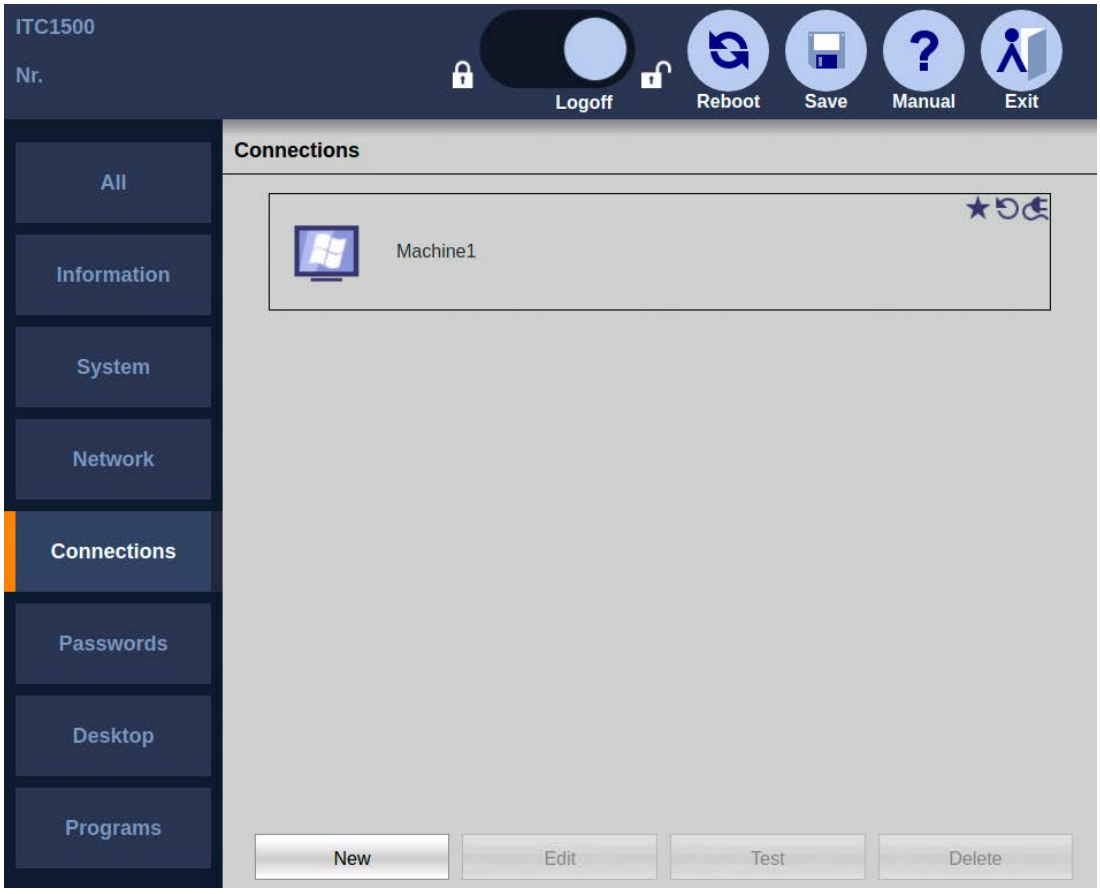
See also

PROFINET basic functions (Page 100)

5.5.7.1 Setting up client-server connections

Structure of the tab

The following figure shows the list of client-server connections in the Start menu "Configuration > Connections".



Below the list there are buttons for editing a selected client-server connection.

Buttons

The buttons have the following functions:

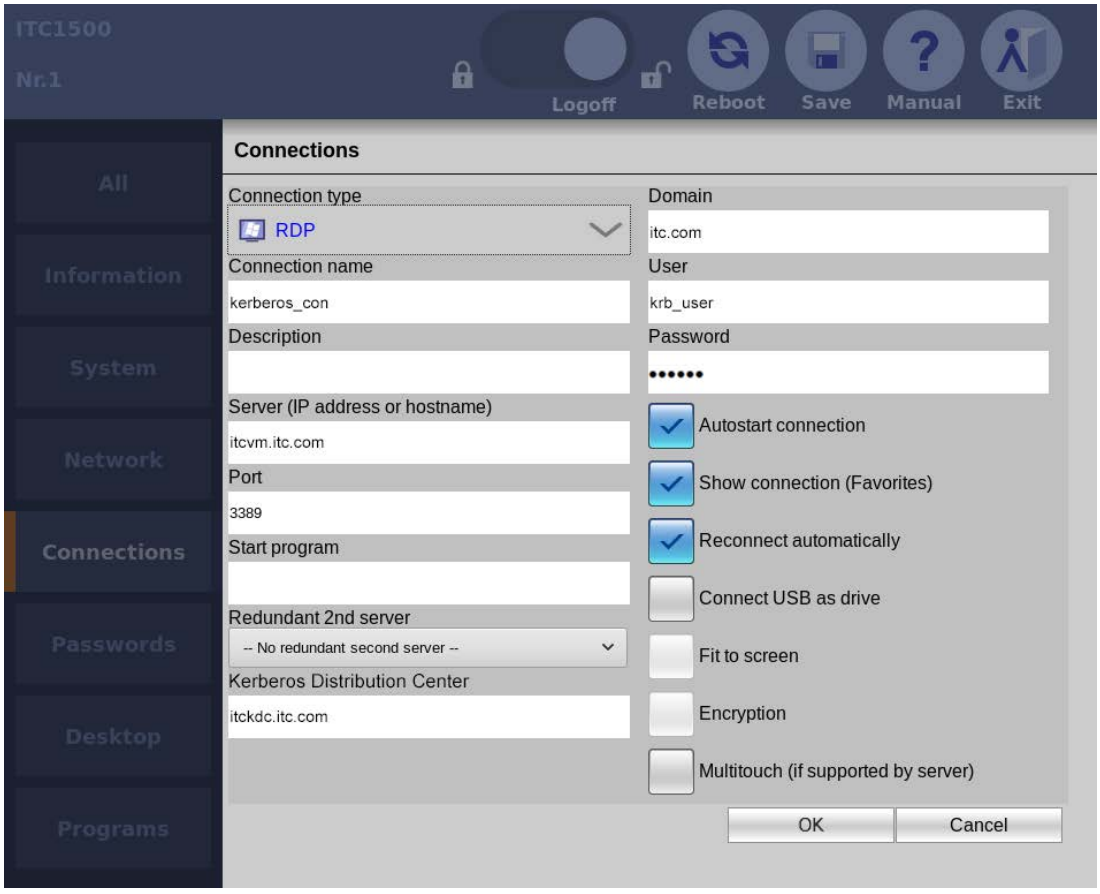
- "New": creates a new client-server connection.
- "Edit": opens the connection settings of the client-server connection.
  Same dialog as "New" with the only difference that the "Connection type" can no longer be changed.
- "Testing": Checks if the server and port can be reached (ping).
- "Delete": deletes the client-server connection.

See also

Opening the configuration (Page 81)

5.5.7.2 Connection settings

By way of example, the following figure shows the connection settings for an RDP connection in the Start menu "Configuration > Connections".



You select a client-server connection, or create a new one. The following connection settings can be specified:

Note

Grayed-out fields

Not all connection settings are available for each connection type (exception: RDP). Connection settings that are not required are grayed out.

- The "Connection type" specifies the type of client-server connection, e.g. RDP connection, VNC connection, etc.
- In "Connection name", you enter a name for the client-server connection, e.g. "Server screen 1". The client-server connection will then appear with this name in selection menus. If the operator selects "Server screen 1" in the taskbar, for example, the client-server connection configured with this name will be started.
- In "Description", you enter a text for the client-server connection. This description then appears in selection menus under "Connection name".
- Under "Server (IP address)", you specify an IP address or host name at which the server can be reached.
- In "URL" ("Web" connection type only), you specify an Internet address at which the web server can be reached.
- The default port is set under "Port". RDP: 3389, Sm@rtServer/VNC: 5900.
- In "Start program" (RDP only), you specify the software program that is automatically started on the server with this RDP connection. For this function, a "Server" type operating system is required on the server PC. The server must be configured accordingly.
- Under "Redundant 2nd server" (RDP only), select a second RDP connection that is already configured. If the first RDP connection configured here fails, the second RDP connection will be started (fallback). And vice versa: If the second RDP connection fails, the first RDP connection will be restarted.

  To use two redundant RDP connections, the following options must be enabled for both connections:
  - "Show connection (Favorites)"
  - "Reconnect automatically"
    If the "Redundant 2nd server" and "Reconnect automatically" options are enabled, three attempts, with a time interval of about 15 seconds, are made to restore the currently active connection before the start of the other connection.
- Under "Kerberos Distribution Center", enter the name of the Kerberos server for Kerberos authentication.

  For a successful RDP connection with Kerberos authentication, fill in the following input fields:
  - "Kerberos Distribution Center": Computer name of the Kerberos server.
  - "Server": Computer name of the server that the client wants to use.
  - "Domain": Name of the domain in which both servers are located.

The required data can be found in the basic information of the respective server in Windows.

You also require:

– A working DNS server.
– Working DNS resolvers on the participating machines in the Kerberos realm.

Enter the IP address of the DNS server in the network settings of the Industrial Thin Client under "DNS server", see section "The "Network" submenu (Page 91)".

- You specify the logon information for logging the device onto the server under "Domain" (RDP, Citrix), "User" (RDP, Citrix, WinCC OA), and "Password".

Note

Password length

With the connection to a Sm@rtServer with WinCC Advanced (TIA Portal) V13 or higher, a password length of more than eight characters is supported after the "Encryption" checkbox is selected.

WinCC OA

In WinCC OA, the "User" and "Password" fields are used for HTTP download of Runtime. Logon in the WinCC OA logon screen is therefore not possible. A password is required to assign a user name.

- If you select "Autostart connection", this client-server connection is automatically established when the device is restarted or rebooted and after modified configuration settings are saved. "Automatic start connection" only works when the "Display connection (favorites)" flag is set for the connection.

Note

Limited number of client-server connections

A maximum of 5 client-server connections can be started at the same time. An error message appears when a 6th connection is activated.

- If you select "Show connection (favorites)", this client-server connection will appear in the taskbar under "Favorites". If the favorites contain 10 connections, you cannot add an additional connection, and this option is no longer available.

  If you deselect the option, the client-server connection is not visible to the operator and can only be started by the administrator in the Start menu "Configuration > Connections" via the "Test" button.

- If "Reconnect automatically" is selected, the device continually attempts to restore a physically interrupted connection to the server. This procedure can be aborted by closing the connection via the taskbar.

Note

Only one user with RDP on Windows operating system

If a second client has established the same RDP connection to the server with the identical logon information, the client-server connection of the first client is interrupted. Even if "Reconnect automatically" is enabled, the device does not try to re-establish the connection to prevent a ping-pong effect between the clients.

Note

Re-establish RDP connection after a server restart

If "Reconnect automatically" is activated for an RDP connection and the server has to be restarted, proceed as follows:

1. Restart the server.
2. Re-establish the RDP connection.

Note

Timeout of the function "Reconnect automatically" for an RDP connection

The function "Reconnect automatically" for an RDP connection attempts to re-establish the connection for a period of about 15 seconds. If this is not possible, the function "Reconnect automatically" is canceled.

- If you select the "Connect USB as drive" option (RDP only), you can access a USB memory device connected to the Industrial Thin Client on the touch screen. The USB data are transferred to the server and displayed there in Windows Explorer for the devices. For additional information, see section "Use USB memory devices (Page 123)".

Note

Security threat to the system

Viruses, trojans, or spam, for example, can reach the server through USB. Use a suitable virus scanner to check the data on the USB memory device, or deselect the "Connect USB as drive" option.

Non-supported operating systems

The "Connect USB as drive" function is currently not supported for the following operating systems of the connection partner:

- Windows Server 2012, 64-bit

- If "Automatic scaling" (only with connection types "Sm@rtServer" and "VNC") or "Full screen" (only with connection type "Web") is enabled, then the Industrial Thin Client scales the server screen to its own display size.
- When "Encryption" is enabled (Sm@rt connection only), the data is transferred encrypted between client and server. In this case, activate encryption on the server as well.

  If the server does not support this function, an error message will be displayed. Depending on the height-to-width ratio, the server screen is displayed within a black bar.

- When "Multitouch" is enabled, you can use a server with a multitouch-capable operating system in multitouch mode.

Note

Server operating system with multitouch support required.

When you enable the "Multitouch" setting for the connection to a server with a **non-**multitouch-capable operating system, it is **not** possible to operate the server via the Industrial Thin Client. Only enable the "Multitouch" setting for the connection to a server with a multitouch-capable operating system.

For VNC and Sm@rtClient connections, only "single-touch"

The VNC protocol used for VNC connections andSm@rtClient connections does not support multitouch functionality.

The server may only be operated with one finger for VNC and Sm@rtClient connections. Do not use multitouch gestures.

5.5.7.3 Setting up startup connection

Introduction

You can designate each client-server connection as an autostart connection. This means that this client-server connection will also be started every time the device starts. The autostart connections can be restarted even after the configuration settings have been changed.

Note

Limited number of client-server connections

A maximum of 5 client-server connections can be started at the same time. If a 6th connection is activated, an error message appears

The order cannot be defined for startup. Therefore, which of the autostart connections will ultimately be displayed on the screen is undefined. However, you can generally switch between the client-server connections.

Procedure

Proceed as follows to identify a client-server connection as an autostart connection:

1. Choose "Configuration > Connections" in the Start menu.
2. Select a client-server connection.
3. Touch the "Edit" button to confirm.
4. Select the "Autostart connection" option.

5.5.7.4 PROFINET basic functions

Introduction

The PROFINET basic functions help to diagnose the device using standard mechanisms. The required diagnostics functions are available, for example, in STEP 7.

Functions

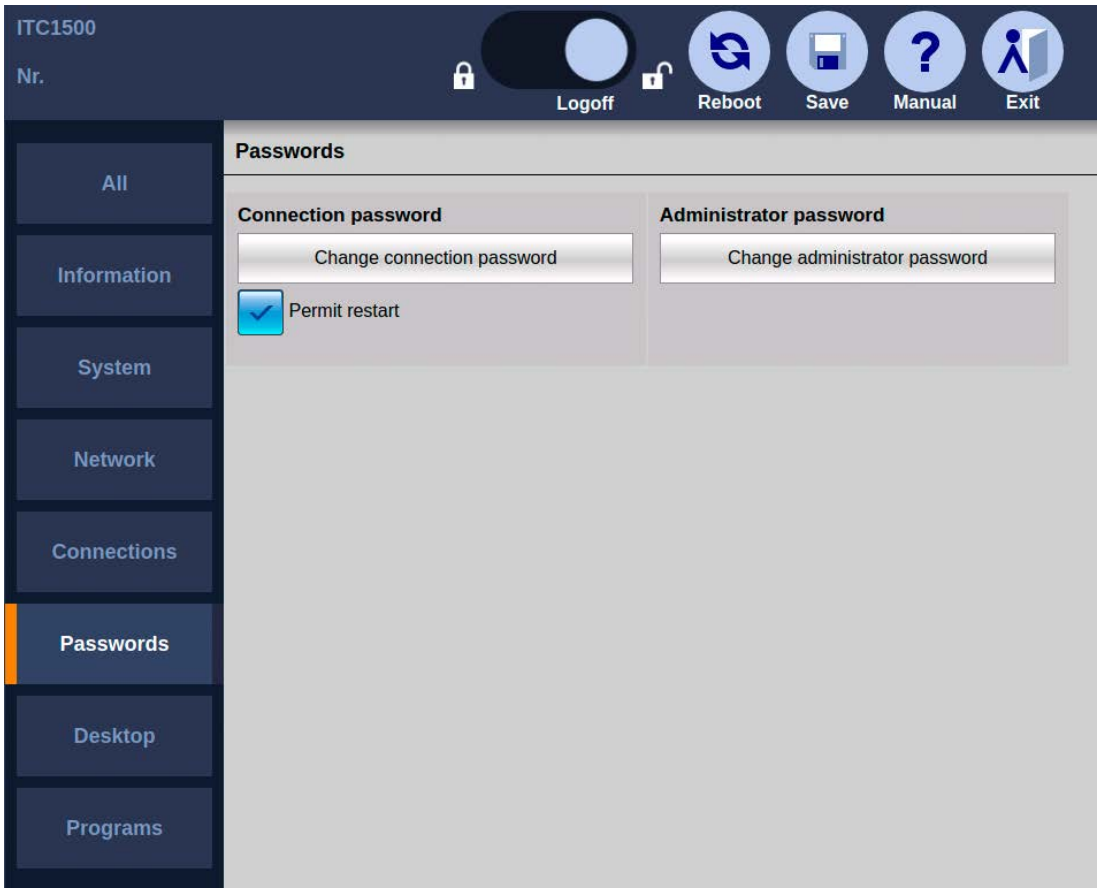
As of SIMATIC Manager V5.4, SP2, the PROFINET basic functions offer the following functions:

- As soon as the device is connected to PROFINET, it is displayed as an available device in the Lifelist in SIMATIC Manager. You can view the properties of the device, e.g., IP address.
  Additional information from the "Target system" context menu is not supported by the device.
- You can assign a name and an IP address to the device in SIMATIC Manager under "Target system > Edit Ethernet device".
- As of TIA Portal V12: The device can be configured in the topology editor.

5.5.8 The "Passwords" submenu

Introduction

The following figure shows the password settings in the Start menu "Configuration > Passwords".



Note

Forced termination of connection

When you save the changed configuration settings, all open client-server connections are terminated and all open programs are closed without a confirmation prompt. The configured autostart connections are re-established.

Logging in as an administrator

A user that is not logged on can operate the Start menu, but only the device data from the configuration settings will be visible ("Configuration > Information").

To edit the configuration settings, follow these steps:

1. Move the blue circle (slider) "Logon" in the toolbar to the right.
2. Enter the administrator password.
3. Click the "Logon" button to close the dialog.

You are logged on as administrator.

Logging off as an administrator

To protect the configuration settings from unauthorized access from the outside, follow these steps:

1. Move the blue circle (slider) "Logon" in the toolbar to the left.

You are logged off as administrator.

Changing the administrator password

During first commissioning or restoring of factory settings, you are prompted to assign a new administrator password.

Note

Unauthorized access

To prevent unauthorized persons from logging on and gaining free access to the configuration settings and client-server connections, you should immediately assign a new administrator password after first commissioning or restoring of factory settings.

The administrator password can be changed in the "Configuration > Passwords" Start menu.

1. Touch the "Change administrator password" button. The "Change password" dialog opens.
2. Enter the old password.
3. Assign a new password.

   Note that the number of characters is limited to a minimum of 8 and a maximum of 32. It is possible to enter a blank administrator password, but not a space as the administrator password.

4. Repeat the new password.
5. If you select "Hide passwords", the password is no longer shown when you log on.

Forgetting the administrator password

If you forget your administrator password, you must restore the factory settings.

Note

Losing the current configuration settings

When restoring to factory settings, the current configuration file is overwritten.

After factory settings are restored, a saved configuration file can be transferred back to the device.

Once the configuration file is restored, the password contained therein will be valid after the device is restarted. Change the password if necessary, and make a note of it.

Closing connections with connection password

You can specify a password for terminating a client-server connection in the Start menu "Configuration > Passwords". If the operator wants to terminate a connection, this connection password must be entered. If the operator enters an incorrect password, the connection will not be terminated.

Note

Misuse

No connection password is assigned in the factory state. Without password protection it is possible for unauthorized persons to terminate client-server connections.

Following initial commissioning and after restoring the factory settings, you should immediately assign a connection password.

Closing Citrix and connection password

When an operator closes a Citrix application program via the user menu or closes the Windows window, Citrix is also terminated without entering the connection password.

The length of the connection password is restricted to a maximum of 30 characters.

Note

If a connection password has been specified, you can alternatively terminate a client-server connection by using the administrator password.

If you select "Allow restart", the menu entry "Restart" will be displayed underneath in the Start menu. The operator can use this entry to restart the device.

Changing the connection password during ongoing operation

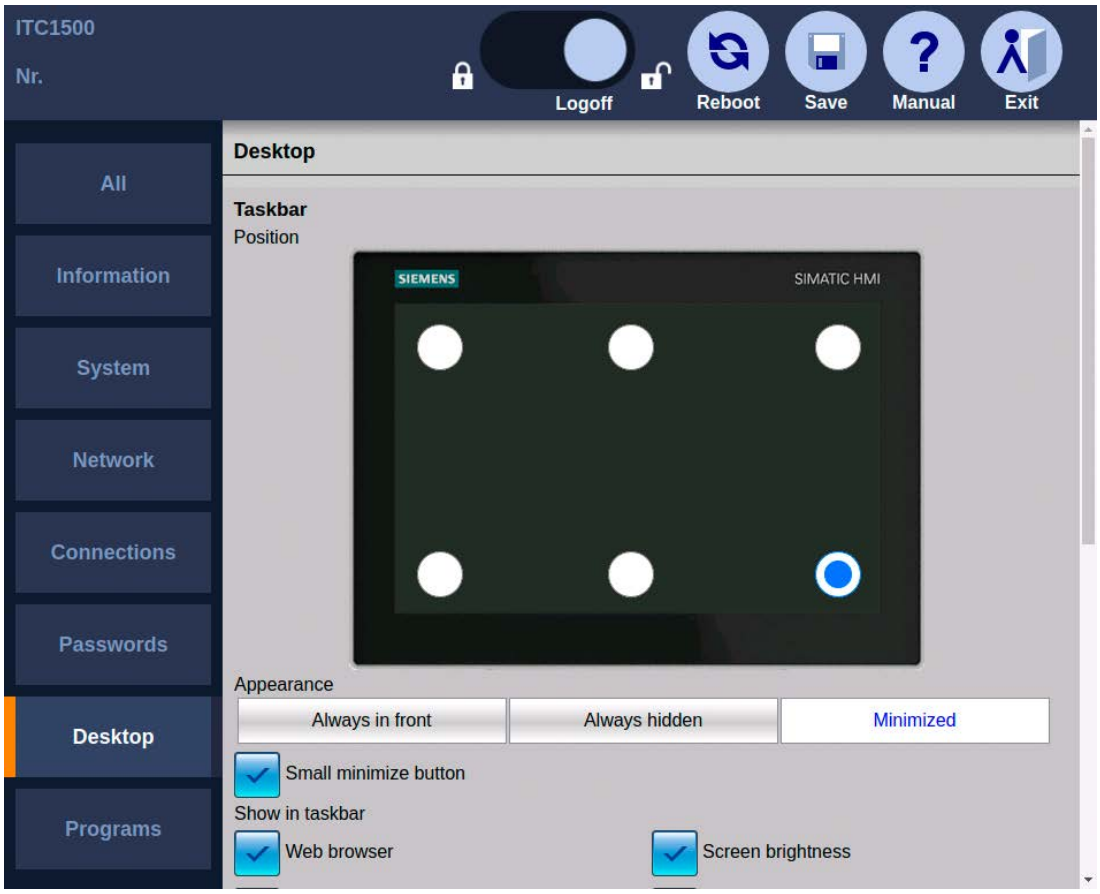
Changing the connection password works in the same way as "Changing the administrator password" (see above), for example from an external PC, while the operator is working on the device. The change of the connection password becomes effective immediately. The operator can then only terminate the current client-server connection with the new connection password.

You can also change the connection password by entering the administrator password instead of the old connection password.

5.5.9 The "Desktop" submenu

Introduction

The following figure shows the desktop settings in the Start menu "Configuration > Desktop".



You can make the following settings:

- Position of the taskbar
- Display of the taskbar
- Menu entries in the Start menu
- Size and position of the on-screen keyboard

- Desktop orientation
- Background image

Specifying the position of the taskbar

Touch one of the 6 buttons on the displayed touch screen. The configuration settings will be saved and the taskbar will then be moved to the corresponding position. The taskbar cannot be moved with drag&drop. The default position of the taskbar is "Bottom center".

Specifying the display of the taskbar

- "Always in front" (default setting)

  The taskbar is displayed after the device is switched on. The buttons to minimize or maximize the taskbar are not displayed. The operator cannot change the taskbar.
- "Always hidden"

  The taskbar is hidden. The operator cannot display the taskbar and, thus, cannot make any changes to the active client-server connections. Because the configuration settings cannot be opened without the taskbar, this setting can only be disabled again with external access, see section "Remote configuration (Page 109)".
- "Minimized"

  The taskbar is minimized in the display. The operator can maximize or minimize the start bar using the appropriate buttons, which are always shown.

Specify size of "Minimize start bar" button

If the "Minimize small button" option is enabled, the height of the "Minimize" button is reduced by half.

Specifying menu entries in the Start menu

The settings show the menu entries of the Start menu in the taskbar.

- Web browser
- Screen brightness
- Clean screen
- USB devices

If you select a menu entry, it will be displayed. If you deselect a menu entry, it will be hidden and can no longer be called.

Specifying the size and position of the on-screen keyboard

In "Position", you can dock the on-screen keyboard at the top or bottom edge of the screen. In "Size", you select one of 5 predefined keyboard sizes.

Setting the desktop orientation

Under "Desktop orientation", select the entry "Landscape (0°)" or "Portrait (90°)" depending on the mounting position of your device.

Setting up a background image

Under "Background image", specify a graphic file to be displayed as the background image. Use the "Browse" button to select a graphic file on the connected USB drive.

Note

Required properties of background images

- Format: PNG, JPG, JPEG
- File size: max. 5 MB
- Resolution: Maximum 1920 x 1080 for ITC2200
- Colors: Maximum 16777216

Display of the background image

- The background image is always stretched to fit the screen resolution, even when this distorts it and grossly enlarges it.
- Therefore, the background image should have exactly the same width x height as the screen resolution, for example 1280 x 800, or at least the same proportions, for example 640 x 400.

Restoring the factory settings

The background image is restored.

See also

Structure and functions of the taskbar (Page 117)

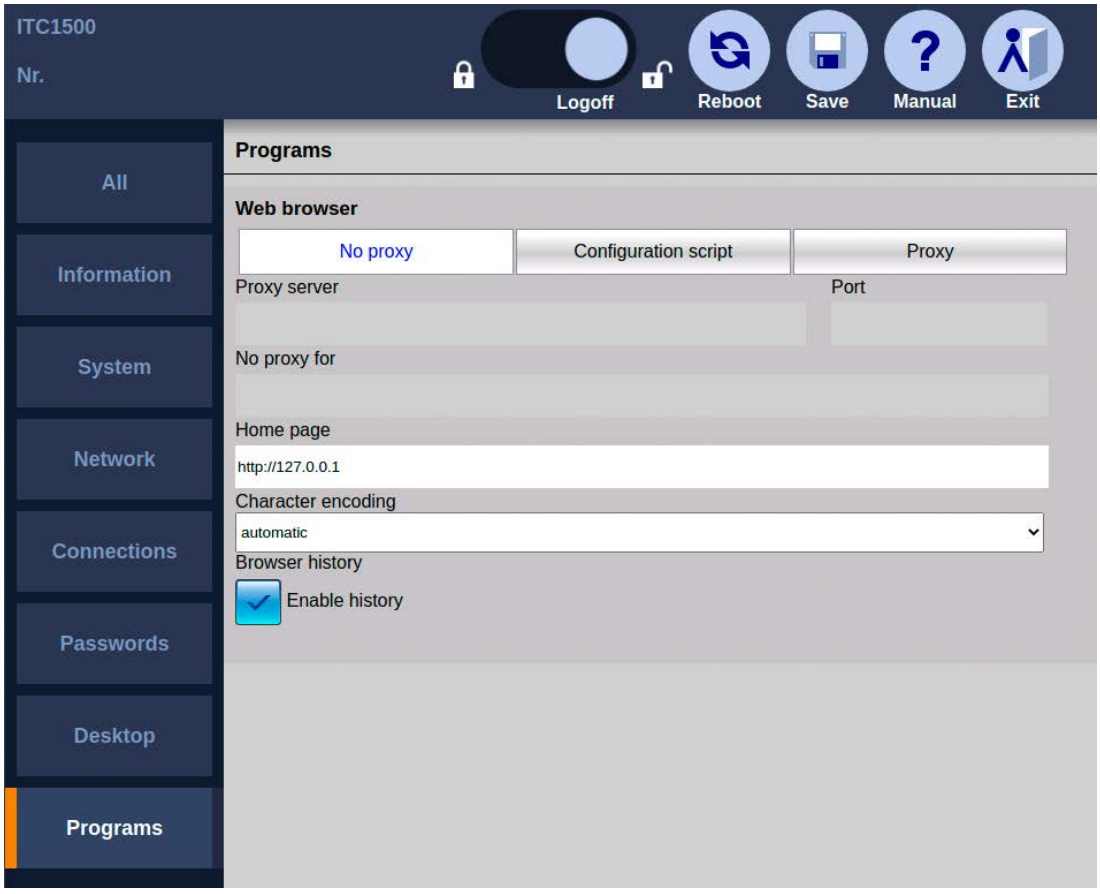
Starting a connection (Page 119)

5.5.10 The "Programs" submenu

Introduction

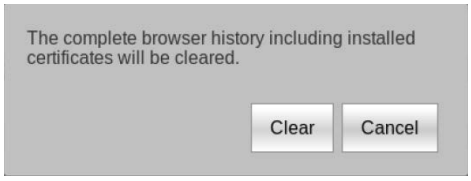
Additional, configurable application programs (software applications) can run on the Industrial Thin Client. The web browser is currently the only application.

The following figure shows the web browser settings in the Start menu "Configuration > Applications".



- If "Proxy" is selected: Enter the address of a central connection node in "Proxy" if your network accesses the Internet from this connection node, e.g., in order to filter web contents or make them available in the cache. In case of doubt contact your system administrator.
- If "Configuration script" is selected: In "Configuration script", specify the address of a script that picks out the appropriate proxy server for each web address. The configuration script contains a JavaScript function with proxy specifications, e.g., for the case that a server does not answer. The configuration script is provided by your network administrator.
- For addresses that you enter in "No proxy for", there is no proxy server request, and a direct connection to the Internet or an intranet will be established instead. Use a comma to separate multiple addresses (see "Proxy bypass").
- If "No proxy" is selected, there is no proxy server request, and a direct connection to the Internet or an intranet will be established instead.
- Under "Port", specify the internal port at which the proxy server can be reached: The default is 8080.
- In "Home page", specify an Internet address that will be called automatically when the web browser starts.

- With "Character encoding", you specify the character set that is used by the web browser if a web page does not provide any information about the character set to be used. The character set "UTF-8" is set by default. You can have the appropriate character set determined "automatically". If characters are represented incorrectly, you can also change to "ISO-8859-1".
- When the "Browser history" has been enabled, the web browser saves data such as websites visited, certificates and cookies. If this function is subsequently disabled, the following dialog is displayed:



  The saved data is deleted again with the "Clear" button.

  The "Enable history" function is disabled in the delivery state of the Industrial Thin Client.

Proxy bypass

You can make the following entries in the "No proxy for" field:

Object for which no proxy is to be used	Content of the input field "No proxy for"	Example	Comments
Domain	Suffix of the domain	".siemens.com, siemens.com"	Both suffix variants must be entered in order to exclude an entire domain.
Host name (without domain)	Host name only	"MyWinPC"	Excludes "MyWinPC".
Host name (with domain)	Host name and domain	"MyWinPC.siemens.com"	Excludes "MyWinPC".
IP address	IP address	"192.168.1.0"	Excludes the device with the IP address "192.168.1.0".
Network	IP address range	"192.168.1.0/24"	Closes all devices with an IP address ranging from "192.168.1.0" to "192.168.1.24".

Placeholder characters are not permitted, e.g. "*" or "192.168.*.*".

No entries are set as default.

The "localhost" and "127.0.0.1" objects are always excluded. No proxy is used for these objects.

Adjusting the display in the web browser

You can enlarge or reduce the display in the web browser:

- Use the key combination <CTRL><+> to enlarge the display.
- Use the key combination <CTRL><-> to reduce the display.

Note

Depending on the keyboard you are using, it may be necessary to press the Shift key to access the "+" and "-" keys. In this case, use <Control><Shift><+> to enlarge the display and <Control><Shift><-> to reduce it.

5.5.11 Remote configuration

Introduction

Remote configuration enables remote configuration and remote update of a SIMATIC Industrial Thin Client from a PC that is connected to the Industrial Thin Client via a network.

Functions

You can perform the following actions from a central PC for an Industrial Thin Client:

- Edit configuration settings
- Back up and restore the configuration
- Identifying a device
- Change IP addresses
- Update firmware
- Restart devices

Remote access

During remote access, you perform the corresponding configuration functions directly on the Industrial Thin Client, i.e. the user interface corresponds to the user interface on the Industrial Thin Client itself.

The remote access to the Industrial Thin Client is made via an encrypted connection in HTML5 format, which means access must be made with a Web browser that supports HTML5 and encrypted connections (https).

Requirement

- The Industrial Thin Client and the PC for remote access are located in the same subnet.
- The "Remote configuration" option is activated in the system settings of the Industrial Thin Client (Page 85).
- A Web browser that supports HTML5 and encrypted connections is installed on the PC.

Procedure

1. Open the Web browser.
2. Enter the IP address or device name of the Industrial Thin Client that you want to configure in the address line of the Web browser.

If a message appears regarding the certificate for the encrypted connection, confirm the message.

5.6 Configuring the server

5.6.1 RDP

5.6.1.1 RDP overview

Introduction

RDP, "Remote Desktop Protocol", is a protocol that the Industrial Thin Client uses to access a server with a Windows operating system, e.g. Windows Server. The Industrial Thin Client can access all programs running on the server, if the programs have been enabled for remote access. The following statements also apply accordingly to Windows 7.

Licensing the Windows Server

You do not require any licenses on your device to access the server. You require the following server licenses:

- One Windows Server license per server
- One Windows Server Client Access License (CAL) per user
- Additionally, one Terminal Server Client Access License (TS User CAL) per user that can be used independent of the device

Note

TS Device CAL cannot be used

In the case of the "TS Device CAL" license, which can be used on a certain device independently of the user, the device is logged onto the license server using the last four digits of the MAC address. When you replace the device, the license is blocked by the license server and released again after about 3 months.

User CAL and Device CAL licenses are supported for all approved Windows operating systems.

Detailed information on licenses and applicable conditions of use are available on the Internet under "Windows Server 2003 Terminal Server Licensing (http://www.microsoft.com/windowsserver2003/techinfo/overview/termservlic.mspx)".

Licensing Windows 7

You do not require any licenses on your device under Windows 7 to access the server. Only one license on the PC for your operating system, e.g. Windows 7.

You do not require any additional licenses on the server for Remote Desktop.

See also

System requirements (Page 75)

5.6.1.2 Administration on the server

Administration Windows Server

The administration on the server depends on the individual IT infrastructure. Establish the settings for the server configuration under the following menu commands under "Start > Programs > Administrative Tools:"

- Terminal services configuration
- Terminal services administration
- Terminal services licensing

You will find more information on the Internet in the "MSDN Knowledge Base" of the "Microsoft support (http://support.microsoft.com)".

You can specify on the server that certain users of the Industrial Thin Client can only access specified programs on the server.

When the device is configured, you assign a password for the connection to the server. If the device establishes a connection to the server, a password will be requested by default irrespective of this. Under "Start > Programs > Administrative Tools > Terminal Service Configuration" you can specify that the password is not requested again.

Administration Windows 7

In order for the Industrial Thin Client to access the server, you must enable remote access on the server. You can enable remote access under "Start > Settings > Control Panel > System > Remote" with the option "Allow users to establish a remote desktop connection." Use the "Select remote users" button to open a dialog in which you select the users that are authorized to access the server.

In addition, you enable the server ports that have been set for remote access in the firewall.

Keyboard language

An English and German on-screen keyboard is available on the device. Depending on the delivery version of the device, additional languages may be available, for example, Hungarian or Spanish. Set the keyboard language on the device so that it matches the keyboard language on the server. If the keyboard languages on the device and the server are different, the keys pressed on the device keyboard will not be interpreted correctly on the server.

Configuring double-click

If it is too difficult to double-click the touch screen with your finger or the touch stylus, then make the setting in Windows Explorer on the server that files and folders should open with a single click under "Tools > Folder options > General > Click items as follows".

You have the option to establish a greater range in which two clicks can be detected as a double-click under [HKEY_CURRENT_USER\Control Panel\Mouse] in the Windows registry of the server. Under "DoubleClickHeight" and "DoubleClickWidth" enter 10 pixels, for example.

Windows 10

If you connect via RDP to a Windows 10 PC on which another user is already logged on, the user must confirm your access to the PC. Alternatively, you can wait 30 seconds to get access automatically. However, the connection is then often interrupted with the misleading error message "Session was disconnected because of unknown error".

5.6.2 Citrix

5.6.2.1 Citrix overview

Introduction

The Citrix Receiver software provides business applications centrally for any terminal devices at all business locations as on-demand service. This may take place in form of hosted applications that are executed on a server in the company data processing center. Rollouts of new applications, updates and patches are thus available immediately to all users.

Citrix server licensing

To access the Citrix server, you do not require any licenses on your device. Depending on your specific requirements, you need a Citrix XenApp or XenDesktop server.

See also

System requirements (Page 75)

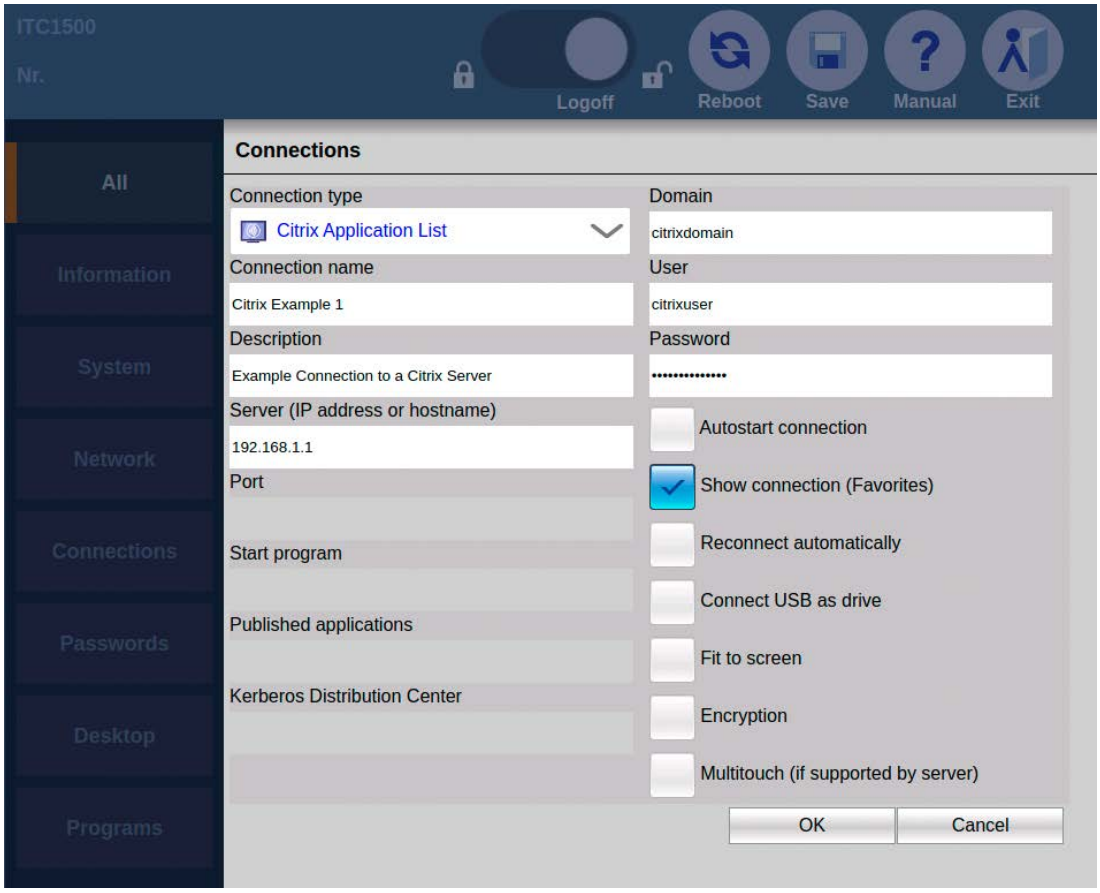
5.6.2.2 Connecting to a Citrix application or a desktop

To access a Citrix application or a desktop, you have the following two options:

- Connection type "Citrix Application List"
- Connection type "Citrix Single Application"

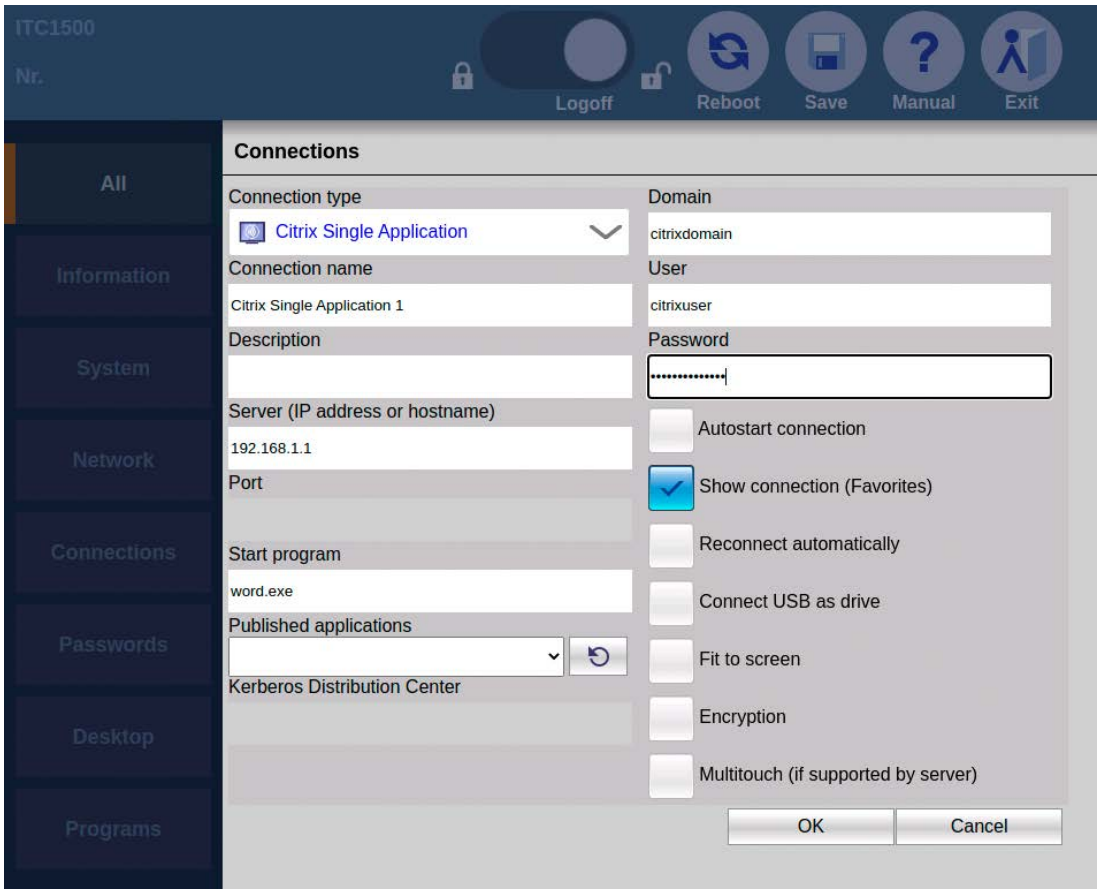
Connection type "Citrix Application List"

You specify all parameters of the Citrix connection with the exception of the application that is to be opened. When the connection is started, the user can select which application is opened.



Connection type "Citrix Single Application"

You specify all parameters of the Citrix connection including the application that is to be opened when the connection is started.



In order for applications to be shown in the start bar, they have to be configured as favorites on the server.

Depending on the server configuration, you can also access these applications or desktops via the Web browser.

5.6.2.3 Restrictions

The following restrictions apply to the Citrix client of the HMI device:

- Automatic scaling is not supported.
- Access to USB storage media is not supported.
- Read/write access to the local file system is not supported.
- Only one connection can be active at any given time. A message is displayed if you try to open a Citrix connection while a Citrix connection is already in place. The user is informed that the existing connection must be closed before the new connection can be established.

- The following functions are not available during the configuration of Citrix connections:
  - "Autostart connection"
  - "Reconnect automatically"
- The Citrix client supports the following certificates:

Certificate	Issuer
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust

5.6.3 VNC

Introduction

Use VNC for remote control of another computer via a network. VNC is the abbreviation for "Virtual Network Computing" and shows the desktop of another computer. In contrast to RDP, all clients display the same server screen.

Requirement

The operating system you use does not play a role because the software is available for all current platforms. The connection via the network uses the TCP/IP protocol and should be configured with a password for security reasons.

Layout

VNC works according to the client-server model. The program consists of the server module VNC server and the client component VNC Viewer. The server program runs on the computer whose screen outputs you want to monitor, whereas the clients receive the screen outputs and in turn send keyboard and mouse inputs to the server.

See also

System requirements (Page 75)

5.6.4 Sm@rtServer

Introduction

With the SIMATIC WinCC Sm@rtServer option, HMI devices communicate with each other via PROFINET. Sm@rtServer thus enables client/server configurations for distributed operator stations in a system.

A description of the Sm@rtServer configuration can be found in the online help of WinCC or in the "WinCC Professional Options" manual.

Requirement

A server HMI device on which the Sm@rtServer has been started is required for client/server operation via Sm@rtServer.

Operating principle

If the Sm@rtServer has been started on a server HMI device, the Industrial Thin Client can access the server HMI device via the "Sm@rtServer" connection type. Depending on the configuration of the Sm@rtServer on the server HMI device, the Industrial Thin Client can monitor or operate the project on the server HMI device.

Licensing

You do not require any licenses in order to access an HMI device. The SIMATIC WinCC Sm@rtServer option is license-free as of WinCC V14 (TIA Portal). There can only be a project compiled with the Sm@rtServer option on the server HMI device you are accessing with the Industrial Thin Client.

See also

System requirements (Page 75)

5.6.5 WinCC OA

Introduction

SIMATIC WinCC OA (Open Architecture) is a SCADA system for visualizing and operating processes, production work-flows, machines and plants in all industries. As of WinCC OA V3.16, ITC V3 devices are supported.

You can find the description of WinCC OA configuration in the online help of WinCC OA under "Special Functions > Industrial Thin Client". You can find additional information on the Internet at SIMATIC WinCC Open Architecture (https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-oa/wincc-oa-basic-software.html).

Requirement

A SIMATIC WinCC OA server that supports Industrial Thin Clients is a requirement for operating a SIMATIC WinCC OA connection.

Operating principle

The Industrial Thin Client operates similarly to a SIMATIC WinCC OA WebClient.

The WinCC OA server provides the client components to the Industrial Thin Client.

Licensing

You do not require any licenses on the Industrial Thin Client in order to access WinCC OA. The license is covered by the user interface license on the WinCC OA server. More on this in the online help of WinCC OA.

See also

System requirements (Page 75)

5.7 Operating ITC

5.7.1 Notes on Sm@rtServer access

Monitoring mode

If you access a device on which only monitoring mode has been configured for Sm@rtServer access, you can only monitor the device; you cannot intervene for control purposes.

Operating right for Sm@rtServer

When you access a device, it is possible that this device is being used at the time. In this case, the Industrial Thin Client does not have operating rights.

If you touch the touch screen, a message is displayed stating that no operator input is possible. How you request or force operating rights depends on the configuration on the device you are accessing with the Industrial Thin Client.

5.7.2 Operating the taskbar

5.7.2.1 Structure and functions of the taskbar

If the taskbar is configured accordingly in the desktop settings, the taskbar will be displayed after the device is switched on. See also section "The "Desktop" submenu (Page 104)".

The operator cannot change the position of the taskbar on the touch screen, but the administrator can do so in the desktop settings.

Functions

The following functions can be called from the taskbar.

Start menu

- Web browser: opens the integrated Web browser, which displays the device information as the homepage by default, see also section "The "Information" submenu (Page 84)". The web browser supports HTML, XML, CSS, JavaScript and Java so that you can establish any type of connection to the Intranet/Internet.
- Screen brightness: adjusts the screen brightness of the background lighting. Two buttons "+" and "-" are displayed on the right for this purpose.
- Clean screen: You use this function to disable the touch screen for input for a period of 15 seconds, for example, if the screen is being cleaned, see section "Cleaning the device (Page 165)".
- USB devices: see section "Use USB memory devices (Page 123)".
- Restart: reboots the device.

  When the "Restart" menu command is hidden, select "Permit restart", see section "The "Passwords" submenu (Page 101)".
- Configuration: central configuration settings of the device.

RDP: 1 Connection list, shows the client-server connection that is currently displayed

If you touch the icon, a list of started client-server connections is displayed. Use the "Favorites" icon to start a client-server connection. The icons have the following meaning:

- Green check mark: Client-server connection is running.
- Red X: Client-server is interrupted, see section "Interrupting and restoring a connection (Page 80)".

Note

Maximum number of connections

A maximum of 5 client-server connections can be started at the same time.

When an attempt is made to start a sixth connection, an error message appears and a selection of started connections is displayed from which a connection can be closed.

You close a connection using the "X" on the right.

Go to the preceding started client-server connection

Go to the next started client-server connection

Favorites

List of client-server connections selected for the taskbar. If you select a client-server connection from the list, the corresponding connection will be established.

On-screen keyboard

Displays the on-screen keyboard. Use the on-screen keyboard to enter alphanumeric values, special characters and function key commands. The on-screen keyboard is automatically displayed if you edit a field. If you touch the icon again, the on-screen keyboard is hidden.

Showing a minimized taskbar

If the "Minimized" option is selected in the "Taskbar" area in desktop settings "Configuration > Desktop", the taskbar is only displayed again when you touch the button with the "Maximize" arrow on the edge of the screen.

Taskbar is hidden

If the "Always hidden" option is selected in the "Taskbar" area in the desktop settings, the taskbar will always be hidden and cannot be displayed.

Note

If the administrator saves changes of configuration settings, the display and position of the taskbar may be changed.

5.7.2.2 Starting a connection

Overview

You can connect to a server From the Industrial Thin Client according to the configured connection settings. The following connection types are supported:

- RDP
- Sm@rtServer/VNC
- WinCC OA
- Web: In addition to the web connection settings, web settings are required for the browser that displays the web connection.

  Note

  Limited number of browser instances

  A maximum of 5 browser instances can be started at the same time. When you open a sixth browser instance, an error message appears.

  You can open the Web browser separately to establish a connection of any kind to the Internet regardless of the maximum number of browser instances and client-server connections.

Note

Limited number of client-server connections

A maximum of 5 client-server connections can be started at the same time. If a 6th connection is activated, an error message appears

Procedure for client-server connection

Proceed as follows to establish a client-server connection:

1. Touch the "Favorites" icon in the taskbar.
2. Select a client-server connection.

The configured connection to the server or system network will be started.

Procedure for web browser

Proceed as follows to establish a connection to the Internet or an intranet:

1. Select the "Web browser" menu command in the taskbar of the Start menu. The web browser will open.

   The IP address of the device is stored as the home page. The home page displays important device data and network settings.
2. Specify a valid Internet address in the address line of the web browser.

5.7.2.3 Changing from one connection to another

You can easily change between the started client-server connections.

- RDP: 1 Connection list: Select a different client-server connection using the icon.
- Go to the preceding started client-server connection.
- Go to the next started client-server connection.

5.7.2.4 Terminating a connection

Introduction

You can terminate a client-server connection as follows:

- Via the menu command "Close".
- For additional options, refer to the section "Special features".

Procedure

Proceed as follows to terminate an active client-server connection:

1. Touch the "Connection list" icon in the taskbar. A list of all started client-server connections opens.
2. Choose the "Close" menu command next to the connection.

3. If required, enter the connection password, see section "The "Passwords" submenu (Page 101)".

Note

Misuse

RDP can be set on the server so that the user stored in the connection settings remains logged in even after an RDP connection has been terminated.

Make sure that only authorized persons have access to the device or log off (see Special features).

Administrator password

You can also enter the administrator password instead of the connection password.

Special features

RDP

Note

Terminate the RDP connection alternatively by using "Start" > "Disconnect". The "RDP session has been terminated by peer!" dialog box will be displayed on the device; acknowledge it with "OK". The connection password is not requested.

You log off from the RDP server with "Start" > "Logoff".

5.7.3 Operating the on-screen keyboard

On-screen keyboard

If you have not connected an external keyboard to the device, use the on-screen keyboard for inputs, e.g., in the configuration settings.

The on-screen keyboard is opened automatically provided:

- You activate an entry field in the configuration dialogs of the Thin Client.
- You use the Sm@rtServer connection type and activate an entry field on the server.
- You use the Web Server connection type and activate an entry field on the server, such as a runtime input/output field on a Unified device.

Note

On-screen keyboard

An English and German on-screen keyboard is available on the device. Depending on the delivery version of the device, additional languages may be available, for example, Hungarian or Spanish. The keyboard language can be changed in the menu "Configuration > System". The following applies to the user interface:

- With German keyboard layout: German user interface
- With English keyboard layout: English user interface
- For all other keyboard layouts: English user interface

Operating the on-screen keyboard

You operate the on-screen keyboard by directly touching the keys of the keyboard on the touch screen. The functions of the keys on the on-screen keyboard are basically the same as those on an external keyboard.

You position the screen keyboard as follows:

- In the desktop settings, you can position the on-screen keyboard at the top ① or bottom ④ edge of the screen.
- Depending on the position at the screen edge, the buttons ② and ③ on the right change:
- The button ② closes the on-screen keyboard.
- The button ③ moves the on-screen keyboard to the other edge of the screen (top or bottom).

Windows key

The "Win" key corresponds to the Windows key on a mechanical keyboard. You use this key to open the Windows Start menu.

Number pad

The on-screen keyboard has a separate number pad that you open with the "NUM" key. If you have connected an external keyboard, you cannot make any entries via the number pad of the external keyboard.

Latch function

If you keep the buttons <Ctrl>, <Alt>, <AltGr> and <WIN> pressed for some time, they are permanently enabled as though they are being pressed even after you have released them.

5.7.4 Use USB memory devices

Introduction

Use the USB port on the back of the device to access connected USB storage devices.

RDP

In the case of an RDP connection you have read and write access to one or several USB storage devices.

With active RDP connection the USB storage devices are exported to the RDP server. A folder with the name "media on <Client hostname>" is created in Windows Explorer, in which a separate subfolder is displayed for each USB storage device. If you change the host name in the configuration settings of the device, the name of the folder is adapted automatically on the RDP server.

Requirement

- The "Connect USB device as drive" option is selected in the connection settings in "Settings > Configuration > Connections".

Procedure

1. Insert the USB memory device in the USB port on the device.
2. Choose "Settings > USB devices" in the taskbar. A media explorer opens.
3. Touch the "View details" icon in the menu bar.
4. Open the desired folder in the tree menu on the left. Its content is displayed in the window on the right.
5. You can cut, copy, paste, and delete files via the menu bar.
6. You use the navigation buttons to navigate back, up, and to the root directory of the USB drive.

Removing a USB memory device

To remove the USB memory device, proceed as follows:

1. Make sure the device is no longer being accessed.
2. Close the accessing application.
3. Close the media explorer via the connection list in the taskbar.
4. Wait for 5 to 10 seconds.
5. Remove the USB memory device from the USB port of the device.

See also

Connecting a USB device (Page 65)

5.7.5 Using a USB reader

The following USB readers are supported for connection type "RDP".

Note

Connect the USB readers to the Industrial Thin Client before establishing the RDP connection. Otherwise, the RDP connection must be closed and re-established.

- SIMATIC MV32x optical handheld readers
- SIMATIC RF10xxR readers, which can be used, for example, in conjunction with the PM-LOGON or SIMATIC Logon software.

With Windows systems, proceed as follows to use the RFID readers:

1. Log on to the device as an administrator.
2. Open "gpedit.msc" via the Windows icon, the Windows search or via the command prompt.
3. Select "Computer configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection"
4. Double-click the "Do not allow supported Plug and Play device redirection" setting.
5. Select "Disabled".
6. Save the setting with "OK".

See also

Connecting a USB device (Page 65)

SINUMERIK operating mode

6

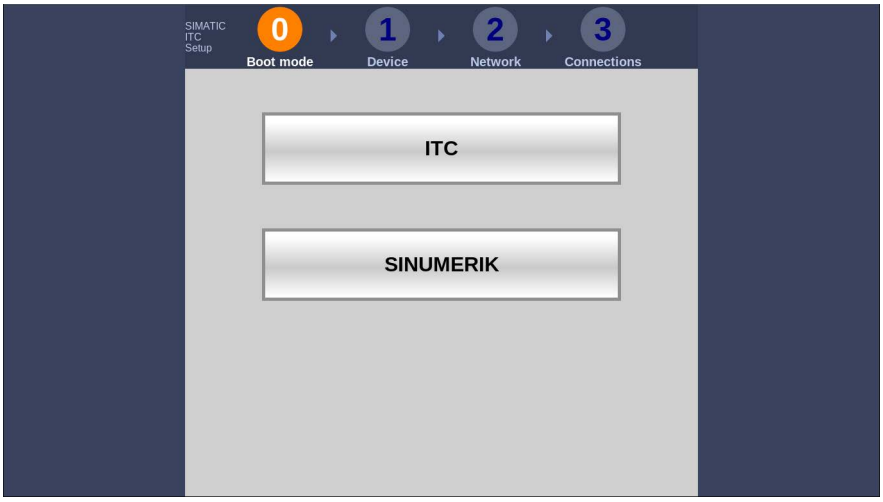
6.1 SINUMERIK commissioning

Requirement

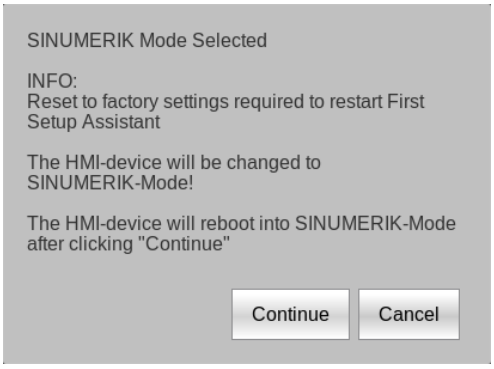
The devices is connected according to the description in these operating instructions to the 24V DC power supply and equipotential bonding is connected.

Procedure

1. Switch on power to the Industrial Thin Client.
   The first commissioning dialog to select the operating mode is displayed.



2. Select the operating mode "SINUMERIK".
   The following dialog appears:



3. Confirm the dialog with the "Continue" button.
   The device restarts.

After successful first commissioning, the SINUMERIK server screen is displayed.

Result

The first commissioning has been completed and the operating mode SINUMERIK has been defined. In the future, the device starts in SINUMERIK operating mode and the first commissioning dialogs are no longer displayed.

The further description of the SINUMERIK operating mode can be found in the following section.

To recommission, you must reset the device to factory settings or update the firmware.

Reset to factory settings in SINUMERIK operating mode

1. Switch off power to the device.
2. Press and hold the "Factory settings" button on the device and switch on the power supply of the device again. The device restarts.

   Use a sturdy blunt tool made of non-conductive material with a diameter of approximately 5 mm. The "Factory settings" button is next to the interface X1 P1 PROFINET (LAN).
3. Press and hold the "Factory settings" button until the boot procedure has finished and the first commissioning dialog is displayed.
4. Select the "SINUMERIK" operating mode in the first commissioning dialog.

Note

Re-commissioning in the SINUMERIK operating mode

When you reset the Industrial Thin Client using the "Factory settings" button, some SINUMERIK settings, such as the rotation of the display, are retained.

Updating firmware in SINUMERIK operating mode

1. Switch off power to the device.
2. Press and hold the "Factory settings" button on the device and switch on the power supply of the device again. The device restarts.

   Use a sturdy blunt tool made of non-conductive material with a diameter of approximately 5 mm. The "Factory settings" button is next to the interface X1 P1 PROFINET (LAN).
3. Press and hold the "Factory settings" button until the boot procedure has finished and the first commissioning dialog is displayed.
4. Select ITC operating mode and follow the instructions of the Setup wizard.
5. Connect a USB drive using an update file ".upd" with the device USB interface. The firmware version of the update file must be more recent than the firmware version on the device.
6. Choose "Settings > System" in the taskbar.
7. In the "Device configuration" area, use the "Update" button to select the update file "*.upd".

   The device restarts and the first commissioning dialog is displayed.
8. Select the "SINUMERIK" operating mode in the first commissioning dialog.

6.2 Networking

6.2.1 System settings

6.2.1.1 Thin Client Unit (TCU)

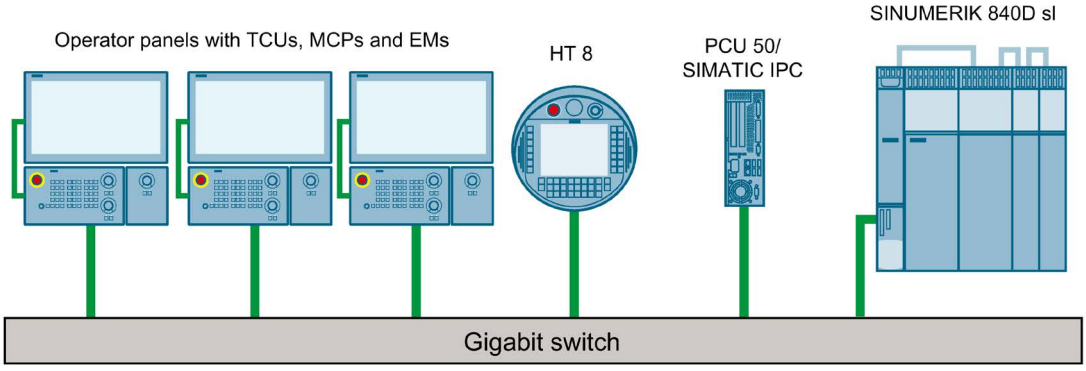
TCU overview

The Thin Client Unit (TCU) for the distributed configuration permits spatial separation of the SINUMERIK operator panel front (OP/TP) and the SINUMERIK PCU/SIMATIC IPC or NCU. With SINUMERIK solution line, the TCU is used to visualize the user interface of the PCU 50, SIMATIC IPC for SINUMERIK with PCU basic software or NCU.

One TCU can be connected to multiple PCUs/IPCs/NCUs. All TCUs and PCUs/IPCs/NCUs that are connected to one other via a Gigabit switch form the "system network". The user interface of a PCU/IPC/NCU is copied to several OPs each with one TCU. This means that all TCUs display the same screen. Operator actions can only be performed on one TCU at a time. This TCU then has user authorization. The PCU can also have its own OP connected directly to it.

The classic operator panel fronts can be used with an IPC 427E if a TCU is available.

The following diagram shows a **configuration example** for a distributed topology:



The mobile SINUMERIK HT 8 handheld terminal works on the thin client principle and combines the functions of an operator panel with a machine control panel.

The configuration and cabling of the whole system based on a permissible configuration is described in Section "Network configurations (Page 139)".

Supplementary conditions

The following supplementary conditions apply for the operation of a TCU:

- In the system network, the number of **active** thin clients is limited:
  - A maximum of 2 TCUs: NCU 710.3 PN
  - A maximum of 4 TCUs: NCU 720.3 PN or NCU 730.3 PN
  - A maximum of 4 TCUs: PCU/IPC

  Any number of TCUs can be operated in the system network.
- CompactFlash Cards cannot be used on the TCU.
- A 16 bit or 32 bit depth of color setting may be selected.
- If a PC keyboard is connected to the TCU, it is not possible to ensure that all special keys, e.g. multi-media keys, will be transferred to the software of the NCU/PCU/IPC.
- Machine control panels connected via a PROFIBUS network are not supported for switchover.
- Distributed memory media that are connected to the TCU via USB can be used.
- The TOP Panels must be networked on the basis of the Gigabit standard, e.g. Gigabit switch or Ethernet cable according to CAT 6 or higher.

6.2.1.2 Settings for SINUMERIK solution line

Fundamentals

The system network for SINUMERIK solution line is structured as a star topology with a central Ethernet switch, to which all Ethernet-based components of the system are connected.

For an NCU, the connection is via the X120 Ethernet socket, for an IPC/PCU, it is via the "Ethernet 2" or "X2" or "X2 P1" connection. There is no default for all other components with two Ethernet connections. These components have an internal 2-port switch and may be used to connect an additional operator component. Thus, in this case, there can be deviations from the strict star topology.

System network

In the system network, the IP address 192.168.214.xxx with subnet mask 255.255.255.0 is pre-selected. Here there is precisely one DHCP server with DNS that can run on one NCU or one PCU/IPC. The server ensures assignment of IP addresses to the Ethernet components in the system network (DHCP clients) from a specified address band.

The following rules apply for assignment of IP addresses in the system network:

- For all NCUs and/or PCUs/IPCs, the commissioning engineer assigns fixed IP addresses in the associated address bands, as well as appropriate computer names (host names). All other operator components are automatically assigned an IP address by the DHCP server. Its name is generated automatically (for MCP, MPP, HT 8), or is entered at commissioning (TCU).

- If there are multiple NCUs, IPCs and/or PCUs in the system network, depending on the boot sequence, the system automatically specifies the DHCP server and automatically ensures synchronization of all necessary data, so that the next time the system boots any other NCU, IPC, or PCU could take on the role of DHCP server. However it is better to specify a DHCP master. This is an NCU, IPC, or PCU in the system network that is available on each system boot and which regularly takes over the task of the DHCP server and DNS server.

  Synchronization of data takes place in any event so that any other NCU, IPC, or PCU can take over this task, unless you deactivate this option in the DHCP configuration. All non-master NCUs/IPCs/PCUs wait while the system boots for a preset time for the master to become available.

Note

In a system network or on a boot server, i.e. on the NCU, IPC, or PCU that accommodates the active DHCP server, a maximum of 30 operator stations may be operated simultaneously with the TCU.

A maximum of 10 operator stations with a TCU may connect up simultaneously with the same HMI application when powering up.

Connection to a company network

Each NCU can be connected via X130, and each PCU/IPC can be connected via "Ethernet 1" to a company network. The company network is used to exchange operating software with servers or to execute part-programs directly from servers in the company network. Company network and system network should always be logically and also physically separated.

Service interface X127

The service interface X127 of the NCU is used for direct connection of a PG/PC for service purposes. Here, access with STEP 7 to the PLC, and with NCU 7x0.3 PN also to PROFINET is possible.

With direct connection (peer-to-peer) of a PG/PC to X127 it is absolutely necessary that the PG is operated as a DHCP client.

6.2.1.3 System boot with system network

System behavior at boot

The system boot behavior is based on the following principle:

- For the configuration of an NCU 7x0 with a PCU/IPC, the default for a network configuration is as follows: The NCU keeps the default IP address 192.168.214.1 on X120, the PCU/IPC keeps the default IP address 192.168.214.241 on Eth2.

- For a configuration of more than one NCU 7x0 without PCU/IPC, with one or morel PCUs/IPCs, a distinction must be made between two cases:
  - All address conflicts and DHCP conflicts are resolved automatically when booting and the system is ready for operation. In this configuration there is **no** guarantee that all NCUs and PCUs/IPCs will always receive the same IP address at each system boot.
  - If the user requires all NCUs, and possibly also the PCU/IPC, to have a defined constant IP address at each boot, for example, because the IP address is stated explicitly in the PLC program, the user must configure a fixed IP address in the adapter settings in the Windows Control Panel for each affected NCU 7x0/PCU/IPC.
- You can specify a DHCP master in the basesys.ini file.
- Assigning names:
  - Assign meaningful names for all NCUs in the basesys.ini file otherwise the names will be generated automatically.
  - A PCU/IPC always has a computer name, which you can change if required.
- The IP addresses of the TCU, MCP/MPP, EKS, HT2, and HT8 are freely assigned within the specified address range on each boot. MCP/MPP, HT2, and HT8 are identified in the PLC via their DIP switch settings.

Using DNS name service

Availability of the DNS (Domain Name System) name service offers the following advantages for system network administration:

- The name service enables easier configuration with names instead of IP addresses for management of operating units: All components in the system network can be addressed via a symbolic computer name. This name can to some extent be freely assigned, to some extent it is derived automatically from a DIP switch setting (MCP, MPP, EKS, HT 8, HT 2).
- A computer node in the system network (NCU, PCU/IPC, TCU, MCP, HT 8, etc.) can be addressed solely through assignment of the IP address, either via a freely selectable name or via an internally generated name in the system network, and thus becomes independent from its network address in the system network. Thus a change in the network address does not necessarily necessitate a series of additional setting changes.
- In addition, the name service is used by the system for address resolution for MCP/MPP, direct keys, and EKS when changing the user authorization.

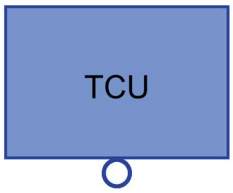
6.2.1.4 Factory default settings

Meaning of the symbols:

- ○ Eth 1 as a DHCP client
- ● Eth 2 as a DHCP server
- ■ Eth 2 with a fixed IP address

Preconfiguration of the TCU

The TCU is configured as a DHCP client and primarily accepts IP addresses from SINUMERIK components, from the DHCP server of such components that are inherent to SINUMERIK, for example, an NCU at X120 or a PCU/IPC on the system network or from a standard DHCP server. The behavior of the TCU cannot be changed here.



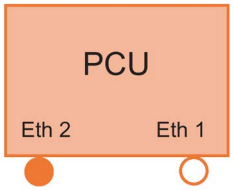
A TCU is a SINUMERIK DHCP client.

The TCU has a single Ethernet connection.

A TCU executes a boot via the network. The boot server is the computer node from which the TCU also obtains its IP address.

Pre-configuration of the PCU

A PCU has two Ethernet interfaces with default settings for use with SINUMERIK solution line:

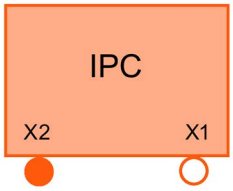


Eth 1 is pre-selected as a default DHCP client for connection to a company network.

Eth 2 is pre-selected as a SINUMERIK DHCP server for connection to a system network. On Eth 2 the fixed IP address 192.168.214.241 is pre-selected.

Preconfiguration of the IPC

An IPC has two Ethernet interfaces with default settings for use with SINUMERIK solution line:



X1 is preset as the standard DHCP client for connection to a company network.

X2 is preset as a SINUMERIK DHCP server for connection to a system network. The fixed IP address 192.168.214.241 is preset on X2.

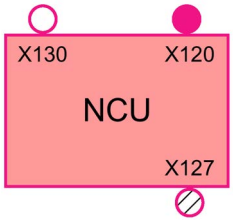
Preconfiguration of the NCU

On the X120, the NCU is preconfigured for the SINUMERIK DHCP protocol. The NCU is pre-selected here as a SINUMERIK DHCP server. On X120, the NCU occupies the fixed IP address 192.168.214.1 with the subnet mask 255.255.255.0 in its capacity as a DHCP server. The DHCP server of the NCU assigns IP addresses from the range 192.168.214.10 – 192.168.214.239 to the DHCP clients.

It is also possible to make the NCU a DHCP client. The configured IP address in basesys.ini is a "requested" IP address, which is rejected in the case of an address conflict and replaced by a dynamic IP from the address range.

In large system networks, it makes sense to set an NCU/PCU/IPC as the DHCP master. If an additional 2-3 hosts are used (NCU/PCU/IPC), the user sets the DHCP priority to "ON_HIGH". For the other hosts, the user sets DHCP priority to "ON_CLIENT_SYNC" or "ON_CLIENT_NO_SYNC".

Restricting the available address band that is managed by the DHCP server of the NCU frees up IP addresses 192.168.214.2 to 192.168.214.9 as well as addresses 192.168.214.241 to 192.168.214.254 for network nodes with fixed IP addresses.



The NCU has three Ethernet connections:

- X120 to connect to the system network with an active DHCP server (Eth 0)
- X130 to connect to the company network as the standard DHCP client (Eth 1)
- X127 as a service connection with an active DHCP server (Ibn 0)

On X130, the NCU is set as a default DHCP client for the address reference from a company network. The IP address received here is specified by the DHCP server from the company network.

On X127, an NCU is a standard DHCP server in contrast to the SINUMERIK DHCP server. On X127, the NCU has the fixed IP address 192.168.215.1 with the subnet mask 255.255.255.224 as Service input. The IP addresses 192.168.215.2 – 192.168.215.23 are dynamically assigned to the DHCP clients. The range 192.168.215.24 - 192.168.215.30 is reserved, and can be used by stations on the network with a fixed IP address, e.g. by a modem.

IP address ranges reserved for NCU and PCU/IPC

The following defaults apply on delivery:

- Connection to the system network with subnet mask 255.255.255.0:

IP address	Network station	Remark
192.168.214.1	NCU on X120	Default
192.168.214.2 – 9	For additional NCUs with a fixed IP address on the system network	Not assigned
192.168.214.10 – 239	For additional TCUs, later for additional PCUs, IPCs, NCUs, MCPs, MPPs	DHCP clients
192.168.214.240	Reserved for EKS (Electronic Key System)	Default
192.168.214.241	Fixed IP address of PCU/IPC on Eth 2	Default
192.168.214.242 – 249	For additional PCUs/IPCs with a fixed IP address	Not assigned
192.168.214.250 – 254	For PGs with a fixed IP address (Service connection)	Not assigned

- Service connection with subnet mask 255.255.255.224:

IP address	Network station	Remark
192.168.215.1	NCU on X127	Default
192.168.215.2 – 23	For service purposes with PG, PC	DHCP clients
192.168.215.24 – 30	Fixed IP address, e.g. for a modem	Not assigned

6.2.2 Commissioning TCU

6.2.2.1 Key assignment

Key assignment

Functions of the keys and softkeys in the "Operator panel service system":

Softkey	Key on OP	External keyboard	Description
↓	HSK1	<F1>	Moves the cursor down a row
↑	HSK2	<F2>	Moves the cursor up a row
Page↓	HSK3	<F3>	Moves the cursor down a page
Page↑	HSK4	<F4>	Moves the cursor up a page
Char↓	HSK5	<F5>	Inserts text or digits
Char↑	HSK6	<F6>	Inserts text or digits
Cancel	VSK7	←	Cancel / Return
Ok	VSK8	→	OK / Confirm
---	NEXT WINDOW	Pos1	Moves the cursor to the top row
---	END	End	Moves the cursor to the bottom row

Exceptions to the above are mainly the result of input fields. Where these are present, the left/right cursor keys move the input cursor rather than performing an OK/cancel function. The Return key takes you to the next field (like the "down" key) rather than closing the entire dialog with OK. There are also Backspace (deletes character to the left) and Delete (deletes character to the right) keys for editing text and numbers. The F5, F6, Backspace, Delete, and Select keys (between the cursor keys) can be used to switch between Yes/No fields.

Note

Special function for Touch Panels without additional keys

Letters and numbers in input fields can be edited with HSK5/HSK6, which switch one character forward or backward. With a touch screen, you can activate all the softkeys and even select rows in a menu simply by touching them.

For operator panel fronts without keys, a virtual keyboard automatically appears.

6.2.2.2 Settings in the "TCU.ini" file

Directories

The tcu.ini file is created in the following directories:

NCU:

```
../siemens/system/etc/tcu.ini
../user/system/etc/tcu.ini
../oem/system/etc/tcu.ini
```

PCU/IPC (Windows 7 and Windows 10):

```
C:\ProgramData\Siemens\MotionControl\siemens\System\etc\tcu.ini
C:\ProgramData\Siemens\MotionControl\user\System\etc\tcu.ini
C:\ProgramData\Siemens\MotionControl\oem\System\etc\tcu.ini
```

Note

The following entries are evaluated by SINUMERIK Operate:

- VNCServer/VetoMode
- VNCServer/AlarmBoxTimeOut
- VNCServer/FocusTimeout
- VNCServer/AdaptResolution
- VNCServer/MaxActiveTCUs
- VNCViewer/ExternalViewerSecurityPolicy

Restrictions

Restrictions for such external operator control units are:

- Neither MCP and direct keys nor an EKS system can be assigned. This also means that these devices cannot be activated to be an operator control unit in the system.
- Direct keys cannot be triggered, i.e. the softkeys to the direct keys can be triggered in the operating software. However, the keys do not appear in the direct key image to the PLC.
- There is no config.ini configuration file, as for a TCU, i.e. a configuration for a TCU is not possible for such an operator control unit (power-up behavior, displacement, t:m:n); however, the displacement mechanism on the external operator control units is effective.
- An external operator control unit is never signaled as active operator station in the PLC.

Configuring the external operator control units in the tcu.ini file in section:

```
[externalTcu]
# EXTERNAL TCU IP-ADDRESSES
# List of accepted TCUs in IP-V4-format (index 1 to maximal 16)
ExternalTcuIP_1=
```

You can also set the desired screen resolution in the tcu.ini file:

```
[VNCServer]
Resolution = ...
```

6.2.2.3 Displacement mechanism for TCUs

To operate a machine with more operating stations then the maximum number, the displacement mechanism ensures that **only the permitted number of TCUs are active** in a shadowing group. The remaining TCUs are switched to passive mode, which means they no longer represent a load with regard to the resources. Thus the number of TCUs that can be connected to one HMI application is practically no longer limited. The limitation is the number of concurrently active TCUs.

Supplementary conditions

The following supplementary conditions apply when operating the TCU:

2 active TCU connected in parallel to NCU 710.3 PN

4 active TCU connected in parallel to NCU 720.3 PN, NCU 730.3 PN

4 active TCUs connected in parallel to PCU/IPC

Displacement rules

You configure the displacement mechanism in SINUMERIK Operate in the "Setup" operating area > menu forward key > "OPs" softkey for the respective operator panel.

The TCU can assume the following states:

- **The TCU is active and has user authorization:** This can be identified as the TCU shows the screen of the operating software and the screen is bright.
- **The TCU is active,** is in the monitoring mode and has no user authorization: This can be identified as the TCU shows the screen of the operating software, however, it is darkened in comparison to the TCU with user authorization.
- **The TCU is passive:** The TCU shows the selection menu of the possible connections instead of a screen of the operating software, and the softkey for selection of the last active connection of the TCU is shown in color.

When powering up, the TCU always always attempts to establish the first connection. The TCUs from a shadowing group establish their specified connection one after the other as long as the maximum number of permissible active operator units is not exceeded.

If a TCU encounters the situation that this number is already reached in its power up, then it attempts to obtain a connection via the displacement mechanism. If it can displace a formerly active operator unit then it takes on the active status itself, otherwise it transitions to passive status immediately after booting.

6.2.2.4 Disable switchover between TCU via PLC

Overview

The TCU switchover disable offers the option of dynamically disabling switchover from one TCU to the next when the system is running via the PLC. For the duration of the disable, a user authorization request to change user authorizations between TCUs will be ignored by the system and rejected.

The rejected user authorization request causes a message to be output in the dialog line of the HMI, in the form of a feedback message for the requester. The message disappears after five seconds.

HMI ↔ PLC data interface

The "switchover disable" function is always active and does not have to be switched on explicitly. The function is controlled by a data bit in the PLC. The HMI transfers the active OP to the PLC, thus forming the basis of the control function in the PLC.

The control bits and control information for this function are stored in the m:n data interface of the PLC. In terms of m:n, this function can be operated separately for the currently overridden HMIs in both m:n online interfaces (DB19.DBW120 ff for HMI1 and DB19.DBW130 ff for HMI2). If a system is not running an m:n, only the first m:n online interface is used for this function.

Switchover disable is controlled by a TCU_SHIFT_LOCK bit, managed by the user, on each HMI in the PLC. The bit address for the first HMI is DB19.DBB126.6 and DB19.DBB136.6 for the second HMI.

The PLC m:n online interface is expanded so that byte DB19.DBB118 is also assigned to the first interface and byte DB19.DBB119 to the second. These bytes acquire the index of the active TCU/OP for the appropriate HMI. The byte is called TCU_INDEX. The appropriate HMI uses the TCU index configured for the active TCU to describe the TCU_INDEX byte.

The TCU_SHIFT_LOCK bit is monitored by the appropriate HMI. A value = 1 triggers the switchover disable. Switchover is enabled if the value returns to 0. The TCU_SHIFT_LOCK bit can be set, for example, to the PLC by the user pressing a key or it can be managed by the PLC user program according to its own logic. The TCU_SHIFT_LOCK bit is managed in the PLC exclusively by the user; the HMI only accesses this bit in read-only mode.

The HMI assigns the TCU_INDEX field with the configured index to the TCU or PCU/IPC with an OP that currently possesses user authorization in the shadow group. If no OP is active, a value of 0 is entered in TCU_INDEX.

If no TCU index is configured for the active TCU/OP, the value 255 = undefined is transferred as a TCU index. This means that the values 0 and 255 may not be configured as the TCU index.

Configuration

The TCU index is configured on the PCU/IPC in the same way as a machine control panel address (MCP address). The TCU index is set in the "OP Properties" dialog of the "System Network Center" program.

Operating principle

If the TCU_SHIFT_LOCK bit is set for switchover disable, a user authorization request is not carried out independently of the mode set on the HMI for allocation of user authorizations (veto mode), i.e. a change of user authorization is rejected.

This message appears on all OPs for approximately 5 seconds:

`"No switchover: Switchover disable set in current PLC."`

While this message is displayed, operations on the OP with the user authorization can still be carried out unaffected.

Note

Active switching of an OP to another PCU/IPC is possible

The switchover disable only relates to changing the user authorization on the OPs in a shadowing group on a PCU/IPC.

This means that active switching away from one OP to another PCU/IPC is not prevented.

Special features

The following special cases should be noted:

- Even if switchover disable is set, the TCU_INDEX field value may change in the PLC. This is the case under the following circumstances:
  - If the OP in possession of the user authorization is actively switched to another PCU/IPC. Depending on whether another TCU takes over the user authorization or whether no TCU is currently active, the index of the TCU or the PCU/IPC itself (if its directly connected OP becomes active) is entered, in exactly the same way as when there is a switchover of user authorization.

    This can also be the value 255, if no TCU index is available for the OP. 0 is entered if an OP is no longer available in the shadow group.
  - If an m:n switchover is in progress. The HMI program of the incoming PCU/IPC deactivates the HMI program which is active on it. Therefore, an OP from the shadow group of the new (incoming) PCU/IPC must receive the user authorization. The TCU index of this OP is entered in the TCU_INDEX field.
  - If a PCU/IPC is disconnected from an NCK/PLC in the context of m:n. No HMI program and, therefore, no OP with user authorization is then available on the exited NCK/PLC. This is signaled independently of a switchover disable by entering the value 0 into the TCU_INDEX field.
- If a TCU is actively switched over to another PCU/IPC, it can be deactivated there, i.e. it does not receive user authorization if a switchover disable is set for the destination PCU/IPC.
- With an m:n PCU/IPC switchover – the PCU/IPC is switched to another NCK and, therefore, to another PLC – the PCU/IPC accepts the switchover disable settings of that PLC.
- The m:n interlock options on the PLC side have priority over the TCU switchover disable, so that a set TCU switchover disable cannot prevent an m:n switchover. If necessary, the m:n interference options should be synchronized here with those for the TCU in the PLC. It may, for example, be practical to set or remove the m:n displacement disable simultaneously with the TCU switchover disable.

Obtaining user authorization

At a TCU, which has no user authorization, press any key. The operating software does not evaluate this key; this only serves to request user authorization.

The settings for the right to veto are stored in file tcu.ini and are only effective if the operating software is installed on the PCU/IPC. You can use the operating software on the OP or TCU in the same way as on an OP connected directly to the PCU/IPC.

6.2.2.5 Example: How to select the behavior of the TCUs during boot up

Example: Distributing boot support across two PCUs/IPCs

Make the following settings to distribute the boot support across two PCUs/IPCs:

- On PCU_1/IPC_1, select "Boot support runtime and configuration only (TFTP/FTP)"
- On PCU_2/IPC_2, select "Boot support IP address only (DHCP)"
- On PCU_3/IPC_3, select the configuration "No boot support"

TCU_1 192.168.214.10	**TCU_2** 192.168.214.11	**TCU_3** 192.168.214.12	**TCU_4** 192.168.214.13

VNC connections:
`192.168.214.241`
`192.168.214.242`
`192.168.214.243`
	VNC connections:
	`192.168.214.241`
	`192.168.214.243`
		VNC connections:
		`192.168.214.241`
		`192.168.214.243`
			VNC connections:
			`192.168.214.241`
			`192.168.214.242`

Switch to system network			
PCU_1/IPC_1 192.168.214.241	**PCU_2/IPC_2** 192.168.214.242	**PCU_3/IPC_3** 192.168.214.243	
Services: **X** DHCP ✔ TFTP ✔ FTP ✔ VNC	Services: ✔ DHCP **X** TFTP **X** FTP ✔ VNC	Services: **X** DHCP **X** TFTP **X** FTP ✔ VNC	
Company network			

In this case, PCU_2/IPC_2 serves as the DHCP server which provides the IP addresses for the connected TCUs. PCU_3/IPC_3 is not involved in booting the TCUs, it is however displayed by the TCUs using VNC.

6.2.3 Network configuration

6.2.3.1 Permissible network topologies

Ethernet connection

A SINUMERIK 840 D sl can only be operated as a network within which the individual components communicate with one another via Ethernet connections. This network must be set up.

The individual components are factory-set so that the most frequently occurring standard configurations can be operated without changing the settings related to the network.

Division into system network and company network

On the SINUMERIK solution line, the components are generally split into a company network on the one hand and a system network on the other.

The connection to the company network provides access to the network drives, for example. On the system network, process data communication and image transmission runs from the components with operator software to the display units of the respective TCU.

This separation is performed via the following specified use of the Ethernet interfaces on the components:

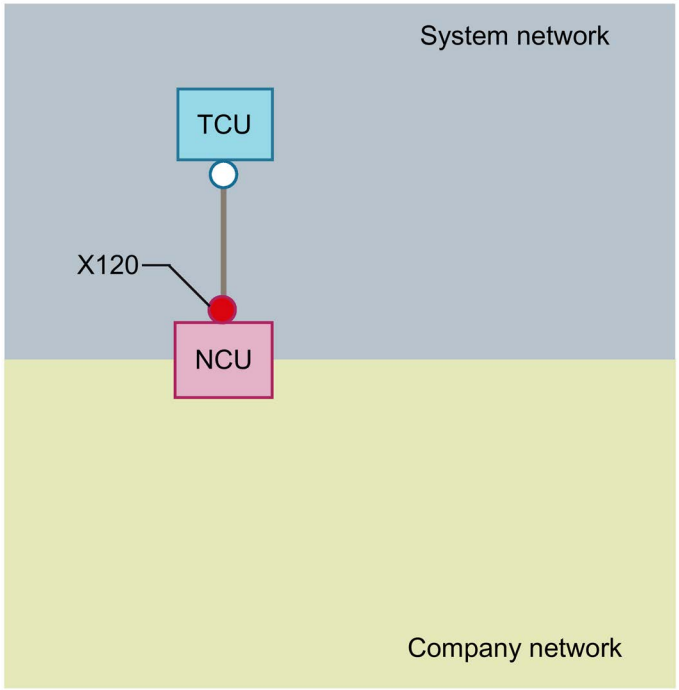
- A TCU is connected exclusively to the system network.
- An NCU is always connected to the system network via X120.
- Ethernet interface Eth 2/X2 of the PCU/IPC is preconfigured for connection to the system network; while Ethernet interface Eth 1/X1 is used for connection to the company network.
- An NCU is connected to the company network via X130.

Meaning of the connections:

○	Eth 1/X1 as DHCP client
●	Eth 2/X2 as DHCP server
■	Eth 2/X2 with fixed IP address
Green connection	Uncrossed Ethernet cable
Gray connection	Crossed Ethernet cable (crossover)

6.2.3.2 Networks without connection to the company network

Configuration 1: NCU and TCU



A direct Ethernet connection is used to connect a TCU to X120 of the NCU. NCU and TCU are suitably preconfigured with IP addresses.

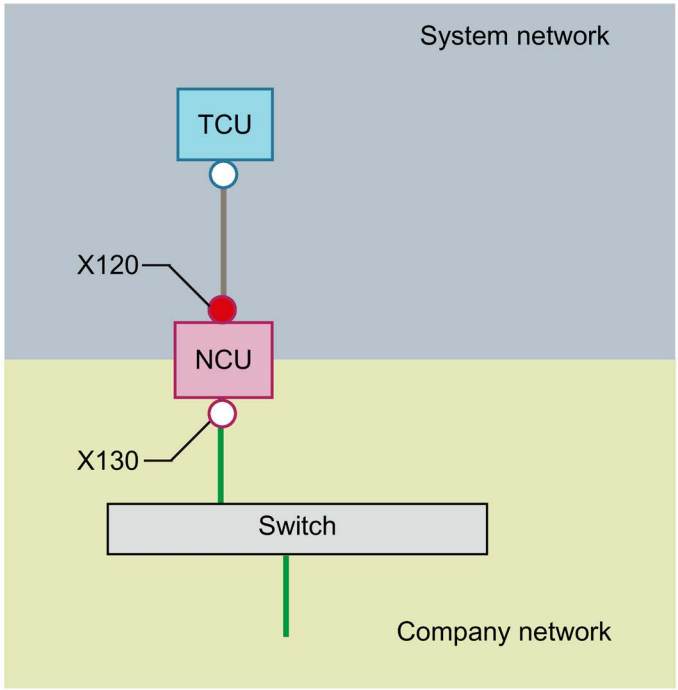
The IP addresses are not significant for further operation.

The TCU is connected to the NCU via a **crossed** Ethernet cable.

The direct connection of the NCU via X120 to the TCU automatically establishes a simple system network consisting of two computer nodes.

6.2.3.3 Networks with NCU connection to the company network

Configuration 2: NCU and TCU



The TCU is directly connected to the NCU via a **crossed** Ethernet cable. On X130, the NCU is connected to a switch to the company network with a straight cable.

As in configuration 1, there is a direct Ethernet connection between a TCU and X120 of the NCU. NCU and TCU are suitably preconfigured with IP addresses. The IP addresses used here are not significant for further operation.

IP configuration: DHCP server on the company network

On the X130, the NCU is set to the address reference via DHCP. If the company network has a DHCP server that provides the NCU with an IP address/configuration, the NCU is integrated in the company network.

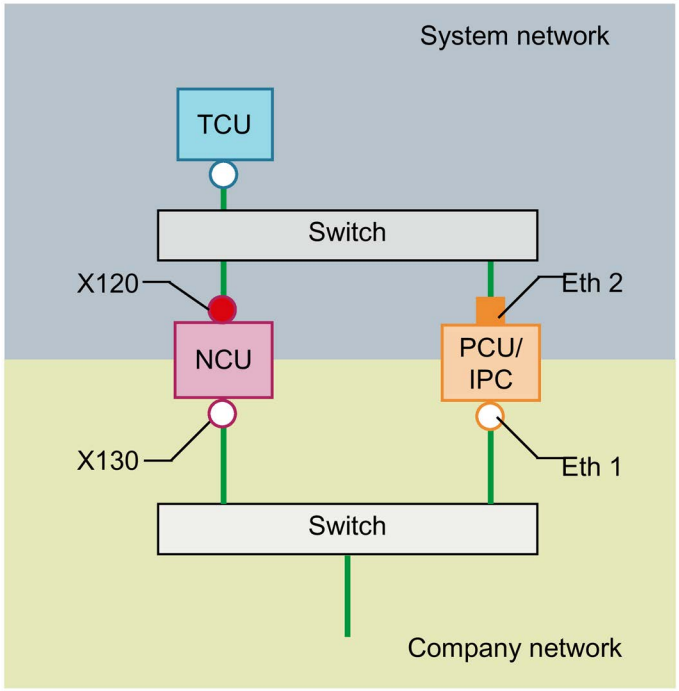
Depending on the infrastructure available or the level of network administration of the company network, the following network parameters must be set for the NCU on X130:

- Computer name on the company network
- The address of a DNS server
- The address of a gateway (default router)

The IP address of the NCU on this connection is also assigned via the network administration.

If the company network offers a low level of administration, in the worst case scenario the network has only one DHCP server that assigns the addresses from a predefined address range, the NCU receives an IP address that is initially unknown.

Configuration 3: PCU/IPC with TCU on NCU



In this configuration, a switch is also required for the system network. All components are connected using straight Ethernet cables.

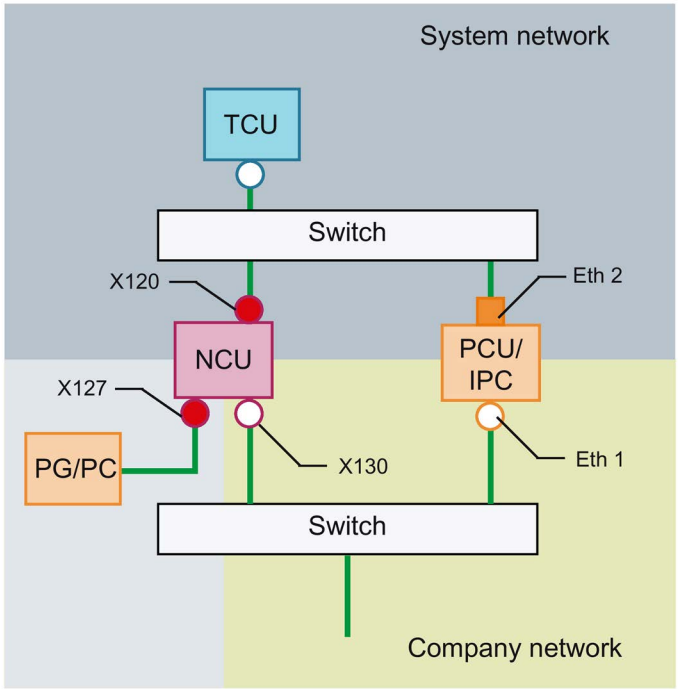
On X120, the NCU occupies the fixed IP address 192.168.214.1 in its capacity as a DHCP server (not used in this configuration). For this configuration on Eth 2, the PCU/IPC is assigned a static IP address in the range 192.168.214.241 – 192.168.214.249 with a subnet mask 255.255.255.0 . The DHCP server of the NCU supplies the TCU with an IP address and serves as a boot server for the TCU.

The observations made for configuration 2 apply here with regard to the connection to the company network. The connection to a switch on the company network is made via a **patch cable** for Ethernet.

To connect one TCU to both HMI systems you must create an additional connection to the NCU for the TCU.

Connecting the programming device (PG) to the NCU

Description



For service purposes a programming device is connected to the NCU at X127 as a standard DHCP client (automatically obtain an IP address). An NCU is a standard DHCP server on X127. On X127, the NCU occupies the fixed IP address 192.168.215.1 with the subnet mask 255.255.255.224.

At X127, IP addresses from 192.168.215.2 onwards are assigned via DHCP; e.g. to connect a programming device. This is the reason that a fixed IP address must not be set at the programming device.

6.2.3.4 Example: Configuring a VNC connection to a PC

Requirements

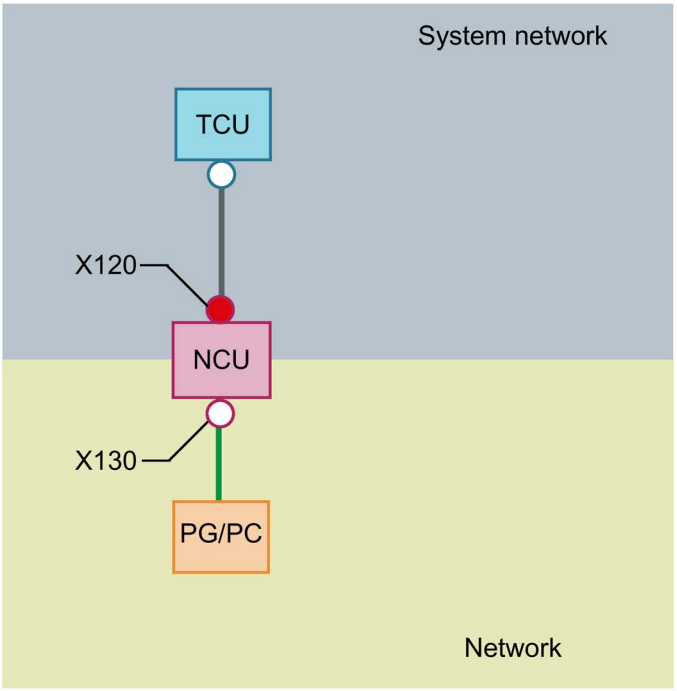
In order to use a TCU to get visual access to a computer from a SINUMERIK system via VNC, the following requirements apply:

- The VNC connections should be configured in the HMI.
- The boot server (active DHCP server) in the system network must be an NCU.
- This NCU must be integrated via X130 or X120, i.e. in the network that contains the computer to be monitored.
- The computer to be monitored must be configured in the config.ini configuration file of the TCU according to the general configuration for a TCU in a separate host section as a switchover target for this TCU.

  Where necessary, a password has to be specified in the configuration, if the VNC server requires one on the target system (see below).

- To ensure that the TCU recognizes the new switchover target, the TCU requires a restart and reboot.
- The screen resolution of the observed computer must be adjusted to the characteristics of the TCU. Otherwise the TCU scales the image it receives to match the display area available to the TCU, which impairs the quality of the display on the TCU.

Configuration



Configuration

The config.ini file is located in the following directory:

NCU:

`/user/common/tcu/<TCU name>/common/tcu`

PCU/IPC (Windows 7 and Windows 10):

`C:\ProgramData\Siemens\MotionControl\user\common\tcu\<TCU name>\common\tcu`

The config.ini file must be stored on the boot server (active DHCP).

Example:

```
[Station]
maxhostindex=2            /* Number of nodes that are defined under
                          [host 1] and [host 2].
mcpIndex=192
tcuIndex=1
eksIndex=0
[host_1]
Address=192.168.214.1     /* Address of the NCU to which the
                          connection is established during booting.
[host_2]
Address=157.163.230.202   /* Address of the PC
password=123456           /* Password of the VNC server on the PC
```

Switching over between the nodes

With the menu back key + MENU SELECT, the following actions are triggered:

- The TCU name is displayed in the header of the displayed window, e.g. TCU1.
- A selection list for connecting to the other nodes is displayed on the TCU.

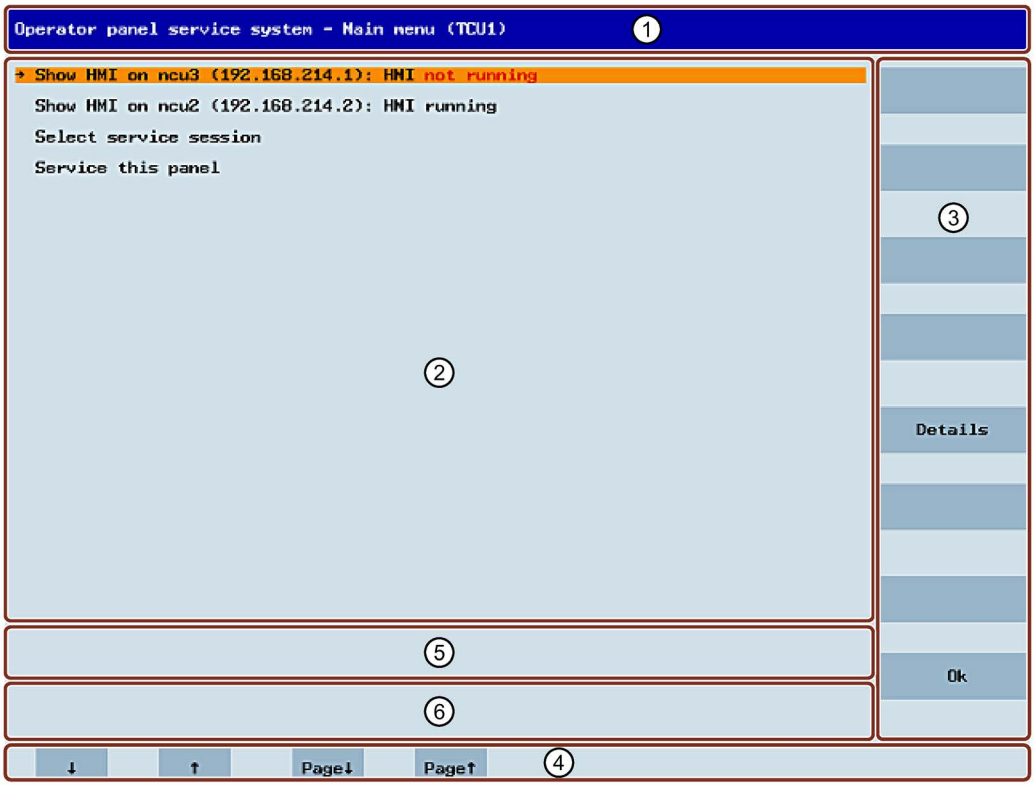
6.2.4 Service and diagnostics

6.2.4.1 Using the TCU's main menu

Displaying the TCU menu

- With touch screens: Simultaneously touch the left-hand and right-hand lower corner of the active display area with one finger at a time.
- With connected keyboard: Press the menu back key and the <MENU SELECT> key

"Main menu"



① "Main menu" title followed by the TCU name in brackets

② Central area with the list of servers and two further permanent items, "Select service session" and "Service this panel":

- "Select service session" triggers a server scan which detects all the VNC servers in the local system network. These are then displayed in a session menu which largely reflects the main menu.
- "Service this panel" opens the "Service menu for operator panel" submenu.

③ Eight vertical softkeys for use depending on the context

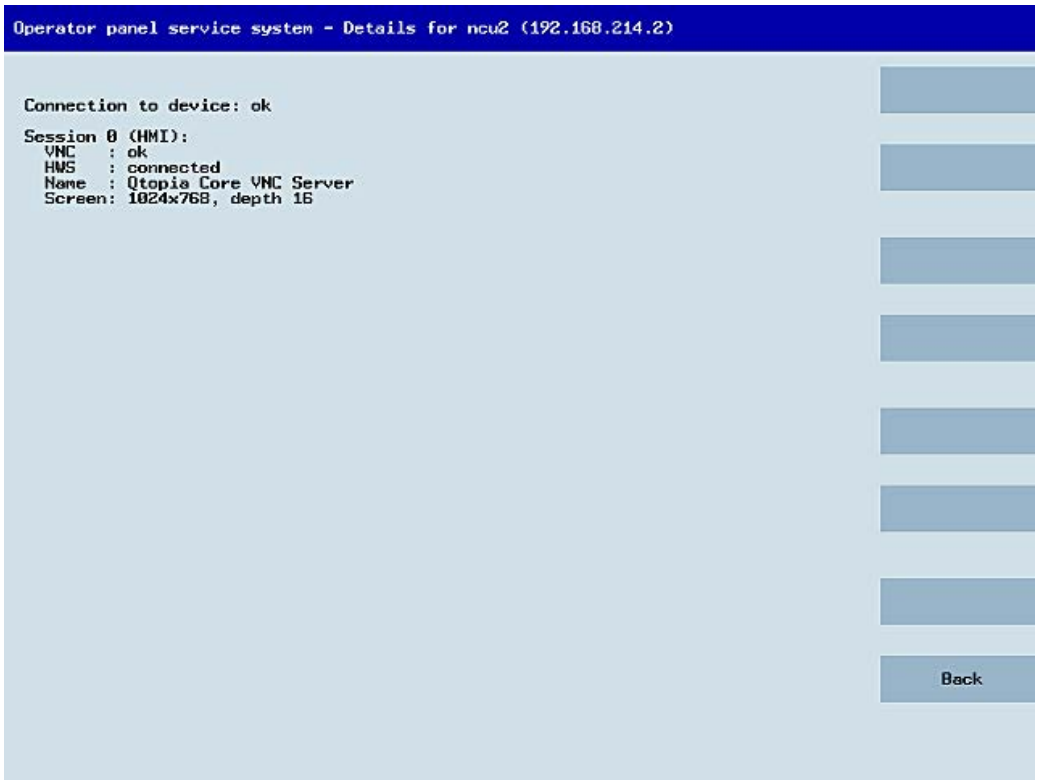
④ Four horizontal softkeys for navigating with the cursor

⑤ Message line whose content can be set via HWS commands from the servers

⑥ Error line in which error messages as well as transient status messages are output

"Details" softkey

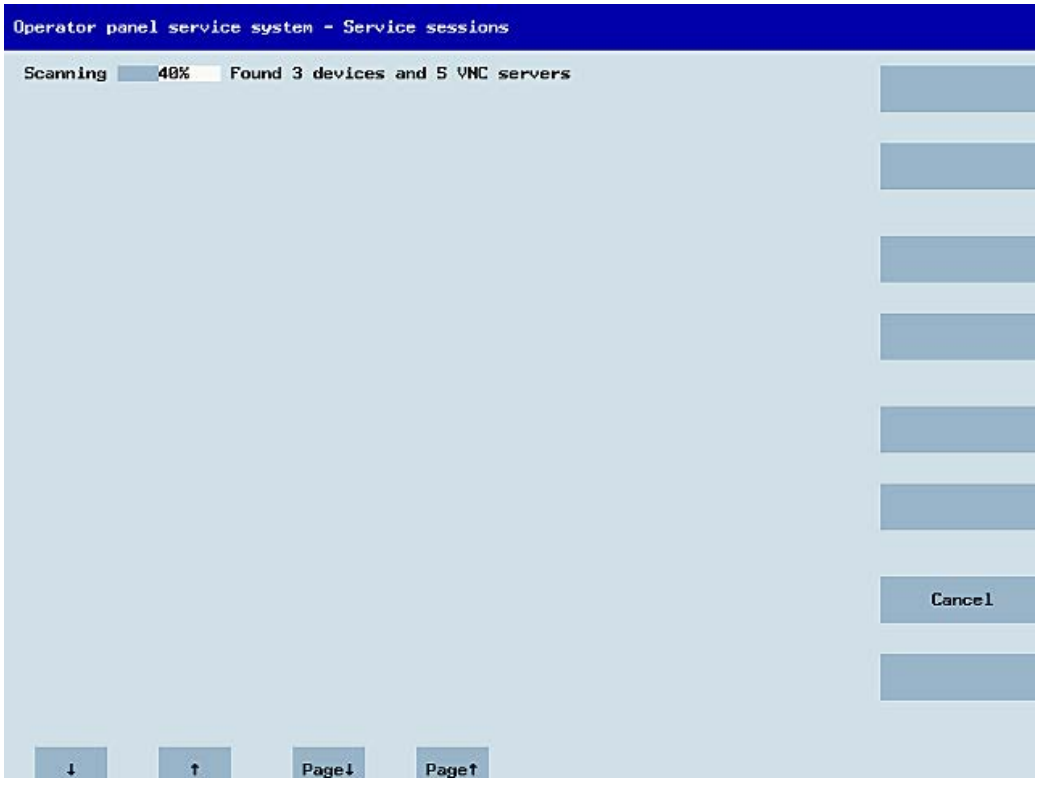
The following connection data for the selected device appears when the "Details" softkey is pressed:



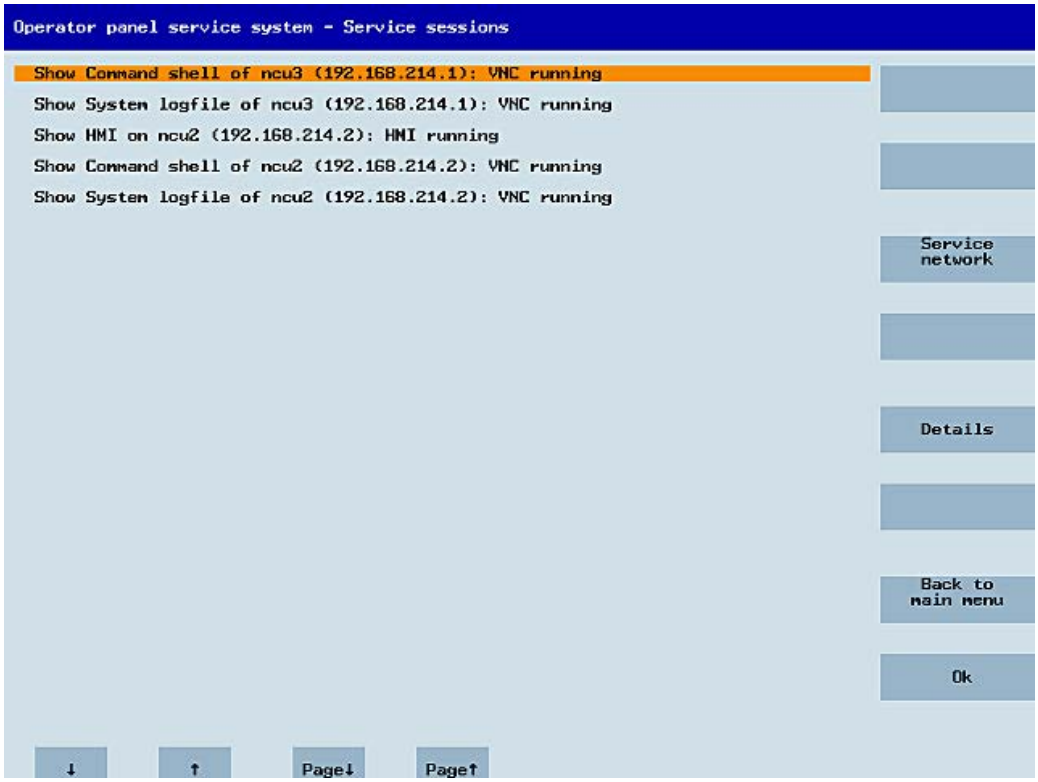
6.2.4.2 Operating the TCU menu "Service sessions"

"Service sessions" dialog

When "Select service session" is selected from the main menu, the resulting process begins by triggering a server scan:



After this, the following dialog appears:



Central area with the server list:

The individual server lines contain either "Show WHAT on NAME (IP)" or the IP address only where the name is unknown.

Session number	VNC server
Session 0	HMI
Session 4	Command shell
Session 5	System logfile
Session 6	System Network Center (SNC)
...	
Session **<N>**	Other servers

These details are followed by a status message regarding the accessibility of the VNC server.

- "Connection not ok" appears if it is already impossible to access the server from the IP side (if switched off, for example).
- "HMI running/ not running", if an HMI VNC server is accessible.

The VSK8, Return or right cursor keys can be used to launch a VNC viewer for the selected server.

Connection status:

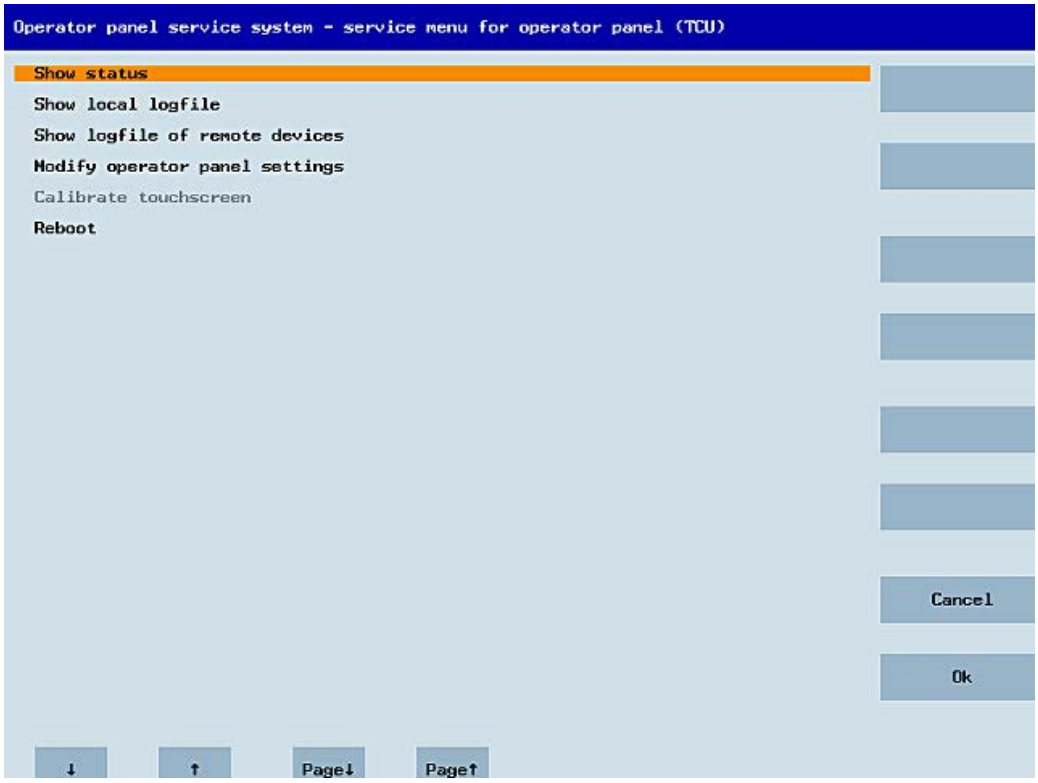
Further details on the connection status can be called with the "Details" softkey. In the next dialog, "not ok" or "not running" are accompanied by an additional error message with more precise details on the reason for the loss of function. With more favorable scenarios, the session name for the VNC server will also be specified along with its resolution.

The connection and HMI status are monitored on a regular basis in the background. This may mean that these specifications change spontaneously if a change is made on the relevant server, e.g. it may be switched off, the HMI may become available, etc.

6.2.4.3 Operating the TCU menu "Service menu"

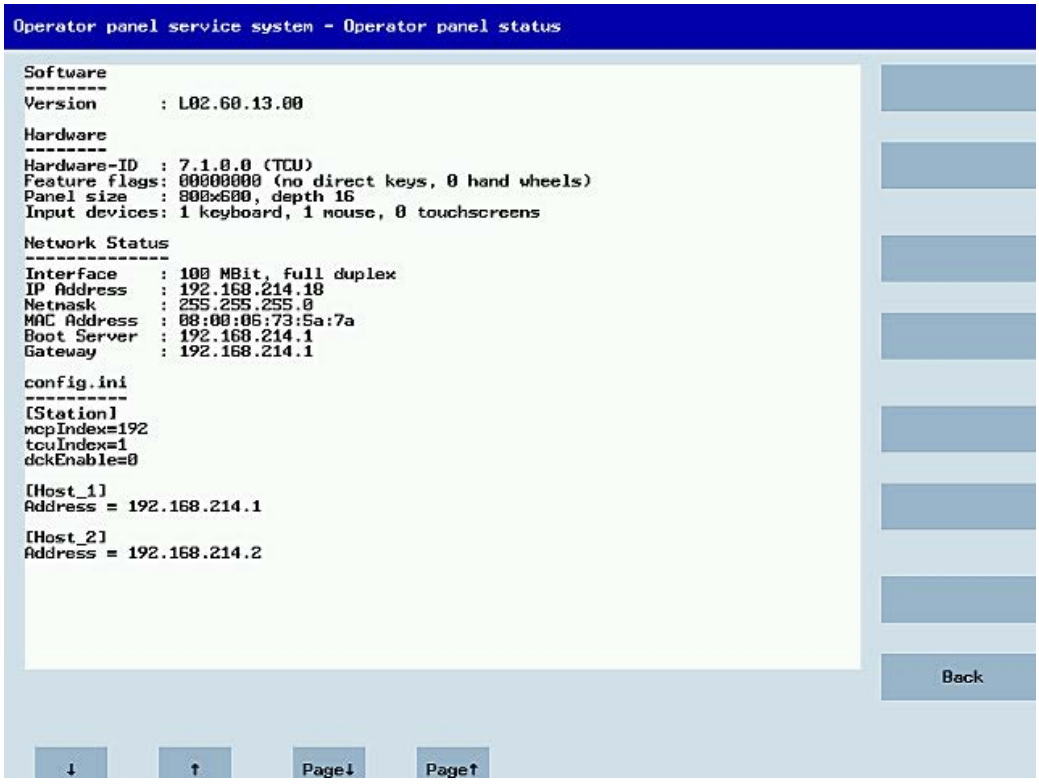
"Service menu for operator panel (TCU)" dialog

The following dialog appears when "Service this panel" is selected from the main menu:



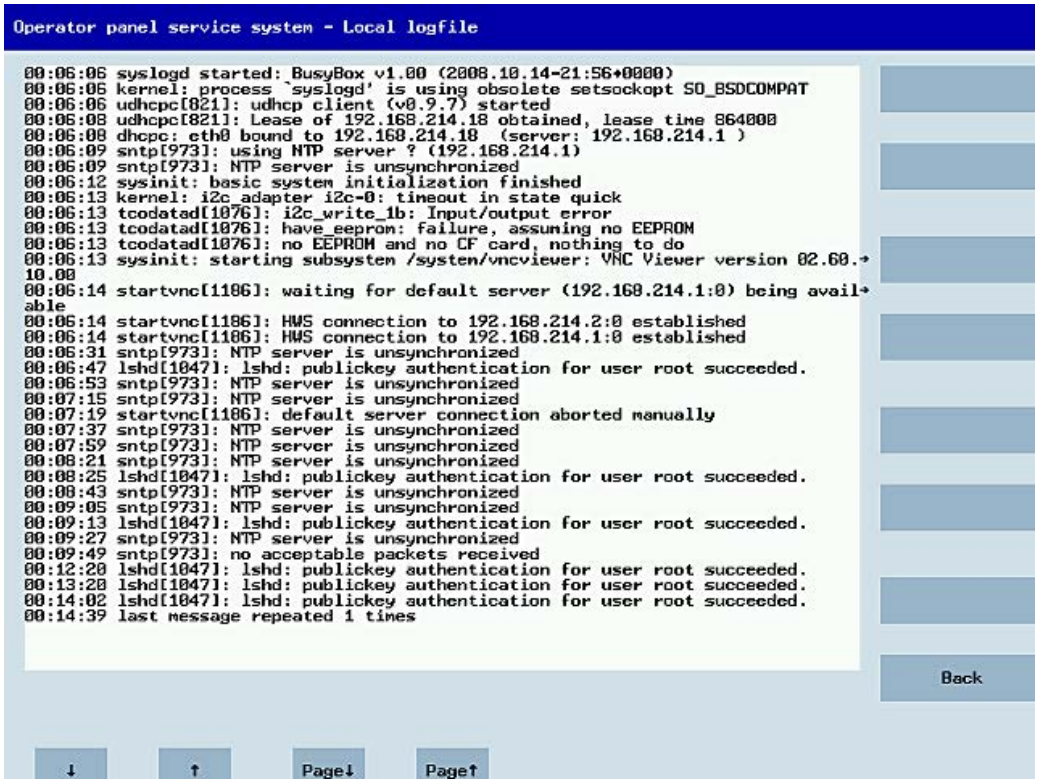
The following menu items are available here:

- "Show status" shows status information, for example: Software version, hardware information, TCU network data, and their configuration:



- "Show local logfile" shows a filtered version of the system log file in the `/var/log/messages` directory, which contains only the messages of the local TCUs.

  Syslog messages received via the network are not displayed.



- "Show logfile of remote devices" shows the log file of the other devices in the network:

  The syslog messages of devices in the system network which send syslog messages by broadcast, such as NCU 7x0, ...

- "Modify operator panel settings" opens another submenu, see next section.
- Calibrate touch screen" is only active if there is a touch screen. This menu item recalibrates an available touch screen.
- "Reboot" initiates a restart of the TCU.

Note

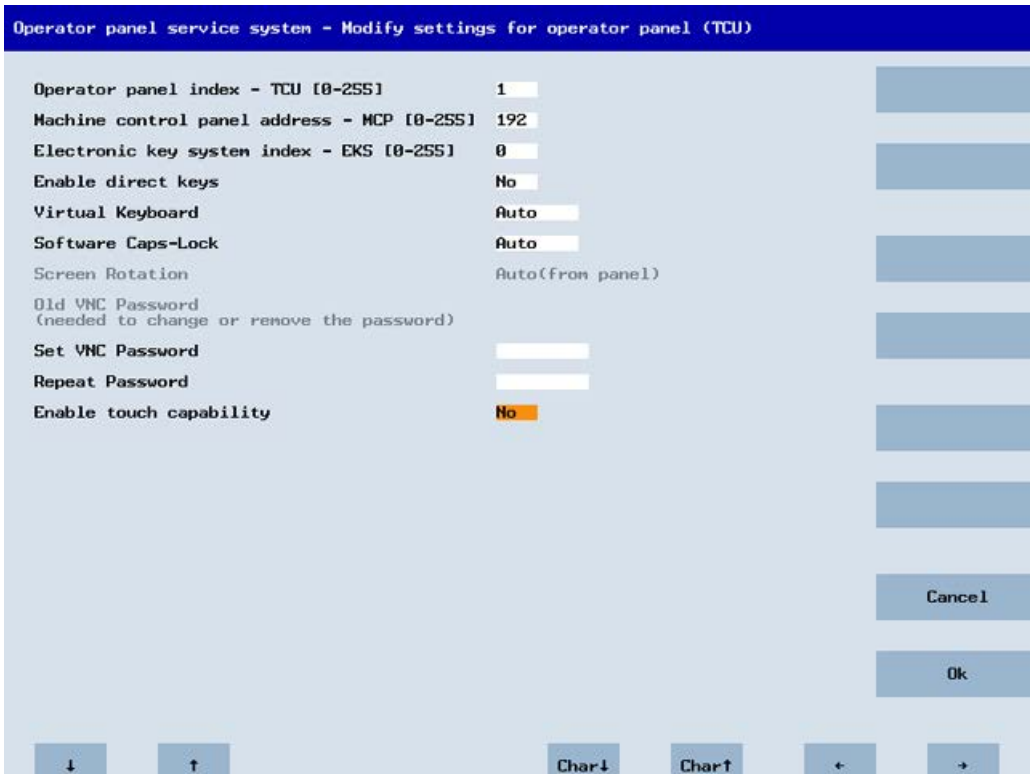
Long lines are broken and wrapped around.

Lines that are longer than the space available wrap round onto the next line so that you do not have to scroll horizontally. When this occurs, the line has a right-facing arrow at its right edge.

6.2.4.4 Operating the TCU menu "Modify settings"

"Modify settings for operator panel (TCU)" dialog

The following dialog appears when "Modify settings" is selected from the main menu:



The following TCU parameters are set here during the first commissioning:

- "HT 8 individual mode" (yes/no)

  This is only visible with HT 8, and is used to switch between Auto Mode and Individual Mode.

  You do not have to make settings for an HT 8 in Auto Mode because the name is generated automatically: ("DIP<n>") MCP address and TCU index are derived from the DIP setting ("DIP<n>").

- "Operator panel index - TCU" (0-255)

  Defines the TCU index; see column "TCU" on the user interface.

- "Machine control panel address - MCP" (0-255)

  Specifies the address of the associated MCP; see column "MCP" on the user interface.

- "Electronic key system index - EKS" (0-255)

  Specifies the index of the associated EKS; see column "EKS" on the user interface.

- "Enable direct keys" (yes/no)

  Specifies whether direct keys are registered with the PLC (yes) or are treated as ordinary keys (no); see column "DCK" on the user interface.

- "Virtual Keyboard" (Auto/On/Off)
  Specifies whether a virtual keyboard is shown on the screen for touch screens. Depending on the panel features (Auto), the HMI decides whether a touch screen or keyboard is available.
  This parameter can also be set manually (On/Off).
- "Software Caps-Lock" (Auto/On/Off)
  The HMI can manage the Caps-Lock status of a keyboard in the software itself, when, for example, the key is not available. This is normally (Auto) switched on via a display machine data item. This machine data item can be overwritten individually for the TCU with the setting (On/Off).
- "Emulation Type" (TCU/TCU20.2/TCU30.3, only for modular TCU30.3)
  Specifies which TCU type is to be emulated when the TCU30.3 is operated as replacement device for an older TCU or as new device on a software version older than 4.7 SP2.
- "Screen Rotation" (0°/90°/180°/-90°/Auto)
  Specifies in which angle the screen is to be rotated in the software. This is useful when the panel is to be rotated during installation.
  For the "Auto" setting, the rotation of the display is taken from the panel.
- "Old VNC Password"
  If a password has already been set, it must be entered here so that it can be changed. If no password has been set, this field is grayed-out. The existing password can also be deleted if, after entering the old password, no new password is to be entered at "Set VNC Password" and "Repeat Password".
- "Set VNC Password"
  Assign a password which is stored in the TCU and, if required, sent to the server when the VNC connection is established.
- "Repeat Password"
  Repeat the password entered at "Set VNC Password".
- "Enable touch capability" (yes/no)

  Specifies whether the screen can be operated by touch. If you deactivate this option, you will need a keyboard to reactivate it (see note).

The values are applied and stored with "OK". You can also make any subsequent adaptations or changes via the user interface in the "Setup" operating area > menu forward key > "OPs" softkey.

Note

After disabling the touch input, the virtual keyboard can only be reactivated using a connected keyboard:

- To call up the TCU menu, press the buttons <F9> and <F10> at the same time.
- You can operate the vertical softkey of the TCU menu with the buttons <Shift> and <Fx>.
- You can change the value of the toggle input field with the space bar.
- You can use the arrow key to navigate withn the field.

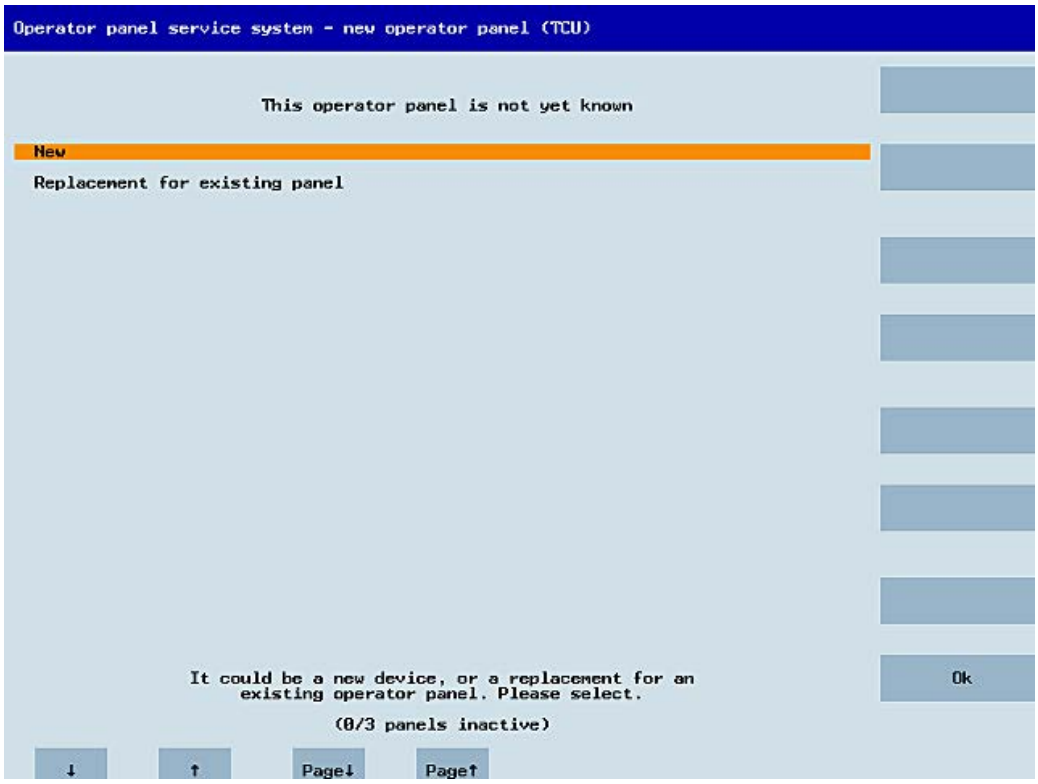
Further information on button operation can be found in the chapter "Key assignment (Page 133)" in the table of the same name.

6.2.4.5 Operating the menu for a new TCU or spare part TCU

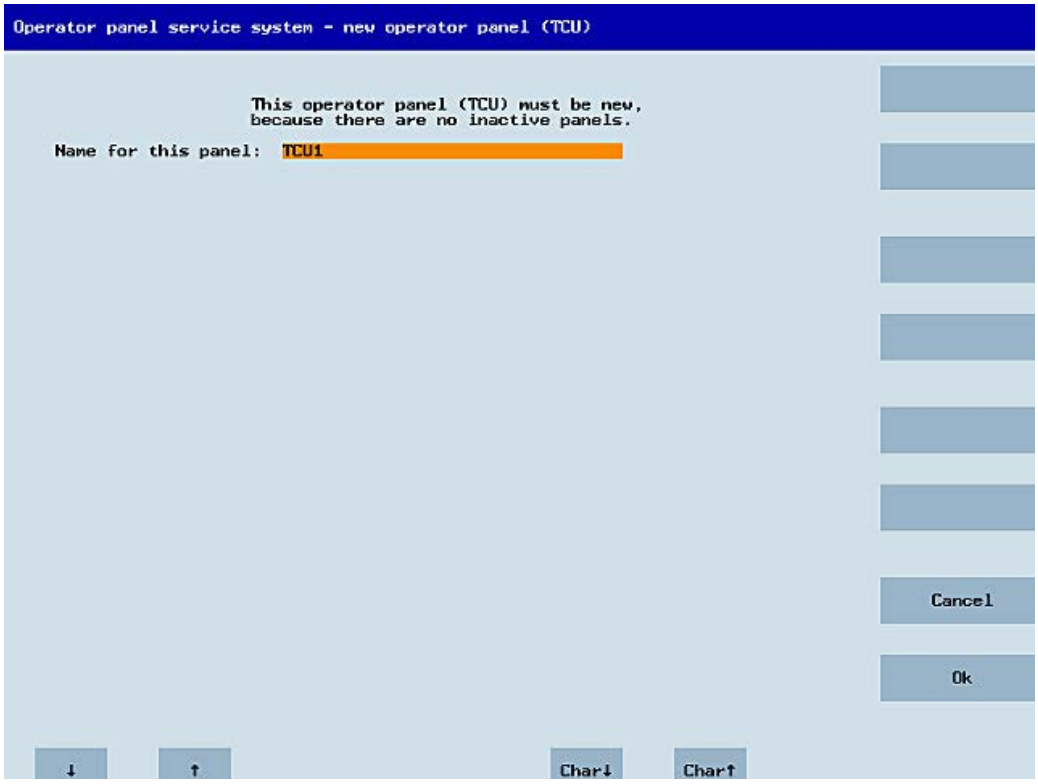
Registering a new TCU

When an unknown TCU, i.e. not yet registered with the boot server, is started, a selection menu containing both the "New" and "Replacement for existing panel" items is displayed. The accessibility of all the registered TCUs is tested in the background.

The status of this test is displayed in the message line: "(0/3 panels inactive)".



If all TCUs are active, the new TCU cannot be a spare part. The system will then automatically switch to the name assignment phase after a set period of time has elapsed.



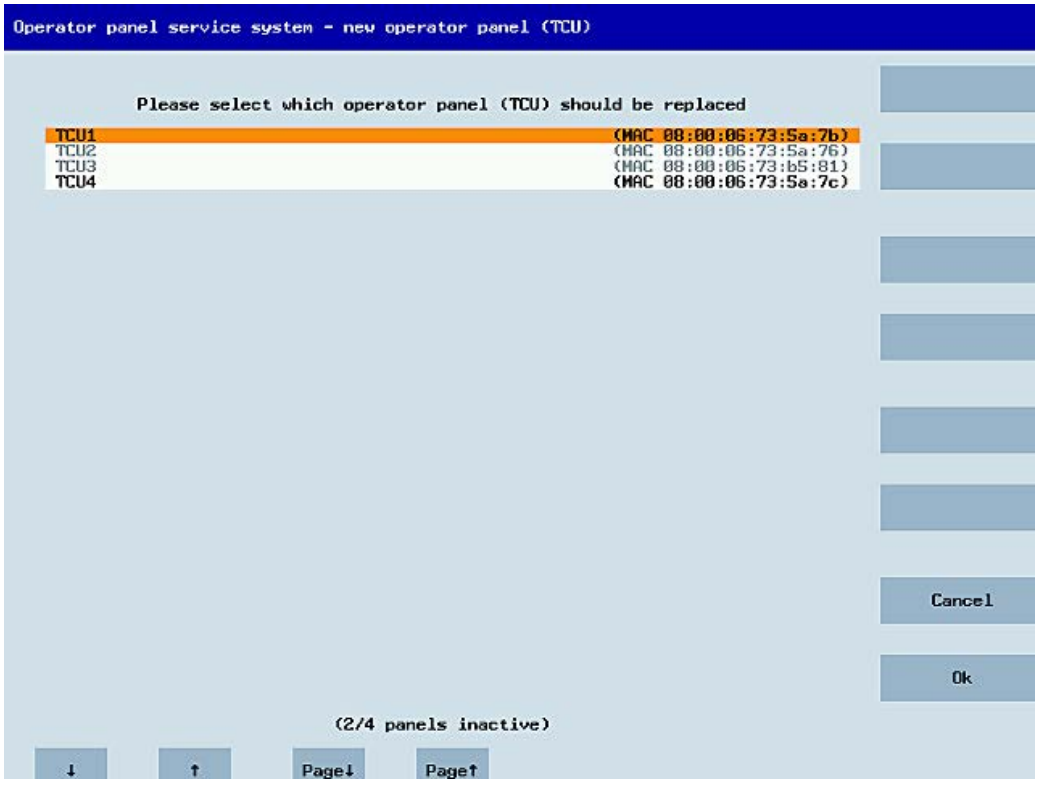
If a TCU30.3 is to be operated with a software version < 4.7 SP2, the TCU is operated in compatibility mode. If required, you can view and change the emulation type in the settings.

Replacing a device

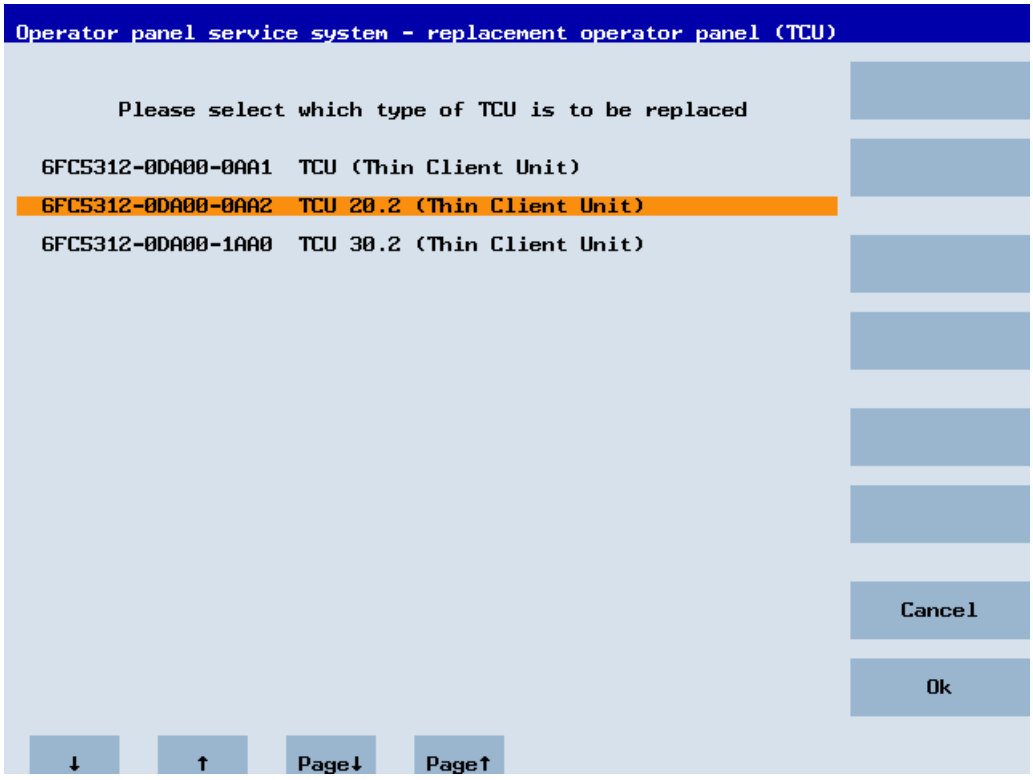
If "Replacement" is selected, all the registered TCUs will appear in a selection menu. Those which are active in the network are grayed out. They are functioning and should not be replaced by a spare part. The cursor automatically defaults to the first line for selection.

As the accessibility test is still running in the background, the active status of the lines may change if panels are switched on or off.

If a name is ultimately chosen, it will be applied to the new TCU along with the associated saved settings.



With the TCU30.3, after selecting the TCU to be replaced, a further dialog to select the emulation type can be displayed in compatibility mode:



If a static.ini of the TCU to be replaced (as of SW4.5) is found on the server, then the type of the old TCU is preselected based on the HW ID found there. If this is not the case, the TCU20.2 type is selected.

The following TCU types can be emulated:

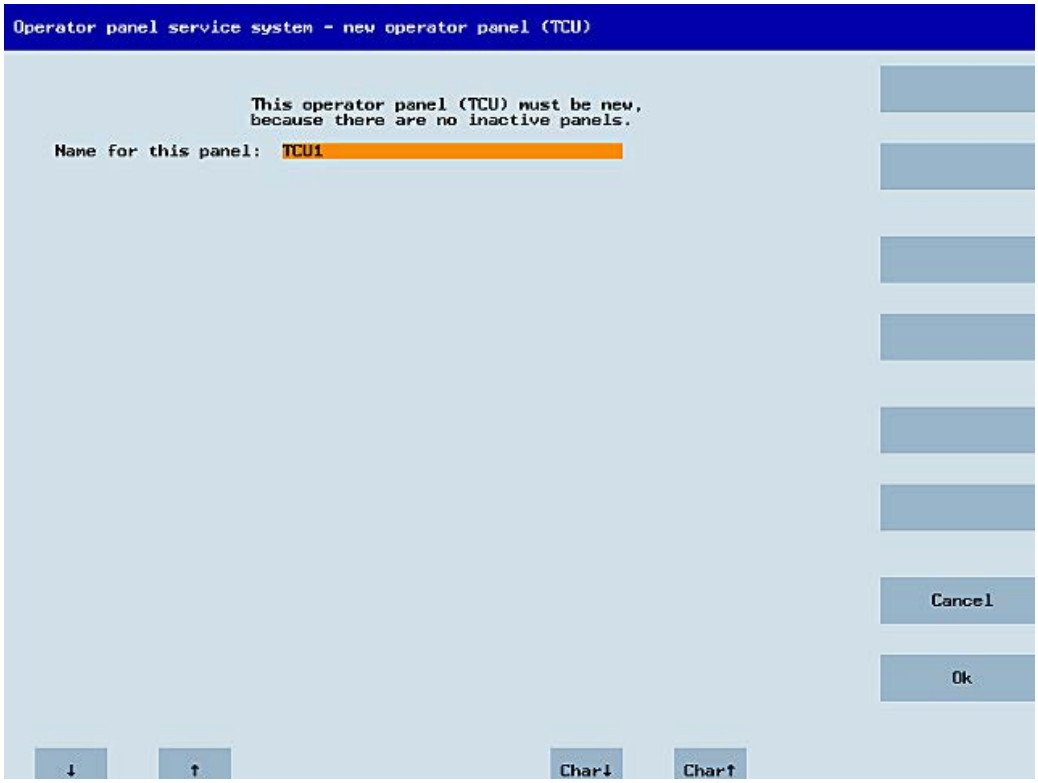
- TCU
- TCU 20.2
- TCU 30.2

Note that if an older TCU is to be replaced by a TCU30.3, some interfaces cannot be used when the HMI version is older than V4.7. The following interfaces are affected:

TCU to be replaced	Interfaces that cannot be used
TCU	X212, X213 (because they do not exist in the TCU)
TCU 20.2	X212 (because it does not exist in the TCU 20.2)
TCU 30.2	X211 (because it does not exist in the TCU 30.3)

Assigning a name

If, as described above, the system automatically follows the "New" path, an additional message will appear: "This operator panel (TCU) must be new, because there are no inactive panels." This message will not appear if "New" is selected manually.



An available TCU name is suggested in the input field, although the user is able to change this. The default name is "TCU<N>", where <N> is the lowest number yet to be used. If, however, the name is already allocated after the OK softkey has been pressed, which may happen if a number of TCUs log on at the same time, and the suggestion has not changed, a new and unused name will be specified.

If the name selected was still available, this will now be allocated, and the TCU settings can still be adapted if required. To enable any changes to be made, a new dialog appears in which all the parameters have been pre-assigned their default values. You can make any changes you like or just select "OK" to accept the existing values.

6.2.4.6 How to register a TCU on the system network

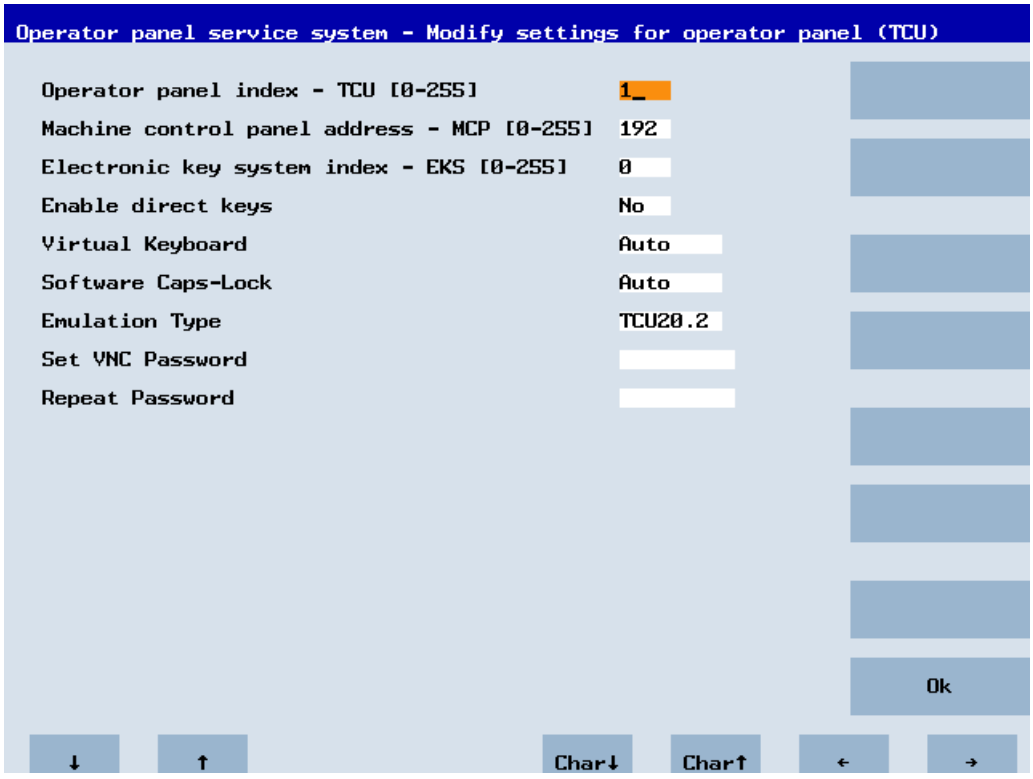
Requirement

The boot server (NCU or PCU 50/IPC) defined in the system network as a DHCP master must be switched on and available in the network.

Using the TCU

Procedure:

1. Connect the TCU.
   This opens the "New operator panel (TCU)" dialog.
2. Select "New" to connect a new TCU and "OK" to confirm.
3. In the next dialog, accept the name suggested by the system or enter a name and confirm this with "OK".
   The following parameters are preselected for the TCU:



4. Restart the TCU to apply the new settings.
5. If you want to change the parameters, select "Main menu" > "Service this panel" > "Modify operator panel settings".

Activate direct keys

The signals from pressing the direct keys are sent directly to the PLC. In the PLC, the keys appear as 16 digital inputs.

Additional information on programming the PLC is provided in:

SINUMERIK Basic Functions Function Manual, Basic PLC Program (P3)

Definition: Operator panel

The term operator station designates a unit that consists of an OP/TP, a TCU or PCU/IPC and a machine control panel (MCP), which are connected to each other via Ethernet.

All TCUs, PCU 50s and IPCs can be used along with the OP/TP with "integrated TCU", e.g. OP 08T, OP 015T, TP 015AT.

Specifying settings without machine control panel

If a PCU, IPC or TCU does not have a machine control panel (MCP), one of the two following options must be set:

- MCP address = 0 or no entry

  After the change of user authorization, there is no switchover of the machine control panel; the previously active MCP remains active.

- MCP address = 255

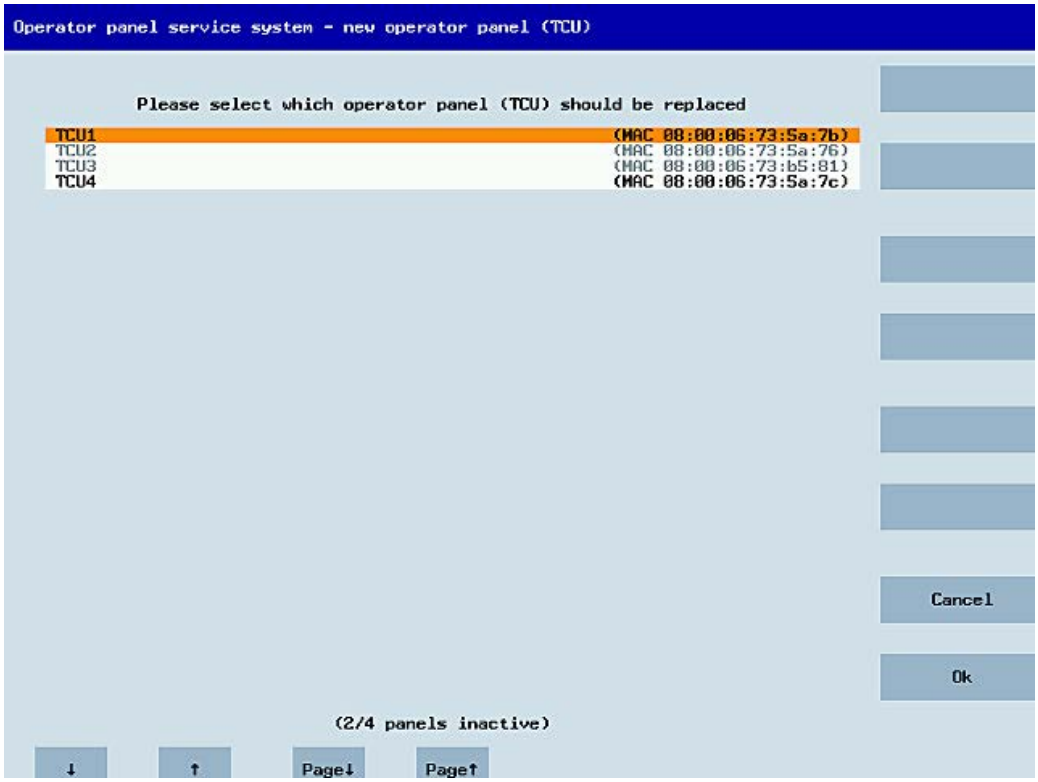
  If the user authorization is transferred to this PCU, IPC or TCU, the previous machine control panel is deactivated, and there is no active machine control panel as from this point.

6.2.4.7 This is how you register a spare part TCU

To connect the spare part TCU, proceed as follows:

1. Connect the new TCU.

   The "New operator panel (TCU)" dialog opens.
   This dialog lists the TCUs on the system network along with their "active" or "inactive" status:



2. Select the name previously assigned to the defective TCU. As a result, the new TCU is recognized on the network and acquires all of the configuration settings from the TCU that has been replaced.

6.2.4.8 Booting of the TCU

Messages during booting

Messages when booting

While the TCU boots, a progress indicator is displayed with messages showing the current status after the BIOS has been loaded and before the operating system is started. While the IP address is being determined via DHCP and the TFTP is being downloaded (boot image), a progress bar indicates that booting of the TCU is not yet complete, or that a fault has occurred.

You can see the current boot phase below the progress bar. If a fault occurs, you can call further information by touching the "F1" field.

Diagnostics options during booting

Diagnostics while booting supplementary conditions

In the following supplementary conditions, the diagnostics window is displayed and booting of the TCU is interrupted:

- When the <1 / F1> function is selected during booting
- When a warning message is displayed
- When a fault occurs

  You can select functions <1 / F1> to <8 / F8> mentioned below by tapping on the Panel. Alternatively, you can do this via the corresponding function keys of a connected USB keyboard.

Using the <1 / F1> function

Key / text	Meaning
F1 protocol	Display detailed information
F2 Readme_OSS	Details of the Open Source licenses
F7 continue	Continue booting of the TCU
F8 reboot	Restart the TCU

Press <1 / F1> to continue

If you select function <F1> in the diagnostics window, the, detailed diagnostic information is output.

Key / text	Meaning
F1 ... F6	Navigate within the window (alternatively, the relevant keys on the OP can be used).
F7 -detail	Display less information
F8 +detail	Display more information
F9 back	Return to diagnostics window

Device maintenance and repair 7

7.1 General information on maintenance and servicing

Observe the following when servicing and repairing protective equipment e.g. such as ground circuits or overvoltage protection components:

- Observe the maintenance and replacement intervals.
- Replace system components, including external cables, fuses and batteries only with equivalent components approved by the respective manufacturer.

7.2 Cleaning the device

The HMI device is designed for low-maintenance operation. However, you should still regularly clean the device front and, in the case of PRO devices, the entire device if necessary.

WARNING

Unintended reaction when cleaning the unit

You risk unintentional actuation of control elements if you clean the device while it is switched on.

You may unintentionally trigger actions of the device or controller. Personal injury or damage to the machinery may result.

Switch off the device before cleaning or, during ongoing operation, clean the touch screen only when it is in a locked state. Note that the touch screen lock automatically ends after 15 seconds.

Detergents

NOTICE

Damage to the HMI device caused by impermissible detergents

Inadmissible and unsuitable detergents can damage the HMI device.

Use only dish soap or foaming screen cleaner as detergents. Do not use the following detergents:

- Aggressive solvents or scouring powder
- Steam jets
- Compressed air

Observe the information on chemical resistance (https://support.industry.siemens.com/cs/ww/en/view/39718396).

Requirement

- The HMI device must be mounted correctly according to these operating instructions.
- Cleaning cloth
- Dishwashing liquid or foaming screen cleaning agent

Procedure

Proceed as follows:

1. Switch off the device or disable the touch screen using the "Clean screen" function in taskbar.

   If you use the "Clean screen" function, the touch screen is disabled for 15 seconds. If the cleaning requires more time, activate the "Clean screen" function several times for the entire cleaning period.

2. Spray detergents on the cleaning cloth and not directly on the device.
3. Clean the device with the cleaning cloth.

7.3 Spare parts and repairs

Repairs

Contact your Siemens representative (https://www.siemens.com/aspa). You can filter according to competence, product and region.

Your contact person can tell you whether a product can be repaired and which modalities apply for returning it.

Also contact your representative before returning your product if you need prioritized handling for repair of the product, a cost estimate, a repair report or fact-finding report.

Your contact person can also give you information about possible spare part procurement.

Spare parts

Spare parts and accessories for the HMI device can be found in section "System components and accessories (Page 25)".

7.4 Recycling and disposal

Due to the low levels of pollutants in the HMI devices described in these operating instructions, they can be recycled.

Contact a certified disposal service company for electronic scrap for environmentally sustainable recycling and disposal of your old devices and dispose of the device according to the relevant regulations in your country.

Before recycling or disposal, delete all data on the device by resetting the device to factory settings; see section "The "System" submenu (Page 85)".

Technical specifications

8

8.1 Labels, certificates and approvals

Note

Approvals on the rating plate

The following overview shows possible approvals.

Only the approvals specified on the rating plate apply to the device.

CE marking

The devices meet the general and safety-related requirements of the following EU Directives and conform with the harmonized European standards (EN) published in the official gazettes of the European Union and confirmed in the EU declarations of conformity:

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)
- 2011/65/EU "Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

If the device has Ex approval, the following also applies:

- 2014/34/EU "Equipment and protective systems for use in hazardous areas" (Explosion protection directive)

EU Declaration of Conformity

The EU Declarations of Conformity are available to the relevant authorities at the following address:

Siemens Aktiengesellschaft
DI FA
Gleiwitzer Straße 555
DE-90475 Nürnberg

The Declaration of Conformity and other certificates are also available at the following Internet address: Industrial Thin Clients Certificates
(https://support.industry.siemens.com/cs/ww/en/ps/16794/cert)

UKCA marking

The devices fulfill the requirements and protection goals of the following regulations and associated supplements and comply with the designated British standards (BS) published in the official consolidated list of the British Government.

- Electromagnetic Compatibility Regulations 2016 (EMC)
- Regulations on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2012 (RoHS)

If the device has Ex approval, the following also applies:

- Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016 (Explosion Protection)

UK Declarations of Conformity

The UK Declarations of Conformity are available to the relevant authorities at the following address:

Siemens plc
Princess Road
Manchester
M20 2UR
United Kingdom

You can also find these for download on the Internet at the following address, keyword "Declaration of Conformity":

Industrial Thin Clients Certificates
(https://support.industry.siemens.com/cs/ww/en/ps/16794/cert)

UL approval

Observe the following information:

- The device shall be supplied from an isolating source, rated 24 VDC.
- Only for use in LAN, not for connection to telecommunication circuits.

Underwriters Laboratories Inc. (E116536 or E472609) in accordance with

- UL 61010-1 and UL 61010-2-201
- CAN/CSA C22.2 No. 61010-1 and 61010-2-201

or

Underwriters Laboratories Inc. (E222109 or E472610) in accordance with

- UL 61010-1 and UL 61010-2-201
- CAN/CSA C22.2 No. 61010-1 and 61010-2-201
- UL 121201 (Hazardous Location)
- CAN/CSA C22.2 No. 213 (Hazardous Location)

Devices with article numbers -...1

Approved for use in

- Class I, II, III, Division 2, Group A, B, C, D, F, G; T4
- Class I, Zone 2, Group IIC T4
- Zone 22, Group IIIA, IIIB T135°C
- non-hazardous locations

Devices with article numbers -...0

Approved for use in

- Class I, Division 2, Group A, B, C, D; T4
- Class I, Zone 2, Group IIC; T4
- non-hazardous locations

FM Approval

Factory Mutual Research (FM) conforming to

- Approval Standard Class Number 3611, 3600, 3810
- ANSI/UL 61010-1
- ANSI/UL 121201
- ANSI/NEMA 250
- CSA-C22.2 No. 94
- CSA C22.2 No. 213
- CSA C22.2 No. 61010-1

Devices with article numbers -...1

Approved for use in

- Class I, II, III, Division 2, Group A, B, C, D, F, G; T4
- Class I, Zone 2, Group IIC T4
- Zone 22, Group IIIA, IIIB T135°C
- non-hazardous locations

Devices with article numbers -...0

Approved for use in

- Class I, Division 2, Group A, B, C, D; T4
- Class I, Zone 2, Group IIC T4
- non-hazardous locations

Installation instructions for cFMus:

WARNING – Do not remove or replace while circuit is live when a flammable or combustible atmosphere is present.

WARNING – Substitution of components may impair suitability of the equipment.

CAUTION – To prevent injury, read the manual before use.

Additional instructions for cFMus, built-in devices:

WARNING – The equipment is intended to be installed within an enclosure/control cabinet. The inner service temperature of the enclosure/control cabinet corresponds to the ambient temperature of the module. Use cables with a maximum permitted operating temperature of at least 20 °C higher than the maximum ambient temperature.

ATEX/UKEX/IECEx approval

Notes on use in hazardous areas

Observe the following FAQ regarding the use of an HMI device in hazardous areas: ATEX-FAQ (https://support.industry.siemens.com/cs/ww/en/view/291285)

When using the device in hazardous areas, ensure that all plugs connected to the device are secured in a captive manner, see section "Securing cables for use in hazardous areas (Page 68)".

You can find more information about explosion protection, EC/EU declarations of conformity and other certificates on the Internet at the following address: Industrial Thin Clients Certificates (https://support.industry.siemens.com/cs/ww/en/ps/16794/cert)

ATEX/UKEX approval

For an HMI device with "Ex" marking, the following approvals apply according to the following standards.

- Standards:
  - EN IEC 60079-0
  - EN IEC 60079-7
  - EN 60079-31
- Approvals:

	II 3 G	Ex ec IIC T4 Gc
	II 3 D	Ex tc IIIC T 70 °C Dc

ATEX certificate number

- Devices with article numbers -...0: DEKRA 19ATEX0111 X
- Devices with article numbers -...1: UL 23 ATEX 3022X

UKEX certificate number

- Devices with article numbers -...0: DEKRA 21UKEX0014X
- Devices with article numbers -...1: UL24UKEX2975X

IECEx approval

For an HMI device with "IECEx" marking, the following approvals apply according to the following standards.

- Standards:
  - IEC 60079-0
  - IEC 60079-7
  - IEC 60079-31
- Approvals:

	Ex ec IIC T4 Gc
	Ex tc IIIC T 70°C Dc

IECEx certificate number

- Devices with article numbers -...0: IECEx DEK 19.0071X
- Devices with article numbers -...1: IECEx UL 23.0042X

Specific Conditions of use

- When used in an area requiring the use of equipment with EPL Gc, the following additional conditions apply:
  - The equipment shall only be used in an area of at least pollution degree 2, as defined in IEC 60664-1.
  - Transient protection shall be provided that is set at a level not exceeding 119V, which is 140% of the peak rated voltage value at the supply terminals to the equipment.

- The front side of SIMATIC ITC V3 built-in series provides a degree of protection of at least IP65. The rear of the device shall be installed in a tool-accessible enclosure that provides a minimum degree of protection of IP54 for Zone 2 in accordance with IEC-EN 60079-7, at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP64 for Zone 22 with Group IIIC in accordance with IEC-EN 60079-31. User must follow details of installation method to complete the Ex tc end-equipment enclosure, see section 3.1.3 (Page 43), taking into account the applicable environmental conditions under which the equipment is used.
- Pedestal (flange bottom) type and Support arm (flange top) type of SIMATIC ITC V3 PRO series assembled with the packaged base adapter provide the degree of protection IP65. The underside of the base adapter shall be installed with a certified enclosure that ensures a minimum degree of protection of IP54 for Zone 2 in accordance with IEC/EN IEC 60079-7, and at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP6X with group IIIC in accordance with IEC/EN 60079-31.
- SIMATIC ITC V3 PRO support arm (round tube) type series assembled with packaged low cover provide the degree of protection IP65. The round tube opening of the device shall be installed with a certified enclosure which has a round tube end of 48.3 mm outside diameter that ensures a minimum degree of protection of IP54 for Zone 2 in accordance with IEC/EN IEC 60079-7, and at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP6X with group IIIC in accordance with IEC/EN 60079-31.
- SIMATIC ITC V3 built-in series is acceptable for use in different external ambient temperature ranges (Ta: 0 ˚C to 35 ˚C/40 ˚C/45 ˚C/50 ˚C) depending on mounting positions, internal ambient temperature for reference is 56.9 ˚C. SIMATIC ITC V3 PRO series is acceptable for use in different external ambient temperature ranges (Ta: 0 °C to 40 °C/45 °C), depending on the mounting position. Users shall access Ambient Conditions section (Page 43) for details.
- For SIMATIC ITC V3 built-in series, the fastener shall only be replaced with 6AV6881-6AD10-0AA0, which is specified by the manufacturer.
- For SIMATIC ITC V3 PRO series, the fastener shall only be replaced with M4 screws specified by the manufacturer.
- USB interfaces are not permitted to connect with USB devices except for equipment with USB cable connection.
- The side cover on the either side of Base adapter (Article number: 6AV7674-1KA00-0AA0) must not be opened during installation or normal operation.
- To avoid an electrostatic charge, wipe the enclosure surface with a damp cloth only.

CCCEx approval

The following approvals according to the following standards are valid for a device with the "CCC" marking.

- Standards:
  - GB/T 3836.1 (Explosive atmospheres - Part 1: Equipment - General requirements)
  - GB/T 3836.3 (Explosive atmospheres - Part 3: Device protection through type of protection "e")
  - GB/T 3836.31 (Explosive atmospheres - Part 31: Equipment dust explosion protection by enclosure "t")

- Approvals:
  - Ex ec IIC T4 Gc
  - Ex tc IIIC T70°C Dc

Special conditions of use

- When used in an area requiring the use of equipment with EPL Gc, the following additional conditions apply:
  - The equipment shall only be used in an area of at least pollution degree 2, as defined in GB/T 16935.1.
  - Transient protection shall be provided that is set at a level not exceeding 119V, which is 140% of the peak rated voltage value at the supply terminals to the equipment.
- The front side of SIMATIC ITC V3 built-in series provides a degree of protection of at least IP65. The rear side of the device shall be installed in a tool accessible enclosure that provides a minimum degree of protection of IP54 for Zone 2 in accordance with GB/T 3836.3, at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP64 for Zone 22 with group IIIC in accordance with GB/T 3836.31. User must follow details of installation method to complete the Ex tc end-equipment enclosure, see section 3.1.3 (Page 43), taking into account the applicable environmental conditions under which the equipment is used.
- Pedestal (flange bottom) type and Support arm (flange top) type of SIMATIC ITC V3 PRO series assembled with the packaged base adapter provide the degree of protection IP65. The underside of the base adapter shall be installed with a certified enclosure that ensures a minimum degree of protection of IP54 for Zone 2 in accordance with GB/T 3836.3, and at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP6X with group IIIC in accordance with GB/T 3836.31.
- SIMATIC ITC V3 PRO support arm (round tube) type series assembled with packaged low cover provide the degree of protection IP65. The round tube opening of the device shall be installed with a certified enclosure which has a round tube end of 48.3 mm outside diameter that ensures a minimum degree of protection of IP54 for Zone 2 in accordance with GB/T 3836.3, and at least IP54 for Zone 22 with Group IIIA and IIIB and at least IP6X with group IIIC in accordance with GB/T 3836.31.
- SIMATIC ITC V3 built-in series are acceptable for use in different external ambient temperature ranges (Ta: 0˚C to 35˚C/40˚C/45˚C/50˚C) depending on mounting positions, internal ambient temperature for reference is 56.9˚C. SIMATIC ITC V3 PRO series are acceptable for use in different ambient temperature ranges (Ta: 0˚C to 40˚C/45˚C) depending on mounting positions. Users shall access Ambient Conditions section (Page 178) for details.
- For SIMATIC ITC V3 built-in series, the fastener shall only be replaced by article number 6AV6881-6AD10-0AA0, which is specified by the manufacturer.
- For SIMATIC ITC V3 PRO series, the fastener shall only be replaced with M4 screws specified by the manufacturer.
- USB interfaces are not permitted to connect with USB devices except for equipment with USB cable connection.
- The side cover on the either side of Base adapter (Article number: 6AV7674-1KA00-0AA0 must not be opened during installation or normal operation.
- To avoid an electrostatic charge, wipe the enclosure surface with a damp cloth only.

根据以下标准，以下许可适用于带有“CCC”标识的设备。

- 标准：
  - GB/T 3836.1 （爆炸性环境 - 第 1 部分：设备 通用要求）
  - GB/T 3836.3 （爆炸性环境 - 第 3 部分：由增安型“e”保护的设备）
  - GB/T 3836.31（爆炸性环境 - 第 31 部分：由防粉尘点燃外壳“t”保护的设备）
- 许可：
  - Ex ec IIC T4 Gc
  - Ex tc IIIC T70°C Dc

安全使用条件：

- 在需要EPL Gc设备的区域使用时，以下附加条件适用：
  - 根据GB/T 16935.1，该设备只应在污染程度不低于2级的区域使用。
  - 应采取措施防止在119V的瞬态干扰下，额定电压超额，瞬态保护应提供不超过设备的供电端子额定峰值电压值140%的保护。
- SIMATIC ITC V3built -in 系列前面板外壳防护等级为IP65。应将其后部安装在一个经认证的外壳中：在气体环境2区使用时，应符合GB/T 3836.3的要求，至少IP54的防护等级；在非导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP54的防护等级；在导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP64的防护等级。用户必须按照详细的安装方法来完成Ex tc终端设备外壳的安装，参见第3.1.3节 (Page 43)，同时考虑设备的适用环境条件。
- SIMATIC ITC V3 PRO系列的底座(法兰朝下)型和支撑臂(法兰朝上)型与包装中的底座适配器组装在一起，提供IP65的保护等级。底座适配器的底部应安装在经认证的外壳中：

  在气体环境2区使用时，应符合GB/T 3836.3的要求，至少IP54的防护等级；在非导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP54的防护等级；在导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP6X的防护等级。
- SIMATIC ITC V3 PRO系列的支撑臂(圆管)型与包装中的底盖组装在一起，提供IP65的保护等级。设备圆管的开孔端应与经认证的外壳连接：能适配圆管末端外径48.3mm，且在气体环境2区使用时，应符合GB/T 3836.3的要求，至少IP54的防护等级；在非导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP54的防护等级；在导电粉尘环境使用时，应符合GB/T 3836.31的要求，至少IP6X的防护等级。
- 根据安装位置的不同，SIMATIC ITC V3 built-in系列可在不同的使用环境温度范围（Ta：0℃至35℃/40℃/45℃/50℃）内使用，内部参考环境温度为 56.9℃，SIMATIC ITC V3 PRO 系列可在不同的使用环境温度范围（Ta：0℃至40℃/45℃）内使用。用户可参阅环境条件部分 (Page 178)了解详情。
- SIMATIC ITC V3 built-in系列，紧固件只能用制造商指定的6AV6881-6AD10-0AA0替换。
- SIMATIC ITC V3 PRO系列，紧固件只能使用制造商指定的M4螺钉替换。
- 除使用USB线缆连接的设备外，USB接口不允许连接任何USB设备。
- 底座适配器两侧的侧盖(商品编号:6AV7674-1KA00-0AA0)严禁在安装或正常使用时打开。
- 为避免静电，仅使用湿布擦拭机箱表面。

IEC 61010-2-201/IEC 61131-2

The devices meet the requirements and criteria of the IEC 61010-2-201 and/or IEC 61131-2 standard.

- IEC 61010-2-201, Safety regulations for electrical equipment for measurement, control, and laboratory use: Particular requirements for control equipment
- IEC 61131-2, Programmable controllers: Equipment requirements and testing

RCM Australia/New Zealand

This product meets the requirements of the standard EN 61000-6-4 Generic standards – Emission standard for industrial environments.

BIS India

This product is certified by the Bureau of Indian Standards (R-41259519) in accordance with

- IS 13252 (Part 1)
- IEC 60950-1

Korea Certificate

This product conforms to Limit Class A for emission of radio interference. This device is not intended to be used in residential areas.

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

EAC (Euroasian Conformity)

The EAC (Eurasian Conformity) marking confirms the conformity with the technical regulations (TR) of the Eurasian Economic Union.

WEEE label (European Union)

Disposal instructions, observe the local regulations and the section "Recycling and disposal (Page 166)".

8.2 Electromagnetic compatibility

The HMI device satisfies, among other things, the requirements of the EMC guidelines of the European domestic market.

EMC-compatible installation of the HMI device

The EMC-compliant installation of the HMI device and the application of interference-proof cable is the basis for interference-free operation.

Observed the following manuals in addition to these operating instructions:

- Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566)
- Industrial Ethernet/PROFINET – Passive network components (https://support.industry.siemens.com/cs/ww/en/view/84922825)

Pulse-shaped disturbance

The following table shows the electromagnetic compatibility of modules with regard to pulse-shaped interference. The precondition for electromagnetic compatibility is that the HMI device meets the specifications and guidelines for electrical installation.

Pulse-shaped interference	Tested with	Corresponds to Test level
Electrostatic discharge in accordance with IEC 61000-4-2	Air discharge: 8 kV	3
	Contact discharge: 6 kV (built-in units on the front, PRO devices all-around)	
	Contact discharge: 4 kV (built-in units on the rear side)	2
Bursts (high-speed transient disturbance variable) in accordance with IEC 61000-4-4	2 kV supply line 1 kV signal line, < 30 m	3
	2 kV signal line, > 30 m	4
High-energy single pulse (surge) according to IEC 61000-4-5 Coupling procedure: 42 Ω, 0.5 µF [1]	Asymmetric coupling (line to ground):	
	• 1 kV supply line, direct voltage	2
	• 2 kV signal cable/data cable, > 30 m	3
	Symmetrical coupling (line to line):	
	• 0.5 kV supply line, direct voltage	2
	• 1 kV signal line, > 30 m	3

[1] Basically, you must connect the HMI device to your own distribution system (or batteries) via an upstream local power supply. If you connect the HMI device directly to your own distribution system, you must provide additional protective measures against overvoltage.

Sinusoidal interference

The following table shows the EMC behavior of the modules with respect to sinusoidal interference. This requires the HMI device to meet the specifications and directives for electrical installation.

Sinusoidal interference	Test values
HF radiation (electromagnetic fields) according to IEC 61000-4-3	80% amplitude modulation at 1 kHz • on 10 V/m in the range of 80 MHz to 1 GHz • on 3 V/m in the range of 1.4 to 6 GHz
HF current feed on cables and cable shields according to IEC 61000-4-6	Test voltage 10 V at 80% amplitude modulation of 1 kHz in the range from 150 kHz to 80 MHz
Magnetic field strength according to IEC 61000-4-8	50/60 Hz; 100 A/m RMS

Emission of radio interference

The following table shows the interference emissions from electromagnetic fields in accordance with EN/IEC 61000-6-4, measured at the following distance.

Radiated emission (interference emission)

Frequency range	Measuring distance	Interference emission
30 to 230 MHz	10 m	< 40 dB (µV/m) quasi-peak
230 to 1000 MHz	10 m	< 47 dB (µV/m) quasi-peak
1 to 3 GHz	3 m	< 76 dB peak and < 56 dB average
3 to 6 GHz	3 m	< 80 dB peak and < 60 dB average

Emission of radio interference voltages

Frequency range	Interference emission
0.150 to 0.5 MHz	< 89 dB quasi peak and < 76 dB average
0.5 to 30 MHz	< 83 dB quasi peak and < 70 dB average

See also

EMC information in section "Notes about usage (Page 39)".

8.3 Mechanical environmental conditions

8.3.1 Storage conditions

The following information is for a device that is transported and stored in its original packaging.

Type of condition	Permitted range
Free fall	≤ 0.3 m
Vibration according to IEC 60068-2-6	5 .. 8.4 Hz, deflection 3.5 mm 8.4 ... 500 Hz, acceleration 1 g
Shock according to IEC 60068-2-27	250 m/s^2, 6 ms, 1000 shocks

8.3.2 Operating conditions

The following information applies to a device installed according to the specifications in these operating instructions.

Built-in units

Type of condition	Permitted range
Vibration according to IEC 60068-2-6	5 ... 8.4 Hz, deflection 3.5 mm 8.4 ... 200 Hz, acceleration 1 g
Shock according to IEC 60068-2-27	150 m/s^2, 11 ms, 3 shocks

Shock pulses within the specified range can be transferred to the display but do not impact the functionality of the device.

PRO devices

Type of condition	Permitted range
Vibration according to IEC 60068-2-6	10 ... 58 Hz, deflection 0.0375 mm 58 ... 200 Hz, acceleration 0.5 g
Shock according to IEC 60068-2-27	150 m/s^2, 11 ms, 3 shocks

Shock pulses within the specified range can be transferred to the display but do not impact the functionality of the device.

8.4 Climatic ambient conditions

8.4.1 Transport and storage conditions

The following information applies to a device that is transported in the original packaging and weather-proof packaging, and stored from some time.

Type of condition	Permitted range
Temperature	–20 ... 60 °C
Atmospheric pressure	1140 ... 660 hPa, corresponds to an elevation of -1000 to 3500 m
Relative humidity	10 ... 90 %
Pollutant concentration	In accordance with ANSI/ISA-71.04-2013 severity level G3

Note

If dewing has developed, wait until the HMI device has dried completely before switching it on.

Do not expose the HMI device to direct radiation from a heater.

8.4.2 Operating Conditions

The following information applies to a device installed according to the specifications in these operating instructions.

The HMI device is designed for weatherproof and stationary operation.

Type of condition	Mounting position	ITC1200/1500	ITC1900/2200/2400
Temperature **Built-in units**, Mounting in landscape format	Vertical	0 ... 50 °C	0 ... 45 °C
	Inclined, maximum inclination 35°	0 ... 40 °C	
Temperature **Built-in units**, Mounting in portrait format	Vertical	0 ... 40 °C	
	Inclined, maximum inclination 35°	0 ... 35 °C	
Temperature **PRO devices** [1]	Vertical	0 ... 45 °C	
	Inclined, maximum inclination 35°	0 ... 40 °C	
Air pressure, operating elevation	1140 ... 795 hPa, corresponds to an elevation of -1000 to 2000 m		
Relative humidity	10 ... 90 %, no condensation [2]		
Pollutant concentration	In accordance with ANSI/ISA-71.04-2013 severity level G3		

[1] For PRO devices, mounting is only permitted in the standard mounting position
[2] Built-in units: no condensation on the back of the device,
PRO devices: no condensation inside the enclosure

Read the information in the section "Notes on use (Page 39)" and the information about the mounting positions:

- Permitted mounting positions for built-in units (Page 43)
- Permitted mounting positions for PRO devices (Page 47)

Note

The system components connected to the HMI device, the power supply for example, must also be suited to the respective operating conditions.

8.5 Information on insulation tests, protection class and degree of protection

Insulation test

The insulation resistance is verified by type testing with the following test voltages:

Circuit	Insulation tested with (type test)
Rated voltage U_e 24 V	707 V DC to other circuits / to ground
Ethernet connector	2250 V DC

Degree of pollution

The device meets the following requirements according to IEC 61010-2-201:

Device type	Built-in unit	PRO device	Degree of pollution
Devices without ATEX approval	Front	Outside	Not applicable because IP65
	Rear	Inside	2
Devices with ATEX approval	Front and rear	Outside and inside	2

Overvoltage category

Overvoltage category II in accordance with IEC 61010-2-201.

Protection class

Protection class III according to IEC 61010-2-201.

Protection from foreign objects and water built-in devices

The device meets the requirements of IEC 60529 and UL50E.

Device side	Degree of protection
Front	When mounted: • IP65 according to IEC 60529 • Enclosure Type 4X/12 (indoor use only, front face only) according to UL50E
Rear panel	IP20 Protection against contact with standard test probes. There is no protection against the ingress of water, dust and noxious gas.

The front protection rating can only be guaranteed if the mounting seal lies flush against the mounting cutout. Read the corresponding information in section "Preparing the mounting cutout (Page 45)".

Protection from foreign objects and water PRO devices

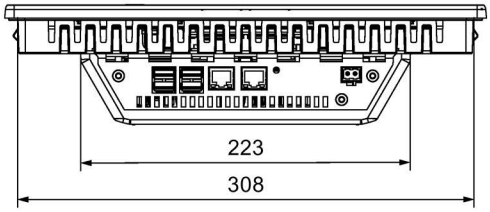
The device meets the requirements of IEC 60529 and UL50E.

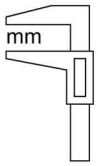
Device side	Degree of protection
Fully enclosed	• IP65 according to IEC 60529 • Enclosure Type 4X/12 (indoor use only) according to UL50E

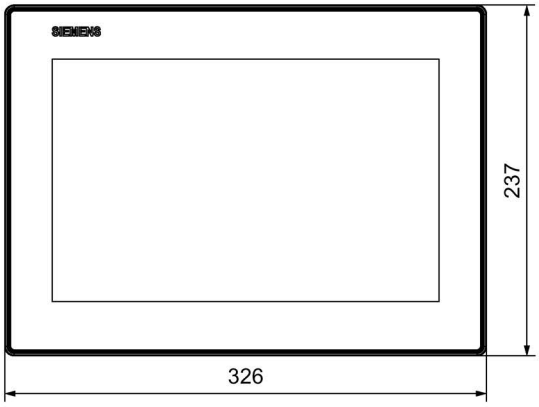
The types of protection can only be ensured if the seals are completely in contact with all mechanical interfaces and the connection compartment and the associated covers are closed.

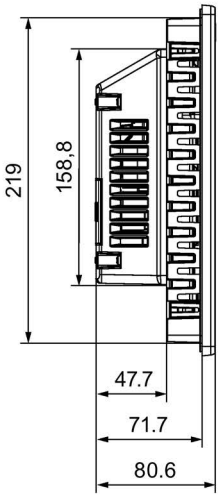
8.6 Dimensional drawings

8.6.1 ITC1200 V3

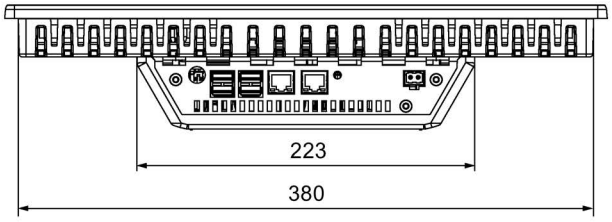


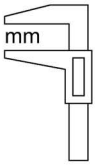


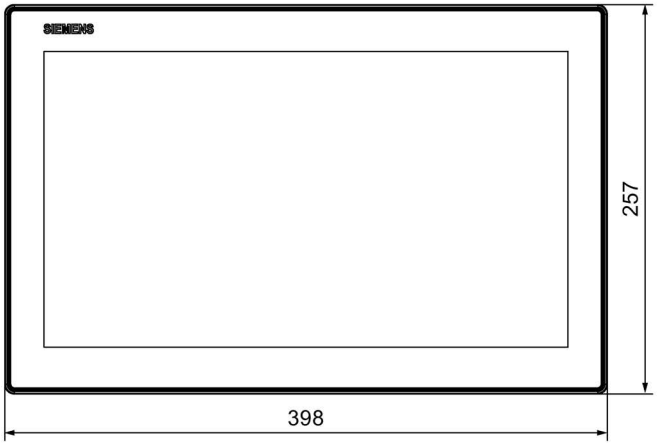


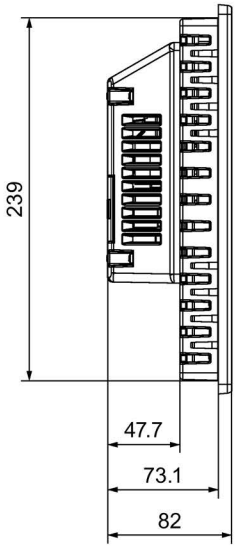


8.6.2 ITC1500 V3

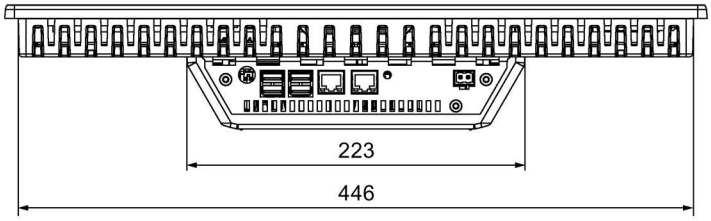


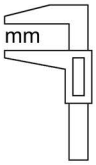


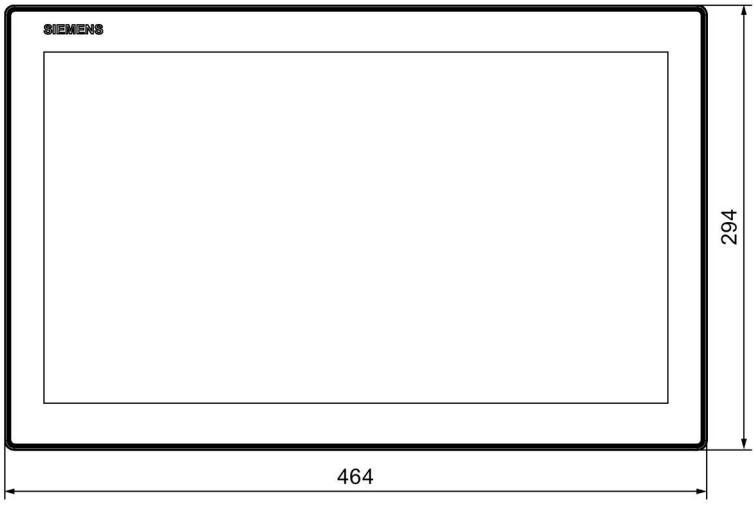


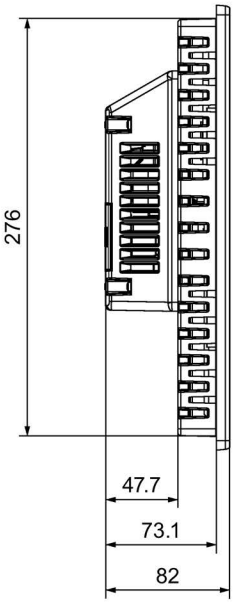


8.6.3 ITC1900 V3

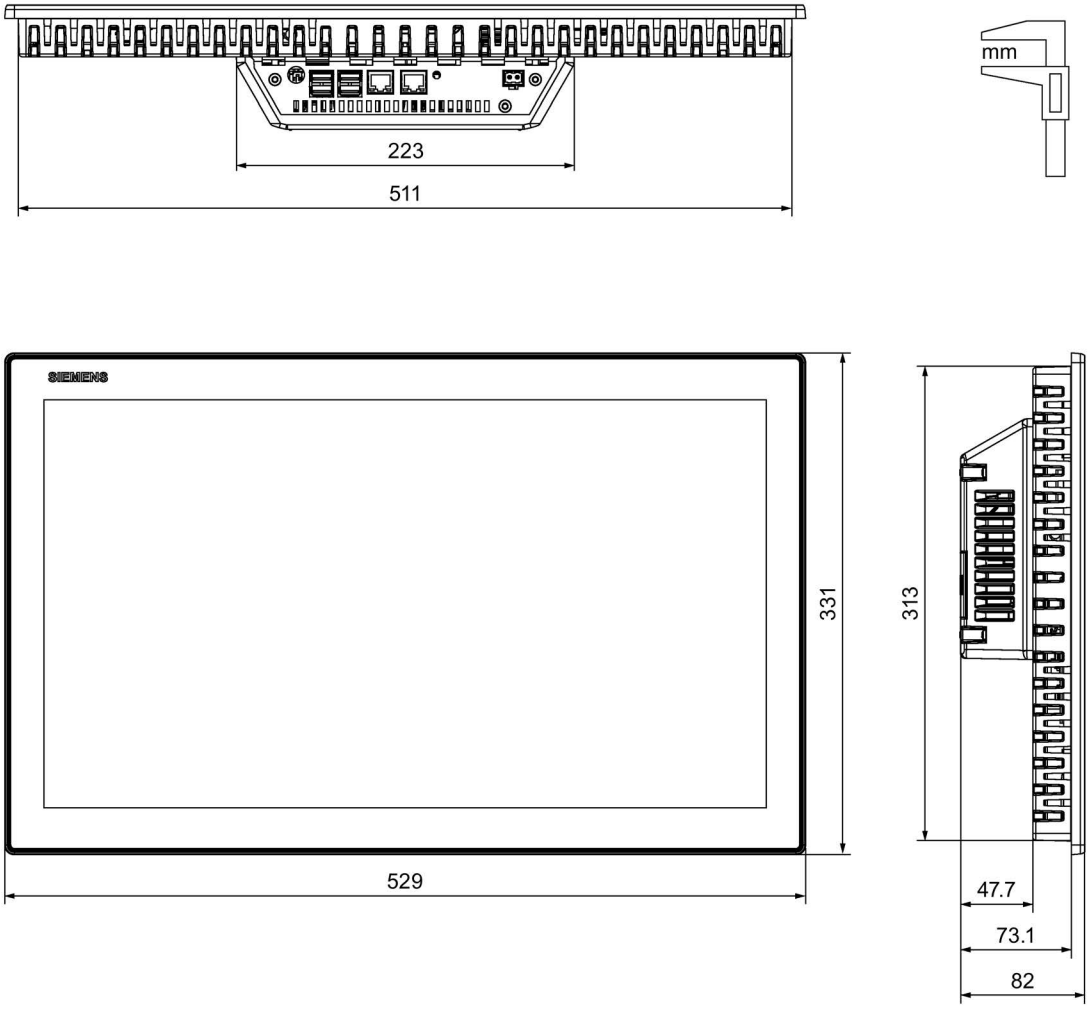




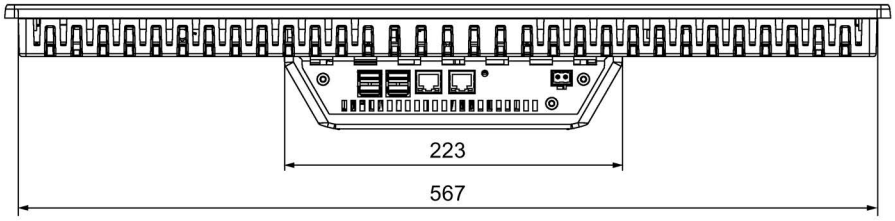


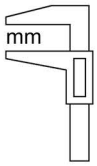


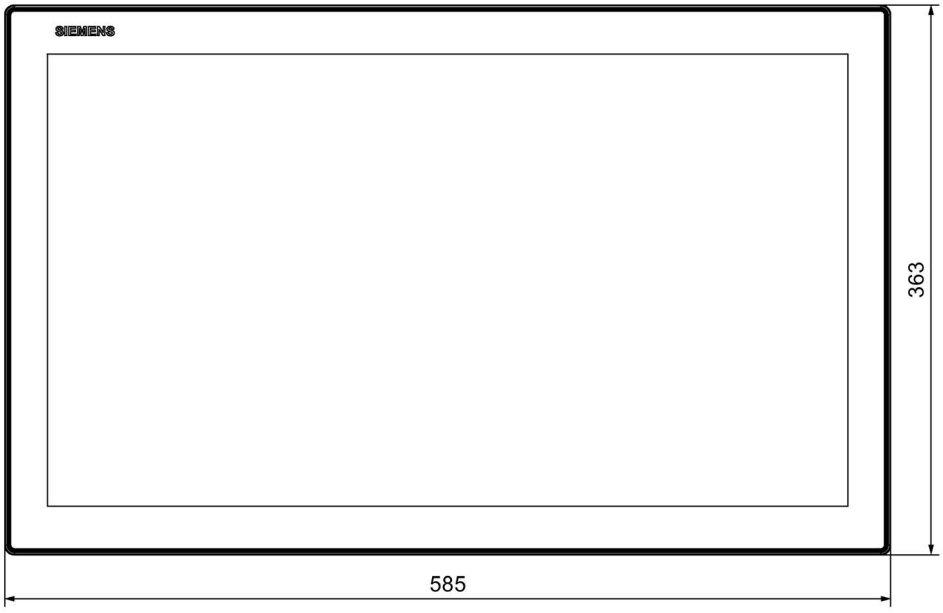
8.6.4 ITC2200 V3

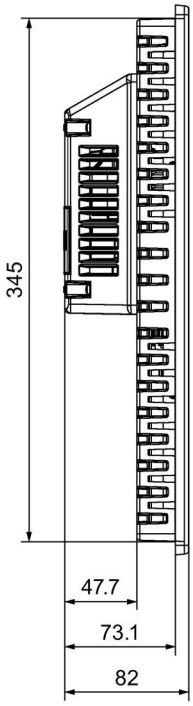


8.6.5 ITC2400 V3



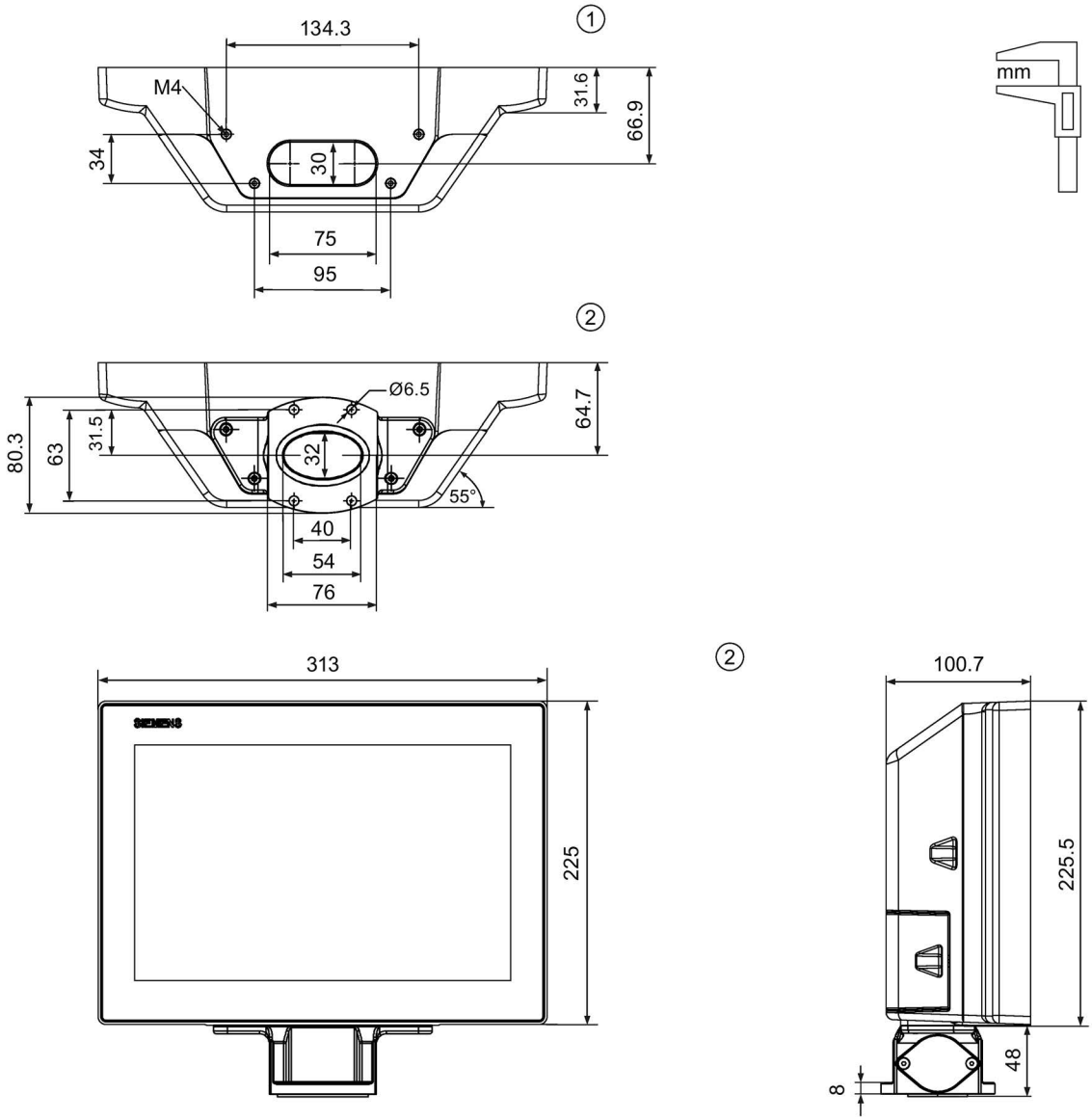






8.6.6 ITC1200 V3 PRO

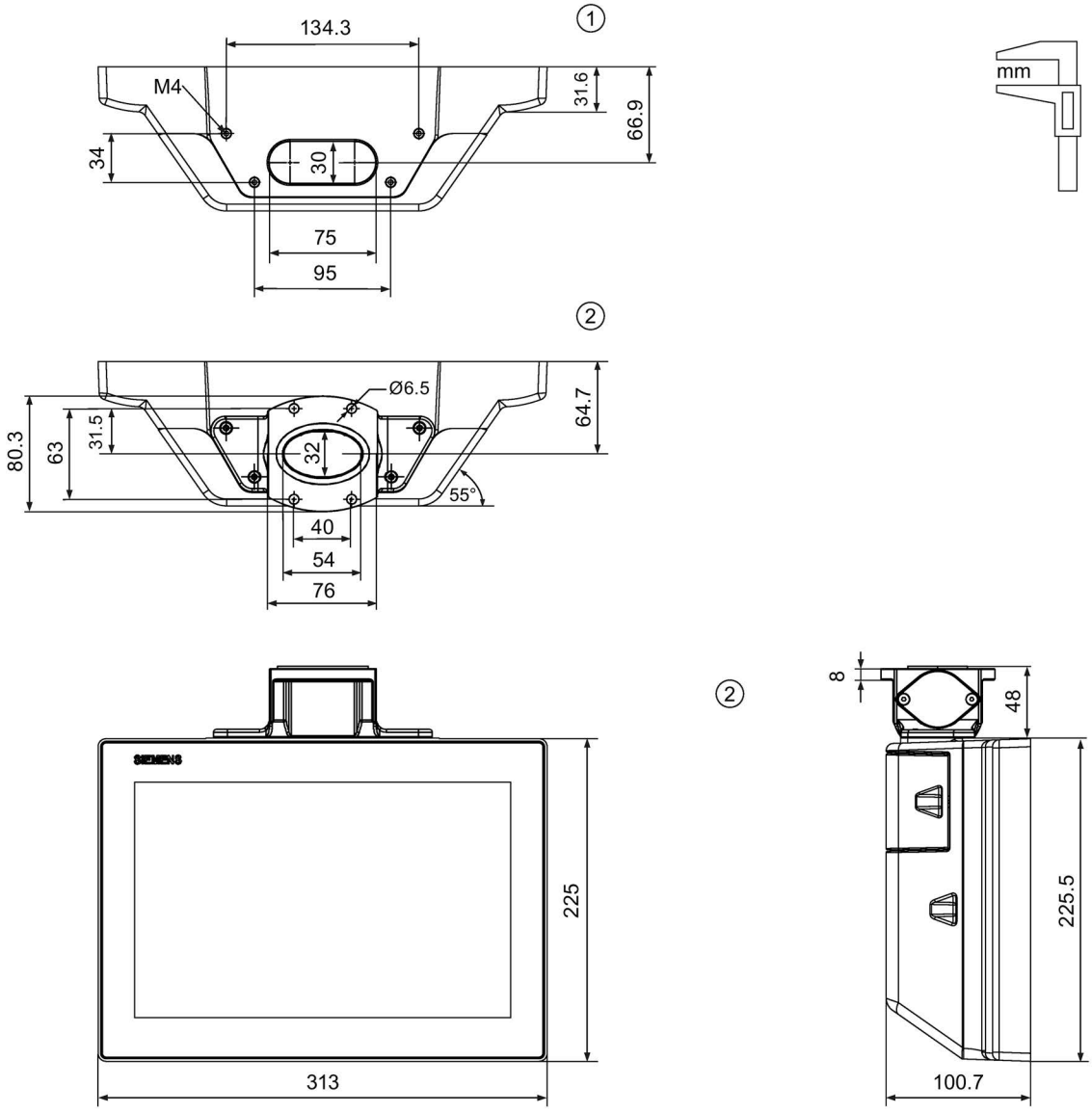
ITC1200 V3 PRO for pedestal (extendable, flange bottom)



① Without base adapter

② With base adapter

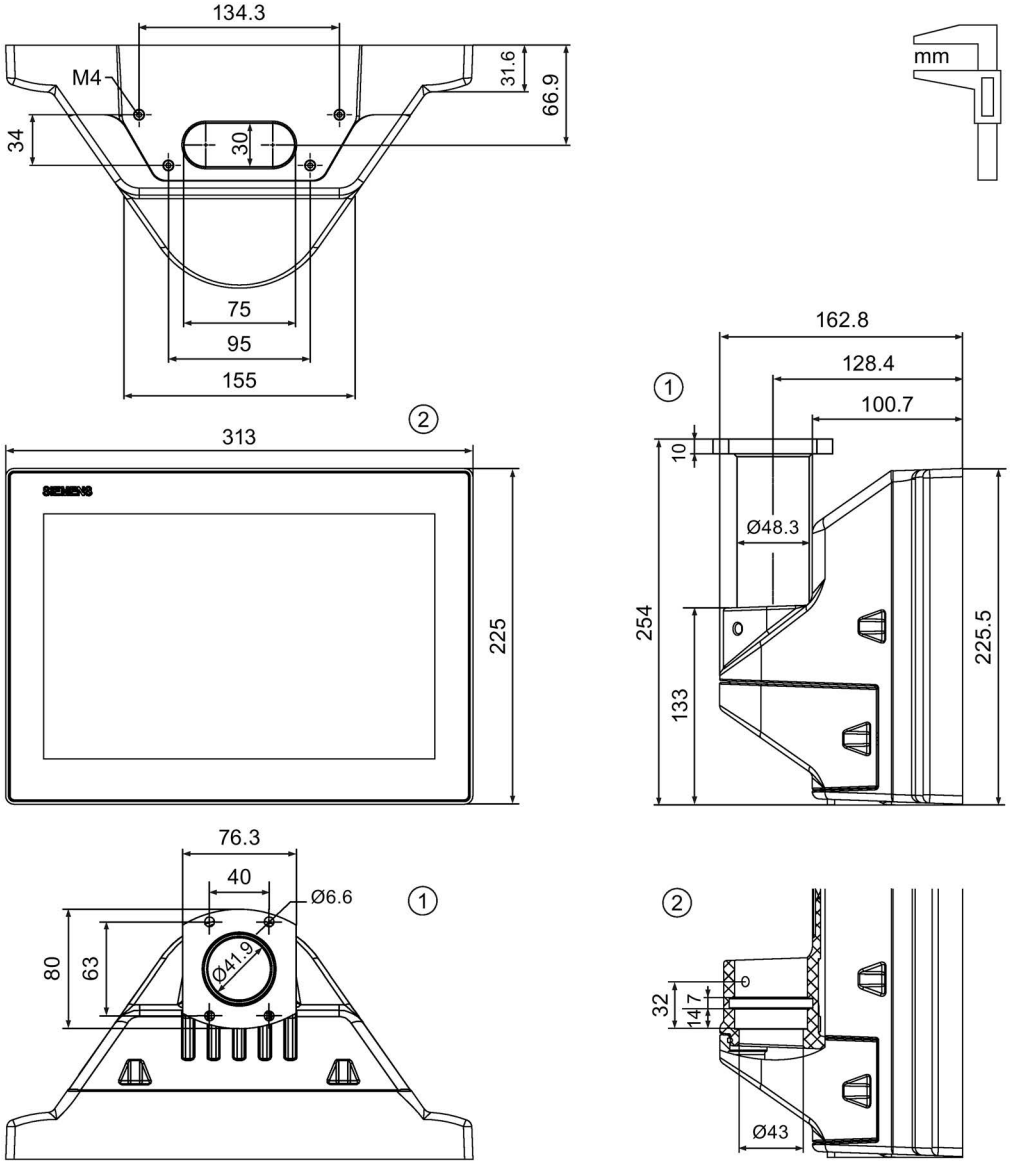
ITC1200 V3 PRO for support arm (not extendable, flange top)



① Without base adapter

② With base adapter

ITC1200 V3 PRO for support arm (extendable, round tube)

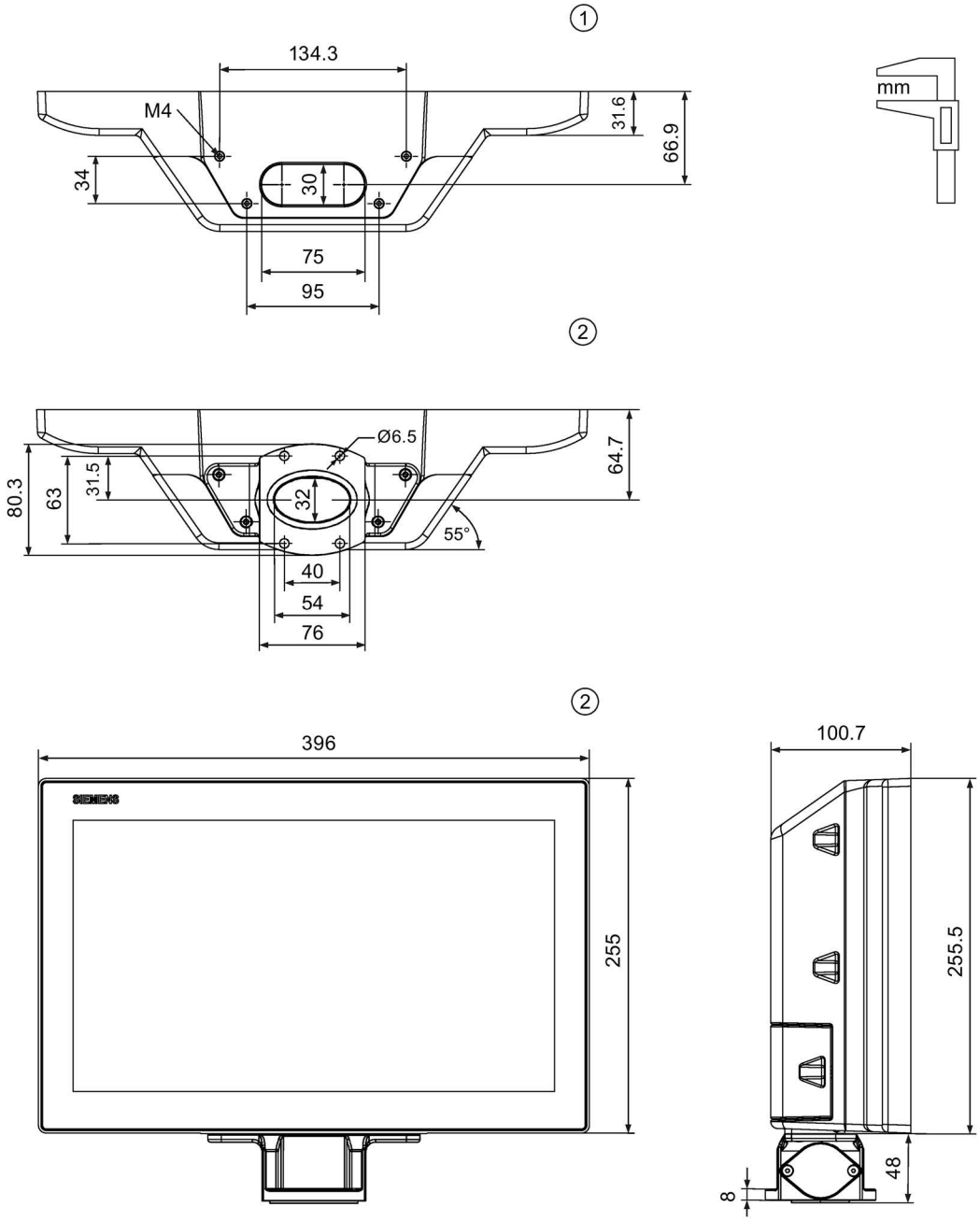


① with flange mount adapter

② without flange mount adapter

8.6.7 ITC1500 V3 PRO

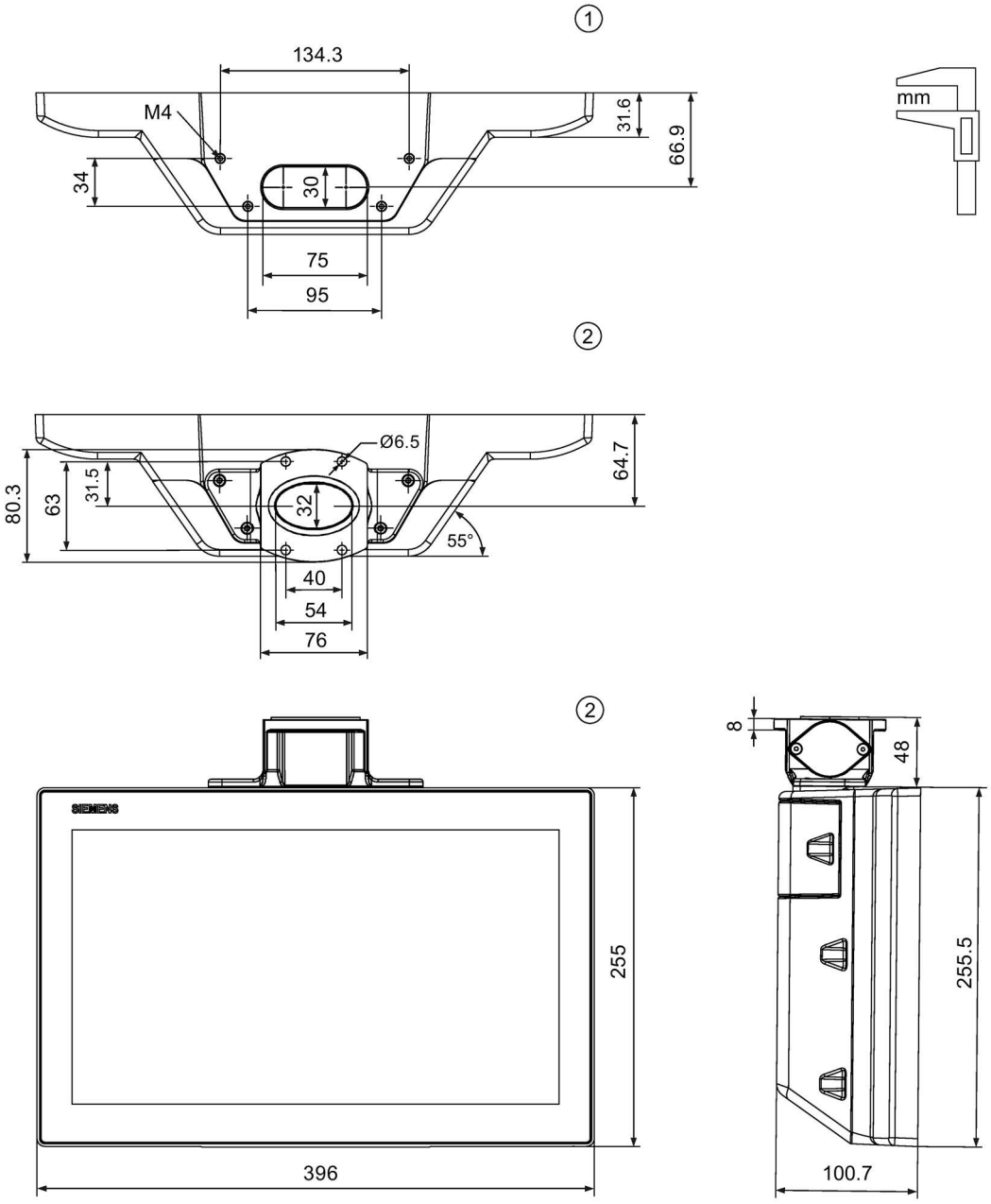
ITC1500 V3 PRO for pedestal (extendable, flange bottom)



① Without base adapter

② With base adapter

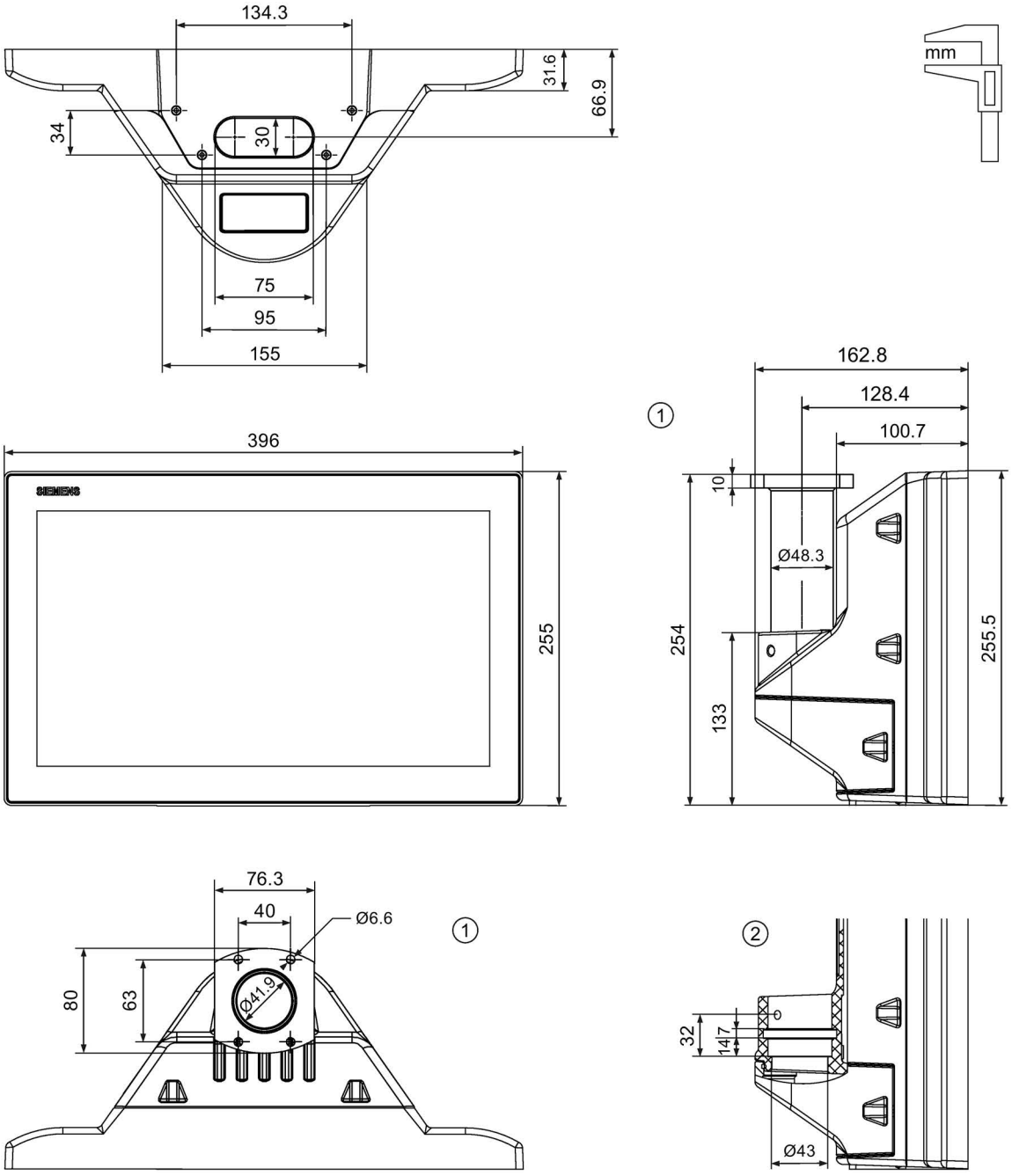
ITC1500 V3 PRO for support arm (not extendable, flange top)



① Without base adapter

② With base adapter

ITC1500 V3 PRO for support arm (extendable, round tube)

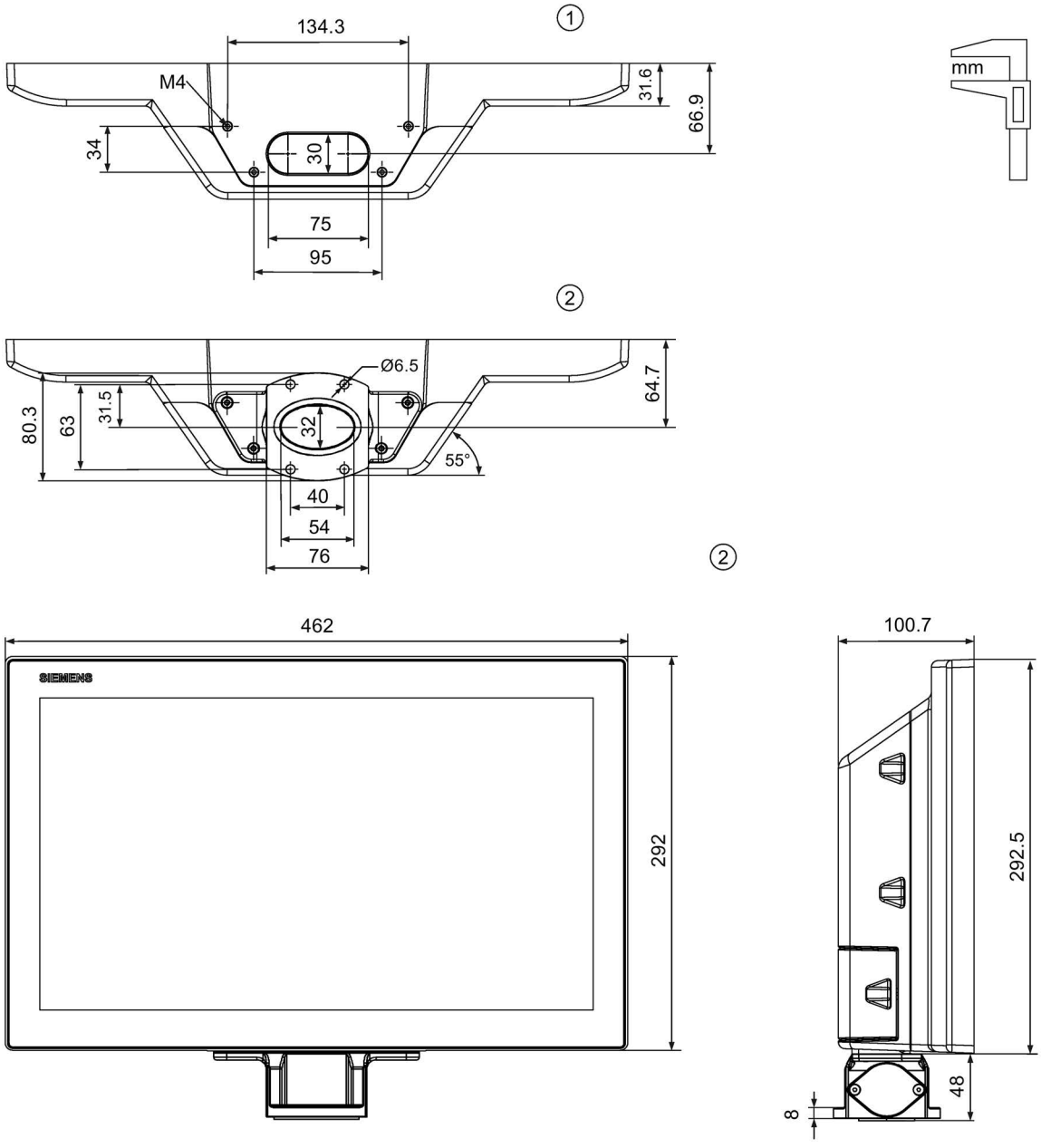


① with flange mount adapter

② without flange mount adapter

8.6.8 ITC1900 V3 PRO

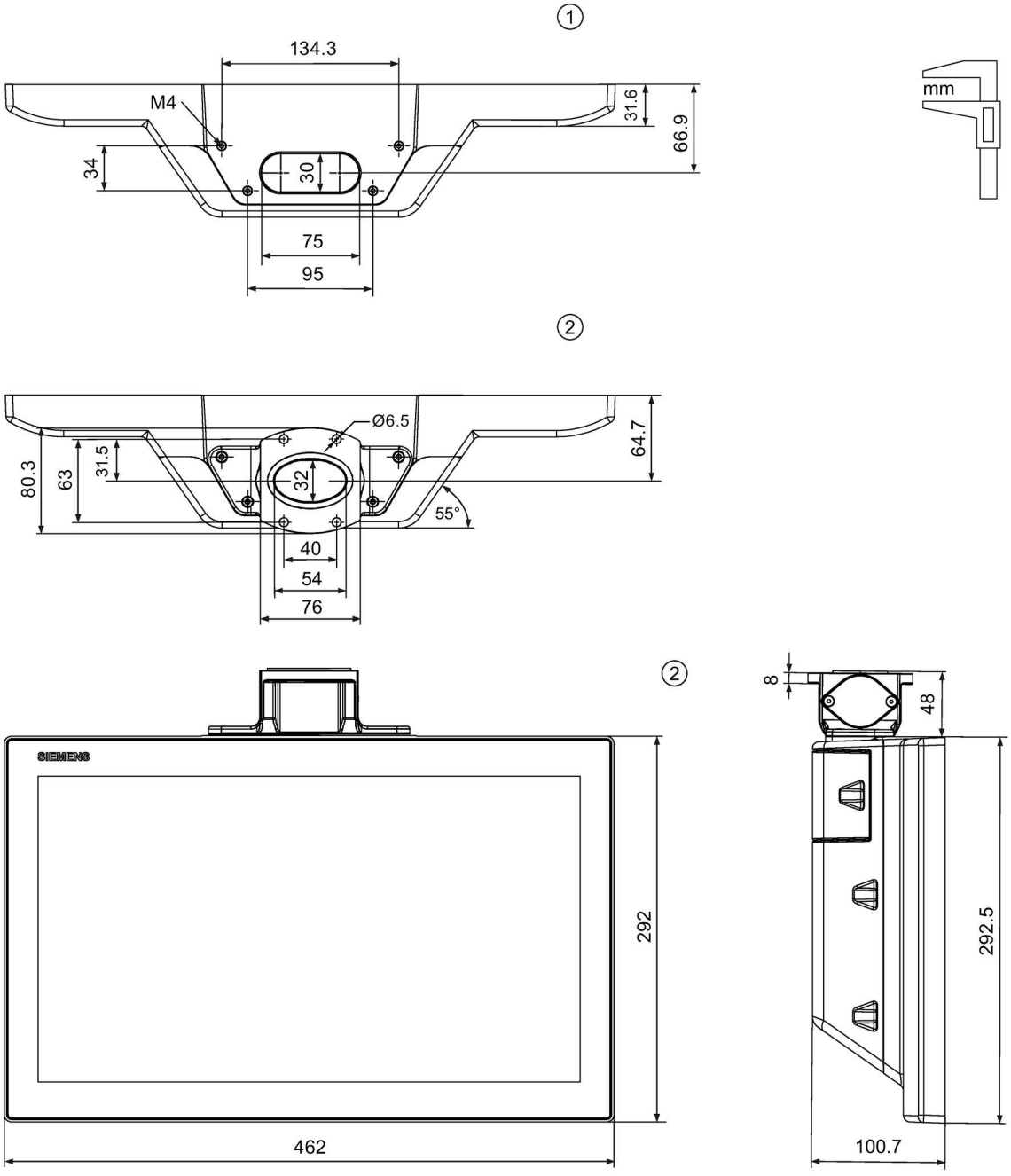
ITC1900 V3 PRO for pedestal (extendable, flange bottom)



① Without base adapter

② With base adapter

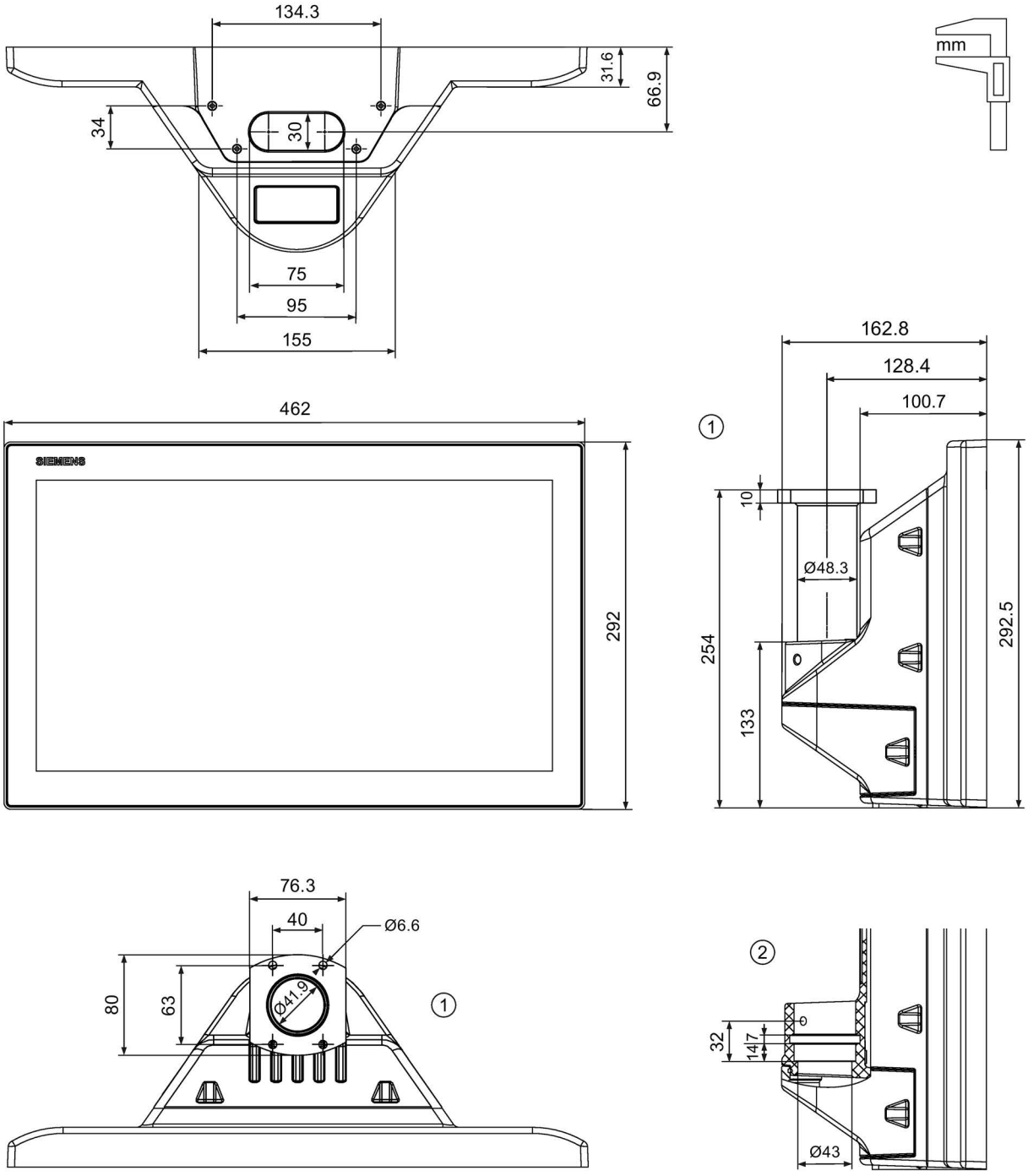
ITC1900 V3 PRO for support arm (not extendable, flange top)



① Without base adapter

② With base adapter

ITC1900 V3 PRO for support arm (extendable, round tube)

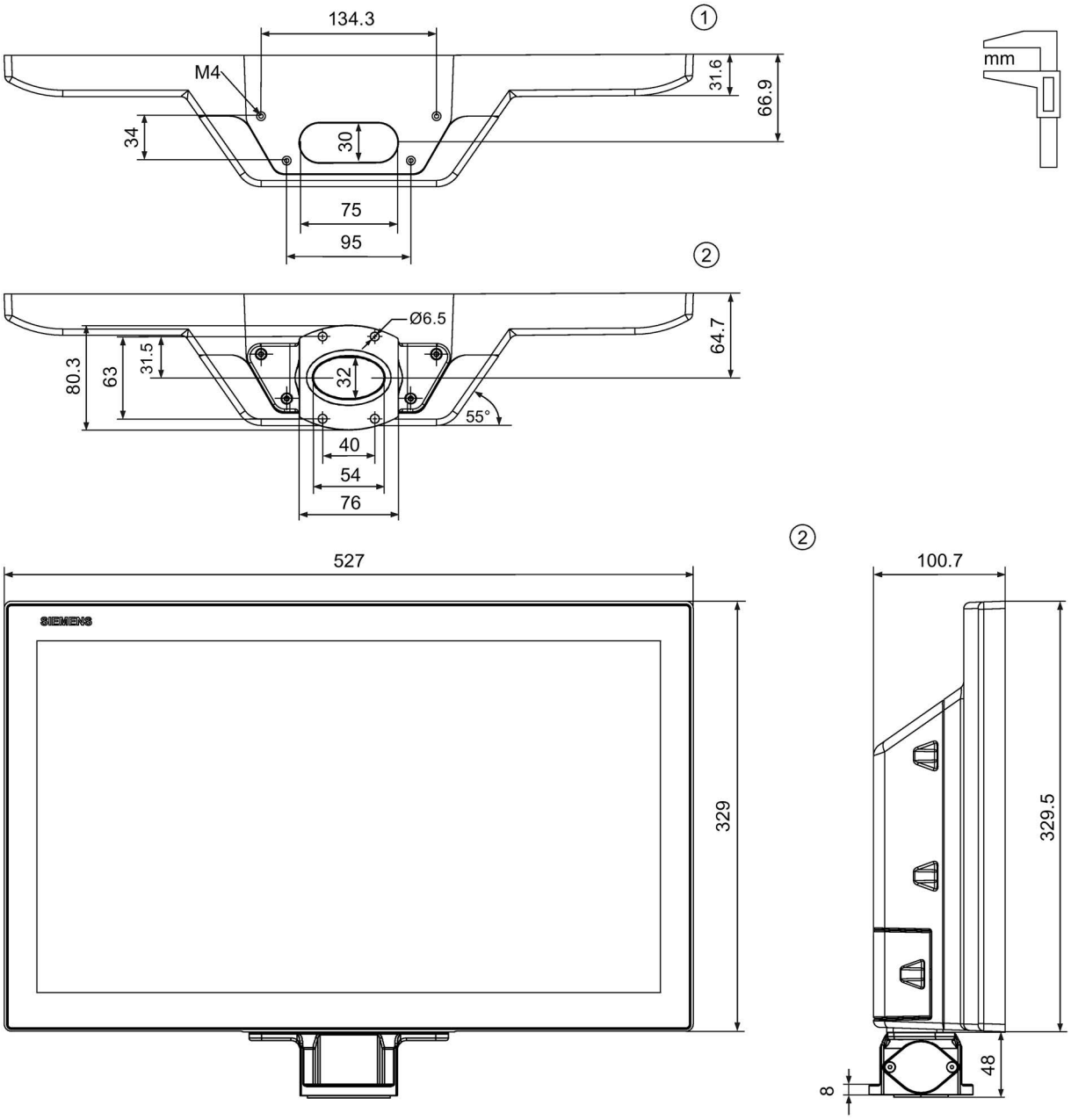


① with flange mount adapter

② without flange mount adapter

8.6.9 ITC2200 V3 PRO

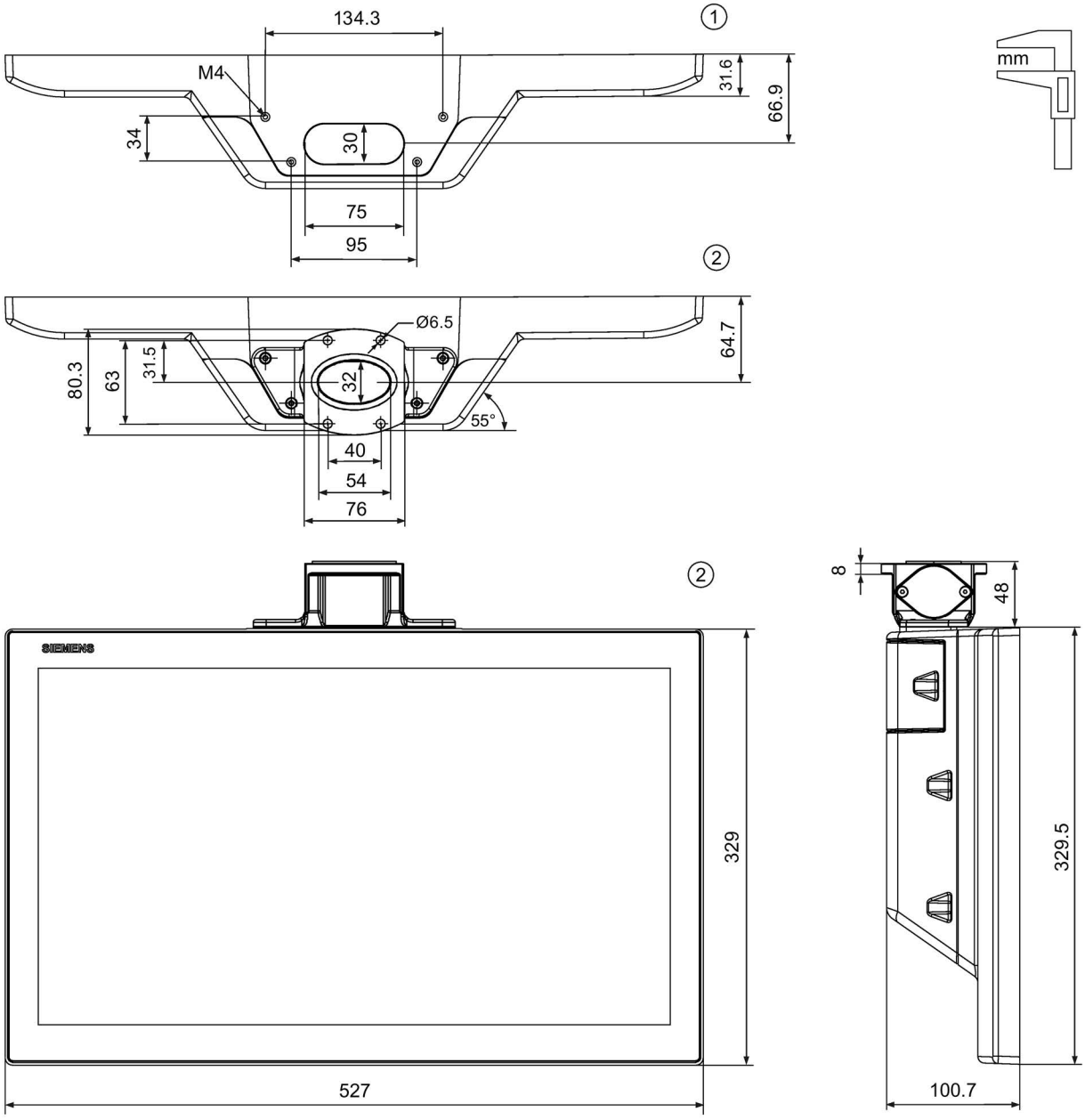
ITC2200 V3 PRO for pedestal (extendable, flange bottom)



① Without base adapter

② With base adapter

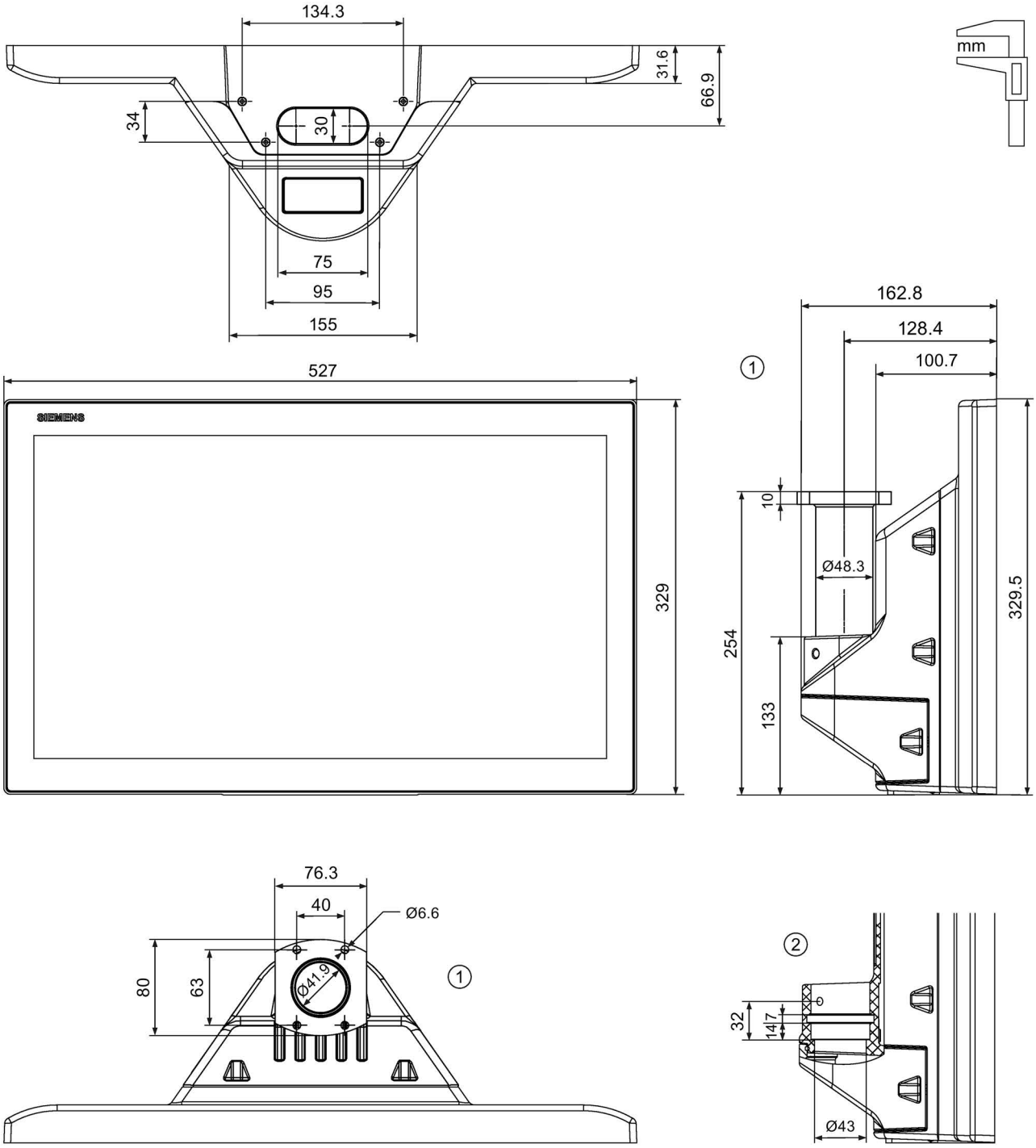
ITC2200 V3 PRO for support arm (not extendable, flange top)



① Without base adapter

② With base adapter

ITC2200 V3 PRO for support arm (extendable, round tube)

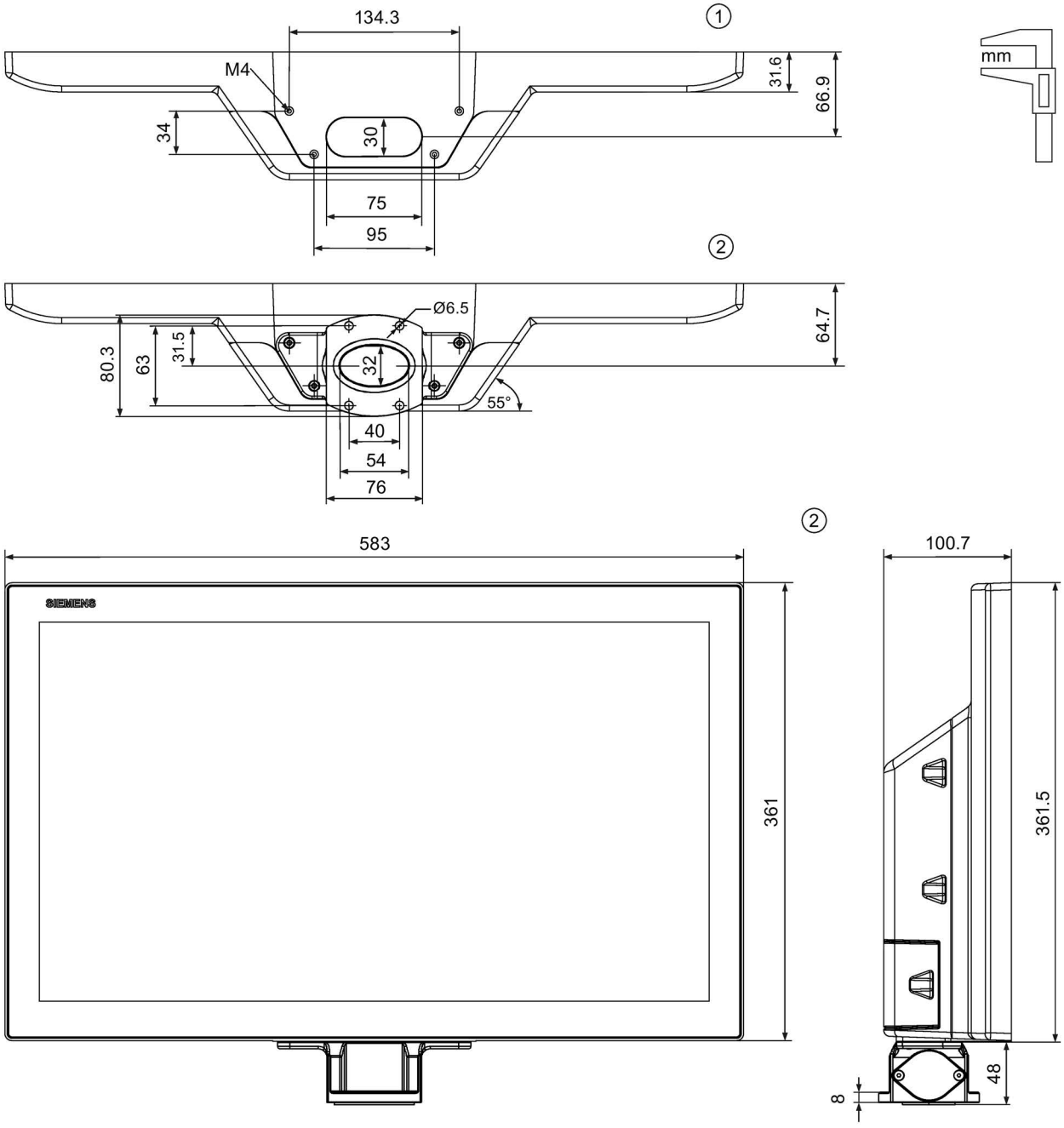


① with flange mount adapter

② without flange mount adapter

8.6.10 ITC2400 V3 PRO

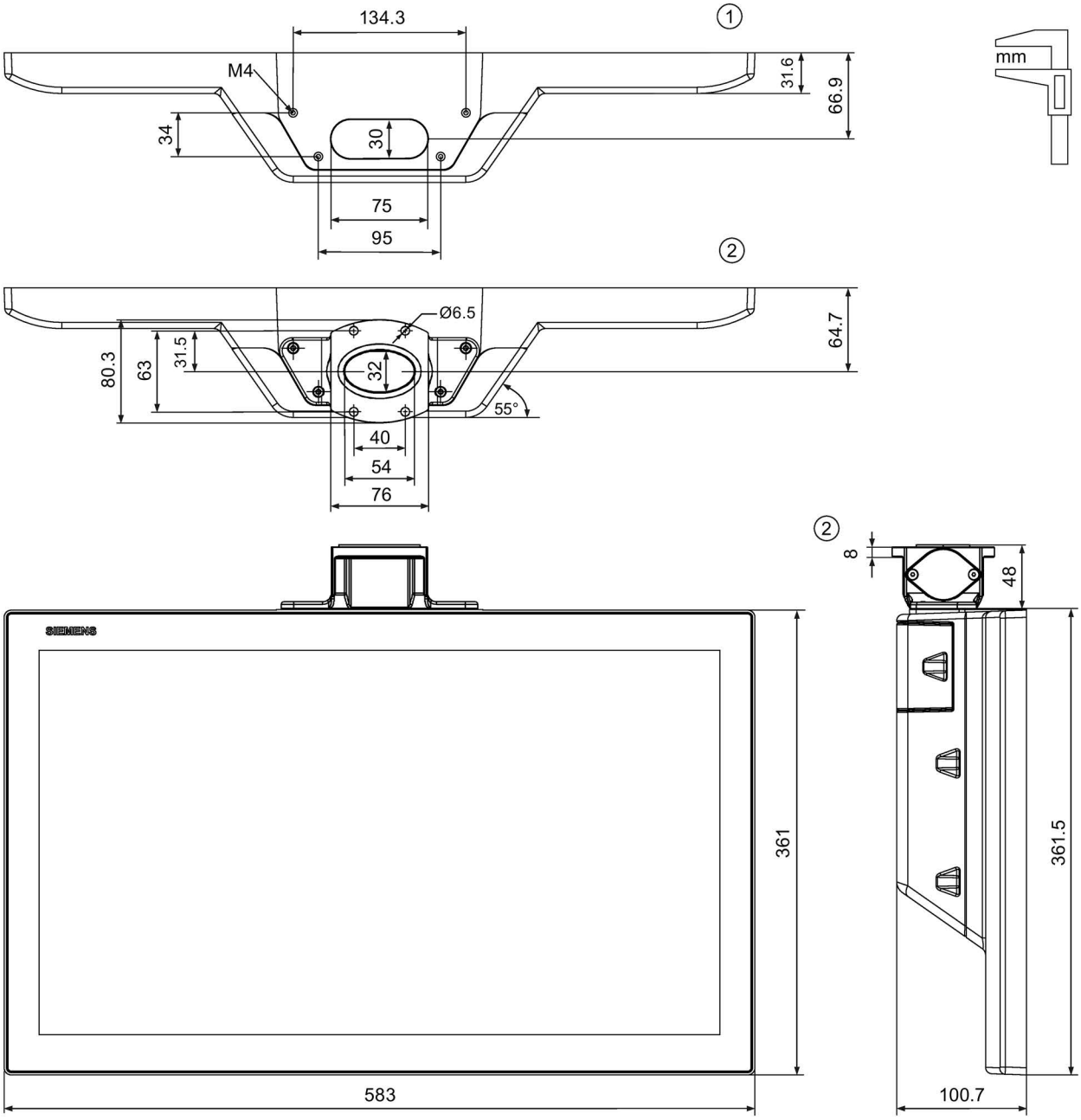
ITC2400 V3 PRO for pedestal (extendable, flange bottom)



① Without base adapter

② With base adapter

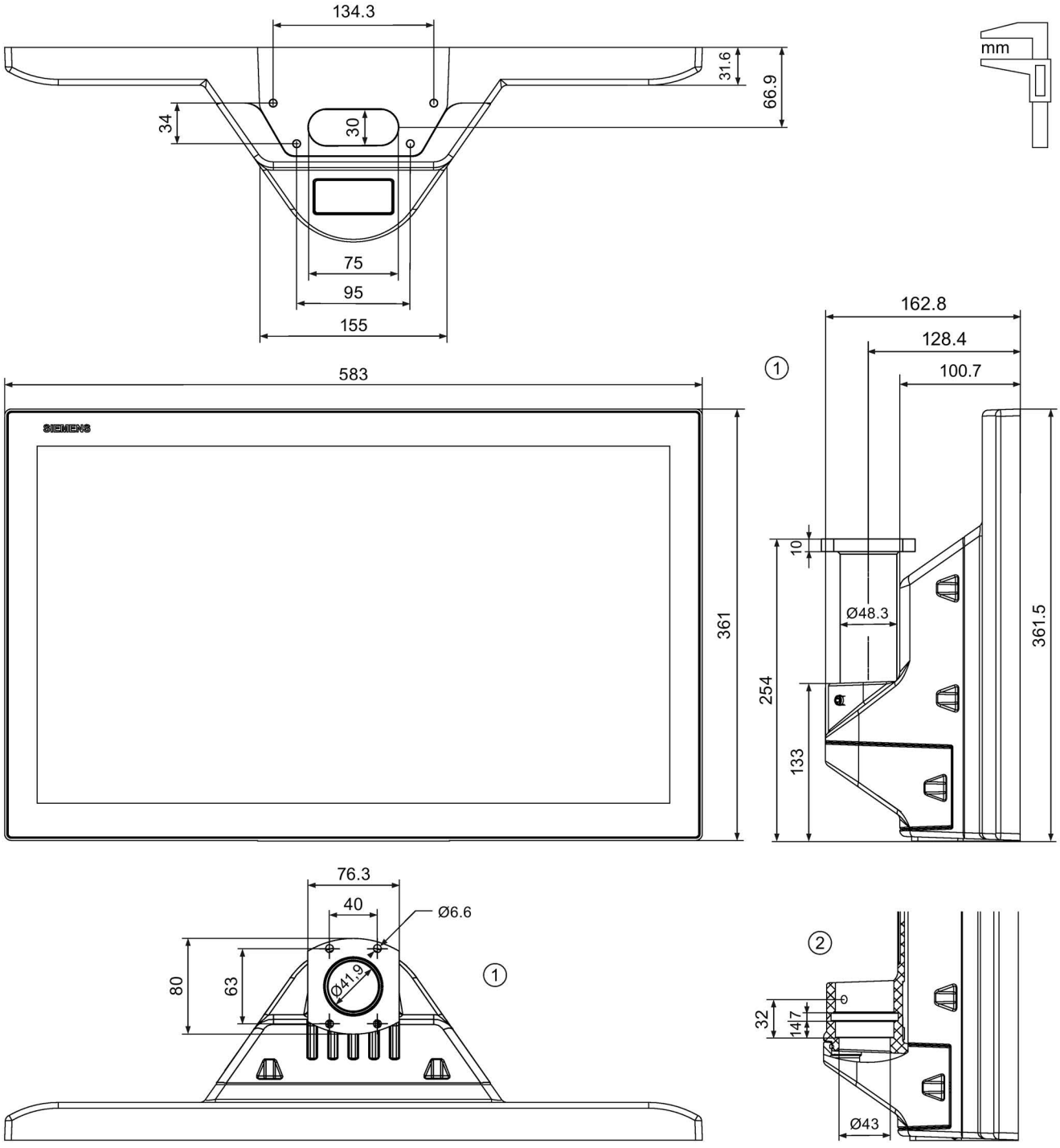
ITC2400 V3 PRO for support arm (not extendable, flange top)



① Without base adapter

② With base adapter

ITC2400 V3 PRO for support arm (extendable, round tube)



① with flange mount adapter

② without flange mount adapter

8.7 Technical specifications

8.7.1 ITC1200/1500 V3 (PRO)

Weight

	ITC1200 V3	ITC1500 V3
Weight without packaging, with power supply plug, mounting clips and strain relief plate	3.7 kg	5.0 kg

Weight of PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom)

	ITC1200 V3 PRO	ITC1500 V3 PRO
Weight without packaging	5.0 kg	6.3 kg

Weight of PRO devices for support arm (extendable, round tube)

	ITC1200 V3 PRO	ITC1500 V3 PRO
Weight without packaging	4.9 kg	6.2 kg

Display

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
Type	LCD TFT	
Display diagonal	12.1"	15.6"
Active display area	261 x 163 mm	344.2 x 193.5 mm
Resolution HD devices	1280 x 800 pixels	1366 x 768 pixels
Resolution Full HD devices	-	1920 x 1080 pixels
Possible colors	Up to 16 million	
Brightness control	Yes, value range 1 to 100	
Backlighting	LED	
Half Brightness Life time (MTBF 1)	50000 h	
Pixel error class in accordance with ISO 9241-307	I	

[1] MTBF: Operating hours after which the maximum brightness is reduced by half compared to the original value. The MTBF increases with reduced brightness or with the use of a screen saver on the server.

Input device

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
Touch screen	Yes, projective-capacitive	

Memory

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
RAM	2 GB DDR3 SDRAM	
Memory	8 GB SSD	

Interfaces

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
X1 P1 PROFINET (LAN)	1 x RJ45 Gigabit Ethernet, 10/100/1000 Mbps [1]	
X1 P2 LAN	1 x RJ45 Gigabit Ethernet, 10/100/1000 Mbps [1]	
X61 ... X64 USB 2.0	4 x Host [2]	

[1] With integrated switch (one IP address only), switch functionality only via LAN
[2] USB type A, maximum load 500 mA, equivalent to USB standard 2.0

Power supply

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
Rated voltage	24 V DC	
Permitted voltage range	+19.2 V to +28.8 V	
Voltage failure buffering time	20 ms, complies with PS2 according to IEC 61131-2	
Rated current	1.3 A	1.8 A
Rated current (min. ... max.), load-dependent	1.1 ... 1.6 A	1.5 ... 2.2 A
Inrush current I^2t	0.5 A^2s	
Power consumption [1]	31.2 W	43.2 W
Maximum permitted transient	35 V (500 ms)	
Minimum time between two transients	50 s	
Internal protection	Yes	

[1] The power loss generally corresponds to the specified value for power consumption.

Miscellaneous

	ITC1200 V3 (PRO)	ITC1500 V3 (PRO)
Audio reproduction	Via onboard beeper	

8.7.2 ITC1900/2200/2400 V3 (PRO)

Weight

	ITC1900 V3	ITC2200 V3	ITC2400 V3
Weight without packaging, with power supply plug, mounting clips and strain relief plate	6.1 kg	7.2 kg	8.7 kg

Weight of PRO devices for support arm (not extendable, flange top) and for pedestal (extendable, flange bottom)

	ITC1900 V3 PRO	ITC2200 V3 PRO	ITC2400 V3 PRO
Weight without packaging	7.4 kg	8.5 kg	10.1 kg

Weight of PRO devices for support arm (extendable, round tube)

	ITC1900 V3 PRO	ITC2200 V3 PRO	ITC2400 V3 PRO
Weight without packaging	7.2 kg	8.1 kg	10.0 kg

Display

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
Type	LCD TFT		
Display diagonal	18.5"	21.5"	23.8"
Active display area	409.0 x 230.0 mm	476.0 x 267.8 mm	527.0 x 296.5 mm
Resolution HD devices	1366 x 768 pixels	-	-
Resolution Full HD devices	1920 x 1080 pixels	1920 x 1080 pixels	1920 x 1080 pixels
Possible colors	Up to 16 million		
Brightness control	Yes, value range 1 to 100		
Backlighting	LED		
Half Brightness Life time (MTBF 1)	50000 h	30000 h	30000 h
Pixel error class in accordance with ISO 9241-307	I		

[1] MTBF: Operating hours after which the maximum brightness is reduced by half compared to the original value. The MTBF increases with reduced brightness or with the use of a screen saver on the server.

Input device

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
Touch screen	Yes, projective-capacitive		

Memory

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
RAM	2 GB DDR3 SDRAM		
Memory	8 GB SSD		

Interfaces

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
X1 P1 PROFINET (LAN)	1 x RJ45 Gigabit Ethernet, 10/100/1000 Mbps [1]		
X1 P2 LAN	1 x RJ45 Gigabit Ethernet, 10/100/1000 Mbps [1]		
X61 ... X64 USB 2.0	4 x Host [2]		

[1] With integrated switch (one IP address only), switch functionality only via LAN
[2] USB type A, maximum load 500 mA, equivalent to USB standard 2.0

Power supply

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
Rated voltage	24 V DC		
Permitted voltage range	+19.2 V to +28.8 V		
Voltage failure buffering time	20 ms, complies with PS2 according to IEC 61131-2		
Rated current	1.8 A	1.7 A	2.1 A
Rated current (min. ... max.), load-dependent	1.5 ... 2.2 A	1.4 ... 2.1 A	1.7 ... 2.6 A
Inrush current I^2t	0.5 A^2s		
Power consumption [1]	43.2 W	40.8 W	50.4 W
Maximum permitted transient	35 V (500 ms)		
Minimum time between two transients	50 s		
Internal protection	Yes		

[1] The power loss generally corresponds to the specified value for power consumption.

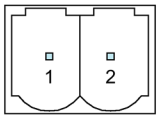
Miscellaneous

	ITC1900 V3 (PRO)	ITC2200 V3 (PRO)	ITC2400 V3 (PRO)
Audio reproduction	Via onboard beeper		

8.8 Description of the ports

8.8.1 Power supply

Plug connector, 2-pin



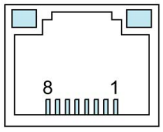
The following table shows the pin assignment of the power supply.

Pin	Assignment
1	+24 VDC
2	GND 24 V

8.8.2 PROFINET (LAN), LAN - 10/100/1000 MBit

Names of interfaces on HMI device: X1 P1 and X1 P2

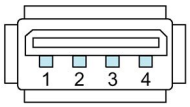
RJ45 plug connector



Pin	Assignment
1	D1+
2	D1–
3	D2+
4	D3+
5	D3-
6	D2-
7	D4+
8	D4-

8.8.3 USB

USB socket



The following table shows the pin assignment of the USB port.

Pin	Assignment
1	+5 VDC, out, max. 500 mA
2	USB-DN
3	USB-DP
4	GND

8.9 Performance data

Performance values

The performance depends on the network capacity in your system. With the SIMATIC WinCC Sm@rtServer option, the performance varies within the values specified in the WinCC documentation.

See also

FAQ 25576569 (http://support.automation.siemens.com/WW/view/en/25576569)

Technical Support

A

A.1 Service and support

You can find additional information and support for the products described on the Internet at the following addresses:

- Technical support (https://support.industry.siemens.com)
- Support request form (https://www.siemens.com/supportrequest)
- After Sales Information System SIMATIC IPC/PG (https://www.siemens.com/asis)
- SIMATIC Documentation Collection (https://www.siemens.com/simatic-tech-doku-portal)
- Your local representative (https://www.automation.siemens.com/aspa_app)
- Training center (https://siemens.com/sitrain)
- Industry Mall (https://mall.industry.siemens.com)

When contacting your local representative or Technical Support, please have the following information at hand:

- MLFB of the device
- BIOS version for industrial PC or image version of the device
- Other installed hardware
- Other installed software

Current documentation

Always use the current documentation available for your product. You can find the latest edition of this manual and other important documents by entering the article number of your device on the Internet (https://support.industry.siemens.com). If necessary, filter the comments for the entry type "Manual".

Printed documentation

If you require a hard copy of the operating instructions, contact Technical Support (https://support.industry.siemens.com).

Tools & downloads

Please check regularly if updates and hotfixes are available for download to your device. The download area is available on the Internet at the following link:

After Sales Information System SIMATIC IPC/PG (https://www.siemens.com/asis)

A.2 Application examples and FAQs

Application examples

You can find an application example for the "ITC" operating mode on the Internet at the following address: Configuration examples ITC (https://support.industry.siemens.com/cs/ww/en/view/109758315)

You can find additional application examples on the Internet at the following address: Thin Clients application examples (https://support.industry.siemens.com/cs/ww/en/ps/16794/ae)

FAQs

You can find frequently asked questions on Industrial Thin Clients on the Internet at the following address: FAQs ITC (https://support.industry.siemens.com/cs/ww/en/ps/16797/faq)

Markings and symbols

B

B.1 Safety-relevant symbols

The following table describes symbols that can be added to your SIMATIC device, to its packaging or to an enclosed document in addition to the symbols described in the manuals.

Symbol	Meaning	Reference
	General danger sign Caution / Attention You must following the operating instructions. The operating instructions contain information on the type of the potential hazard and enable you to identify risks and implement countermeasures.	ISO 7000 No. 0434B, DIN ISO 7000 No. 0434B
ONLY EX MODULES	Attention, only relevant for modules with Ex approval	
	Follow the instructions	ISO 7010 M002
	May be installed by qualified electricians only	IEC 60417 No. 6182
F<2N DISPLAY F<4N HOUSING	Mechanical load for HMI devices	
CABLE SPEC.	Connection cables must be designed for the ambient temperature	
EMC	EMC-compliant installation	
U = 0V	No mounting or pulling & plugging under voltage	
230V MODULES	Dangerous electrical voltage for 230V modules	ANSI Z535.2
24V MODULES	Protection class III, supply only with protective low voltage (SELV/PELV)	IEC 60417-1-5180 "Class III equipment"

Symbol	Meaning	Reference
INDOOR USE ONLY INDUSTRIAL USE ONLY	Only for industrial applications and indoor areas (control cabinet)	
	Device is to be integrated or installed in a control cabinet	
ZONE 2 USE CABINET IP54	Integrate or install devices approved for Ex Zone 2 in a control cabinet with at least IP54	
ZONE 22 USE CABINET IP6x	Integrate or install devices approved for Ex Zone 22 in a control cabinet with at least IP6x	

Abbreviations

C

CAL	Client Access License (Windows Server)
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DIP	Dual In-Line Package
DNS	Domain Name System
DP	Distributed I/O
ESD	Components and modules endangered by electrostatic discharge
EKS	Electronic Key System
EMC	Electromagnetic Compatibility
EN	European standard
FAT	File Allocation Table
GND	Ground
HF	High Frequency
HMI	Human Machine Interface
HT	Handheld Terminal
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HSK	Horizontal Soft Key
IEC	International Electronic Commission
IP	Internet Protocol
IPC	Industrial Personal Computer
MAC	Media Access Control
MCP	Machine Control Panel
MPI	Multipoint Interface (SIMATIC S7)
MPP	Machine Push Button Panel
MS	Microsoft
MSDN	Microsoft Developer Network
NCK	Numerical Control Kernel
NCU	Numerical Control Unit
NTFS	New Technology File System
OP	Operator Panel
PC	Personal Computer
PCU	Panel Control Unit
PG	Programming device
PLC	Programmable Logic Controller
PPI	Point-to-Point Interface (SIMATIC S7)
PELV	Protective Extra Low Voltage
PN	PROFINET
RDP	Remote Desktop Protocol
RJ45	Registered Jack Type 45

SNC	System Network Center
TCU	Thin Client Unit
TFT	Thin Film Transistor
TFTP	Trivial File Transfer Protocol
TOP	Thin Client Operator Panel
TP	Touch Panel
TS-CAL	Terminal Server Client Access License (Windows Server)
UL	Underwriter's Laboratory
USB	Universal Serial Bus
VNC	Virtual Network Computing
VSK	Vertical Soft Key

Glossary

Browser

A browser is a computer program that is used to start Web sites in the Internet.

Client-server system

A client/server system is a network structure in which the resources are offered by a central server that the workstations (clients) can access.

Degree of protection

The degree of protection specifies the suitability of electronic equipment for a variety of ambient conditions – and the protection of persons against potential danger when using this equipment.

The degree of protection specified by IP differs from the protection class. But both involve protection against touching dangerous electric voltage. The degree of protection also classifies the protection of equipment against dirt and moisture.

Domain Name System (DNS)

The DNS is a service in the Internet that converts domain names into IP addresses.

Dynamic Host Configuration Protocol (DHCP)

DHCP enables dynamic assignment of an IP address and additional configuration parameters to computers in a network, via an appropriate server.

Electromagnetic Compatibility (EMC)

Electromagnetic compatibility (EMC) refers to a usually desirable state, in which technical equipment does not disturb one another with unwanted electrical or electromagnetic effects. Electromagnetic compatibility deals with technical and regulatory questions of undesired, mutual influence in electrical engineering.

EMC

Electromagnetic compatibility is the ability of electrical equipment to function properly in its electromagnetic environment without influencing this environment.

Ethernet

Ethernet is a fixed-cable data network technology for local area networks (LANs). Ethernet enables data transfer in the form of data frames between all devices that are connected in a local area network, for example, computers, printers.

HMI device

An HMI device is a device used for the operation and monitoring of machines and plants. The statuses of the machine or plant are indicated by means of graphic elements or by indicator lamps on the HMI device. The operator controls of the HMI device allow the operator to interact with the processes of the machine or plant.

Plant

General term referring to machines, processing centers, systems, plants and processes which are operated and monitored on an HMI device.

PLC

A PLC is a general term for devices and systems with which the HMI device communicates, for example, SIMATIC S7.

Process visualization

Visualization of technical processes by means of text and graphic elements. Configured plant screens allow operator intervention in active plant processes by means of the input and output data.

PROFINET

PROFINET is a standard for an industrial Ethernet in automation systems.

Project

Result of a configuration using a configuration software. The project normally contains several screens with embedded system-specific objects, basic settings and alarms. The project is transferred to an HMI device and monitored and operated with the HMI device.

Protection class

The protection class is used in electrical engineering to classify and identify electrical equipment in relation to existing safety measures designed to prevent electric shock. There are three protection classes for electrical equipment.

Remote Desktop Protocol (RDP)

RDP enables network access to applications that are executed on a Windows Terminal Server. In this process the RDP regulates transmission of screen content and keyboard and mouse inputs over the network.

Screen

Form of the visualization of all logically related process data for a plant. The visualization of the process data can be supported by graphic objects.

Sm@rtServer

The Sm@rtServer option from SIMATIC WinCC (TIA Portal) enables communication between HMI systems based on Ethernet networks or via the Intranet/Internet. This enables an HMI device to be monitored and remotely controlled by another HMI device.

Virtual Network Computing (VNC)

VNC enables network access to applications that are executed on a remote computer regardless of the platform. In this process the VNC controls transmission of screen content and keyboard and mouse inputs over the network.