SYSTEM MANUAL

SENTRON

Digitalization solutions

Circuit protection devices with communication and metering function

siemens.com/lowvoltage

SIEMENS

SIEMENS

SENTRON

Circuit protection devices with communication and metering function

System Manual

09/2025

L1V30827018B_RS-AB_008

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
Smart Infrastructure
Electrical Products
Postfach 10 09 53
93009 Regensburg
GERMANY

℗ 10/2025 Subject to change

Table of contents

Introduction

1

Note

This document refers to firmware version V7.1 of the system.

1.1 Reference documents

You can find more information in the following documents:

Title	Article number
Circuit protection devices with communication and measuring function Installation Instructions (https://support.industry.siemens.com/cs/ww/en/view/109791805)	L1V30827020A
SENTRON Powercenter 1000 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109793297)	L1V30610178A
5ST3 COM auxiliary switch and fault signal contact Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109793296)	3338214103
5SL6 COM miniature circuit breaker Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109793301)	3355484128
RCM&EM 5SL6 COM miniature circuit breaker Operating Instructions (https://support.industry.siemens.com/cs/de/de/view/109814723)	3355484120
5SV6 COM arc fault detection device Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109793300)	3355484127
3NA COM electronic module Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109793298)	2568024102
SENTRON Powercenter 3000 Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109763838)	L1V30579222004
3RV2 COM wireless auxiliary and signaling switch for 3RV2 motor starter protectors Operating Instructions (https://support.industry.siemens.com/cs/de/de/view/109817772)	A5E51924610001A
5TY1 COM ECPD electronic circuit protection device Operating Instructions (https://support.industry.siemens.com/cs/si/en/view/109827430)	L1V30912073A
SENTRON Powercenter 1100 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109973382)	L1V30972515001A

Title	Article number
5SV8 COM RCM residual current monitor Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109973379)	L1V30940519A
5SV8 COM MRCD modular residual current device Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109973380)	L1V30940523A
5SV8 residual current measuring devices and modular residual current protection devices Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109975845)	A5W02378652A
SENTRON Powercenter 2000 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109990979)	A5W02680366A
5TT4 COM digital input/output module Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109990980)	A5W02664028A

1.2 Technical Support

You can find further support on the Internet at:

TechnicalSupport (https://www.siemens.com/support-request)

1.3 Advanced training courses

Find out about regional training courses on offer via the following link.

Training for Industry (https://www.siemens.com/sitrain-lowvoltage)

Here you can choose from:

- Web-based training courses (online, informative, free)
- Classroom training courses (course attendance, comprehensive, subject to fee)

If the correct training course is not shown, you can also get information from your local sales representative.

Safety instructions

2

2.1 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/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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 at (https://www.siemens.com/cert):

2.2 Open Source Software

This product, solution or service ("Product") contains third-party software components. These components are Open Source Software licensed under a license approved by the Open Source Initiative (https://www.opensource.org) or similar licenses as determined by SIEMENS ("OSS") and/or commercial or freeware software components. With respect to the OSS components, the applicable OSS license conditions prevail over any other terms and conditions covering the Product. The OSS portions of this Product are provided royalty-free and can be used at no charge.

If SIEMENS has combined or linked certain components of the Product with/to OSS components licensed under the GNU LGPL version 2 or later as per the definition of the applicable license, and if use of the corresponding object file is not unrestricted ("LGPL Licensed Module", whereas the LGPL Licensed Module and the components that the LGPL Licensed Module is combined with or linked to is the "Combined Product"), the following additional rights apply, if the relevant LGPL license criteria are met: (i) you are entitled to modify the Combined Product for your own use, including but not limited to the right to modify the Combined Product to relink modified versions of the LGPL Licensed Module, and (ii) you may reverse-engineer the Combined Product, but only to debug your modifications. The modification right does not include the right to distribute such modifications and you shall maintain in confidence any information resulting from such reverse-engineering of a Combined Product.

Certain OSS licenses require SIEMENS to make source code available, for example, the GNU General Public License, the GNU Lesser General Public License and the Mozilla Public License. If such licenses are applicable and this Product is not shipped with the required source code, a copy of this source code can be obtained by anyone in receipt of this information during the period required by the applicable OSS licenses by contacting the following address:

Siemens AG
Smart Infrastructure
Electrical Products
Technical Support
Postfach 10 09 53
93009 Regensburg
Germany

You will find Technical Support under (https://www.siemens.com/support-request).

Keyword: Open Source Request (please specify Product name and version, if applicable)

SIEMENS may charge a handling fee of up to 5 EUR to fulfil the request.

Warranty regarding further use of the Open Source Software

SIEMENS' warranty obligations are set forth in your agreement with SIEMENS. SIEMENS does not provide any warranty or technical support for this Product or any OSS components contained in it if they are modified or used in any manner not specified by SIEMENS. The license conditions may contain disclaimers that apply between you and the respective licensor. For the avoidance of doubt, SIEMENS does not make any warranty commitment on behalf of or binding upon any third-party licensor. The Open Source Software used in the product and the license agreements concerning this software can be found in the Readme_OSS.

2.3 User policy for mobile devices

Tips for customers using mobile devices

A wide range of applications can be installed on mobile devices. A certain cybersecurity risk is associated with the use of these devices. The following information will allow the user to use the apps with the highest possible degree of cybersecurity.

What can go wrong?

The use of mobile devices increases the risk of data loss and data theft in different ways. Typical situations include:

- Loss or theft of devices, e.g. in the hotel room, on the airplane, in a rental car or taxi, in the conference room, in the lobby or during breaks.
- Leaving the mobile device in unsuitable hands. If children are allowed to play with the device, they can inadvertently perform operations or change configuration settings.
- Reading information off the screen or eavesdropping on conversations. When you are in public, you should be conscious of the fact that other people can be watching you or listening to you, thereby obtaining information which could damage your company, your customers, your business partners or colleagues.

How can I stay cybersecure?

- Use a virtualization software to separate private and business affairs in your mobile device.
- Activate security mechanisms, such as the PIN for your tablet, smartphone or mobile phone and the password for your laptop.
- Use passwords that cannot easily be guessed to protect your mobile device.
- When entering passwords, make sure that nobody is watching.
- Keep the operating system and the installed applications up to date.
- Mobile devices must be protected against malware and other threats. For this reason, no unnecessary apps and no apps from unknown origins should be installed. A malware scanner should also be installed if possible.
- Lock your mobile device as soon as you have finished using it.
- Every time you install an app, make sure to check which permissions the app requires. For example, a flashlight function does not require access to the internet or your contacts. Never use unprotected internet access, such as WLAN hotspots in airport lounges, hotels, conference centers, restaurants or cafés.
- It is imperative that you use a VPN solution every time you set up a connection to the World Wide Web.
- If possible, set up device tracking for your mobile device so that it can be found, or even locked, if it gets lost. This function varies from one mobile device to the other.
- Do you know your service provider's emergency number? You can ask your provider to lock your device or perform a remote wipe in the event of an emergency.

- Deactivate all unnecessary functions. If you do not need GPS tracking, for example, you can deactivate this function.
- Back up your data regularly. Save your backup to another safe place.
- Employees must be conscious of their responsibilities when it comes to cybersecurity. Cybersecurity training courses are advisable for this reason.

2.4 Five safety rules for work in or on electrical installations

A set of rules, which are summarized in DIN VDE 0105 as the "five safety rules", are defined for working in or on electrical systems as a preventative measure against electrical accidents:

1. Isolate
2. Secure against reclosing
3. Verify absence of operating voltage
4. Ground and short-circuit
5. Provide protection against adjacent live parts

These five safety rules must be applied in the above order prior to starting work on an electrical system. After completing the work, proceed in the reverse order.

It is assumed that every electrically skilled person is familiar with these rules.

Explanations

1. The isolating distances between live and de-energized parts of the system must vary according to the operating voltage that is applied.
   "Isolate" refers to the all-pole disconnection of live parts.
2. The feeder must be locked against inadvertent reconnection to ensure that it remains isolated for the duration of the work. This can be achieved, for instance, by locking the motor and system circuit breakers in the OFF position or by unscrewing the fuses and using lockable elements to prevent them from being reinserted.
3. The de-energized state of the equipment should be verified using suitable test equipment, e.g. a 2-pole voltmeter. 1-pole test pins are not suitable for this purpose. The absence of power must be established for all poles, phase to phase, and phase to N/PE.
4. Grounding and short-circuiting are only mandatory if the system has a rated voltage greater than 1 kV. In this case, the system should always be grounded first and then connected to the live parts to be short-circuited.
5. These parts should be covered, or barriers erected around them, to avoid accidental contact during the work with adjacent parts that are still live.

Circuit protection devices with communication and measurement function and monitoring devices with communication function

3

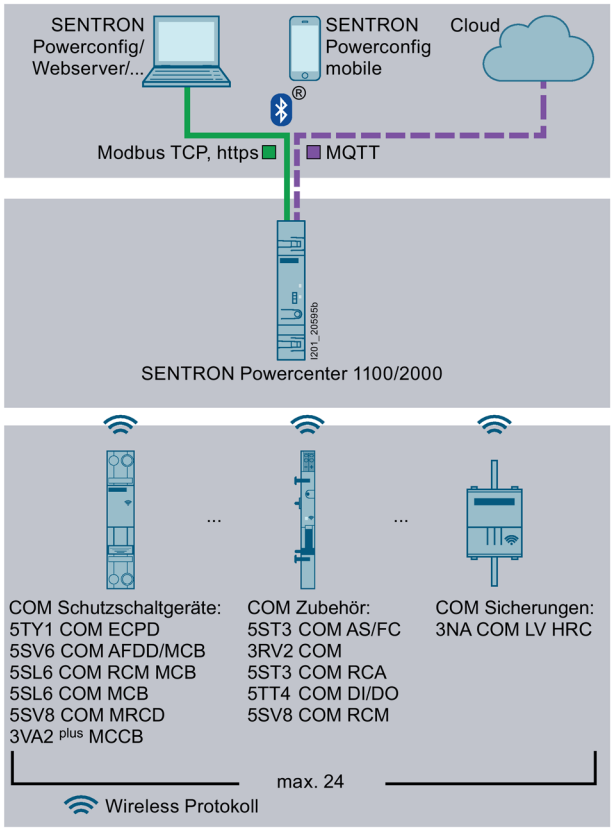
The SENTRON COM circuit protection devices with communication and measuring functions are an integral part of SENTRON digitalization solutions.

System availability is increased by the early response to warning messages. The protection functions still offer secure, reliable protection in the final circuit. As a result, the communication and measuring function makes it easier to find the causes during malfunctions due to reporting the cause of the tripping operation, which in turn allows conclusions to be drawn about malfunctions of operating equipment. Another advantage is provided by the integrated operating hour and trip counters, which contribute to improved planning of maintenance work. In addition, circuit protection devices with measurement and communication function capture electrical parameters such as energy, active power, current, voltage, line frequency and temperature. This helps increase transparency and energy consumption in the final circuits can be broken down. By setting alarm threshold values and additionally measuring residual currents in several frequency ranges, it is possible to pinpoint the causes of errors.

Due to their compact construction, the circuit protection devices are ideal for the retrofit market or even new construction. The system can be simply put into operation via the SENTRON Powerconfig PC software or SENTRON Powerconfig mobile for mobile devices.

You can find more information in the Installation Manual - SENTRON circuit protection devices with communication and measuring function (https://support.industry.siemens.com/cs/de/en/view/109791805).

A SENTRON Powercenter 1000 or SENTRON Powercenter 1100 or SENTRON Powercenter 2000 data transceiver forms the core of the SENTRON COM system of communication-capable circuit protection devices. This acquires measured values of the paired circuit protection devices and transfers them to the higher-level systems. The measured values from up to 24 communication-capable SENTRON devices are wirelessly transferred to a SENTRON Powercenter 1000/1100/2000, which stores selected data for up to 30 days. Higher-level systems can access the data via the interfaces of the data transceiver. Either on site via Bluetooth® or via Ethernet in the local network. In this case, a Modbus TCP protocol is used, which can easily be integrated by other systems.



The system of circuit protection devices with communication and measuring function increases system availability due to increased transparency through to the final circuit through wireless transmission and storage of measured values.

Because the devices communicate via radio frequency, radio approval is required for each country in which they are operated.

Existing country radio approvals
(https://support.industry.siemens.com/cs/de/en/view/109801197)

Further countries on request.

3.1 SENTRON Powercenter data transceiver

3.1.1 SENTRON Powercenter 1000

The SENTRON Powercenter 1000 data transceivers gather data from communication- and measurement-capable 5SL6 COM miniature circuit breakers, 5SV6 COM arc fault detection devices, 5ST3 COM auxiliary switch and fault signal contacts, 3NA COM communication-capable fuses, 3RV2 COM wireless auxiliary and signaling switches for 3RV2 motor starter protectors, 5TY1 ECPD and 5SV8 residual current measuring devices.

They communicate wirelessly with up to 24 terminal devices within a switchgear bay or a distribution board. The recorded data can be accessed via Bluetooth® using a mobile terminal device on site or forwarded to higher-level systems by means of Modbus TCP. Selected measured values are stored in the SENTRON Powercenter 1000 for up to 30 days and can be displayed via the Ethernet interface.

Energy flows among other things can be visualized and optimized with the SENTRON Powermanager energy monitoring system. Via the SENTRON Powercenter 3000 IoT data platform, the recorded data can be viewed directly in a web interface or transferred to Cloud applications and evaluated.

The screwless plug-in terminals allow the 24 V DC (SELV) power supply to be looped through to other devices in the distribution board, and with its 1TE size, the space-saving SENTRON Powercenter 1000 enables easy mounting on the DIN rail.

3.1.2 SENTRON Powercenter 1100

The SENTRON Powercenter 1100 can be used as a newer alternative to the SENTRON Powercenter 1000. Other terminal devices with firmware > V4.0, such as the 5TY1 COM ECPD or 5SV8 COM RCM, can be connected in addition to the terminal devices mentioned above (5SL6 COM MCB, 5SV6 COM AFDD, 5ST3 COM AS+FC, 5ST3 COM RCA, 3RV2 COM MSP).

The up to 24 terminal devices are connected in the usual way via a wireless protocol. The data can be retrieved either on site via Bluetooth® or from the local network using Modbus TCP. The 1TE width and 24 V DC power supply are also unchanged.

The following changes and new features apply only for the SENTRON Powercenter 1100:

- Support for terminal devices with firmware version < V4.0 and ≥ V4.0
- Two Ethernet connections with switch function
- Improved storage function for historic measured values from connected terminal devices
- Additional secure protocol https via REST-API
- Slide switch on front for activating write protection
- Role-based access control (RBAC): Login with username and password with assigned authorizations
- Product information accessible via QR code (ID link) on the front

3.1.3 SENTRON Powercenter 2000

Der SENTRON Powercenter 2000 data transceiver with cloud connectivity is based on the proven hardware of the SENTRON Powercenter 1100. All the same device functions are still available, such as the connection of 24 RF terminal devices, long-term data storage, Bluetooth® and Modbus TCP interfaces, the switch function of the Ethernet ports and advanced security requirements (write protection, RBAC, https via REST API).

Additional functions of the SENTRON Powercenter 2000 include:

- MQTT interface: Support for an MQTT protocol, enabling a native connection to different cloud services. This greatly simplifies the integration and automation in IoT environments. Advantages of cloud solutions include: Long-term data storage, data analyses, location-independent access, active alarm annunciation in the event of a fault, automatic report creation, and many more.
- Integrated web server: The integrated web server permits simple and direct access to the measured and status values of the system. The IP address of the SENTRON Powercenter 2000 simply needs to be entered into the web browser of the local network.

3.2 5ST3 COM auxiliary switch and fault signal contact

5ST3 COM auxiliary switches and fault signal contacts are ideal for retrofitting devices that are not available as communication-capable versions. They are mounted on to the electromechanical master unit and extended by communication and metering functions for temperature, switch position and the number of shutdowns.

In order to work in the most space-saving manner, the 5ST3 COM auxiliary switch and fault signal contact is a measurement and communication-capable add-on module, which only uses 0.5 TE. This can be mounted on to the series 5SY, 5SP4 and 5SL miniature circuit breakers and the 5SV residual current operated circuit breaker and 5SV1 and 5SU1 RCBO switches.

The supply voltage of 24 V DC (SELV) can be bridged to other devices via the screwless plug-in terminals.

3.3 5SL6 COM miniature circuit breaker

5SL6..MC (EM)

5SL6..MF (EM+RCM)

5SL6 COM miniature circuit breakers do not just protect final circuits such as conventional miniature circuit breakers during overload and short-circuits, they also acquire information about the status and the faults in the electrical circuit.

Measured values such as current, voltage, temperature, line frequency, power, energy, operating hours, tripping operations and operating cycles are communicated wirelessly to the higher-level SENTRON Powercenter 1000/1100/2000 data transceiver. Monitoring of the electric circuit enables predictive error detection by reporting pre-warnings if, for example, the set load current limit is exceeded.

In addition to the power measurement function and the condition monitoring function, the 5SL6 COM version with RCM function (5SL6..-.MF) enables the measurement and monitoring of residual currents in accordance with IEC 62020-1 (residual current monitoring, RCM for short). This involves simultaneously monitoring residual currents in several frequency ranges, and enables the differentiation of error statuses in the system.

The device only requires the external and N-conductor connection (230 V AC) and no additional power supply (24 V DC) for the communication and measuring function. With a width of 1 TE, the 5SL6 COM miniature circuit breaker is as large as conventional miniature circuit breakers without communications capability. The 5SL6 COM is designed for nominal currents of 2 ... 32 A and available in the tripping characteristics B and C.

3.4 5SV6 COM arc fault detection device

With the communication-capable 5SV6 COM arc fault detection device, which has the integrated function of a miniature circuit breaker, the affected final circuit can be protected with regard to overload, short-circuit and fault arcs.

The measured values and statuses are wirelessly transmitted via the integrated communication and metering function. Thus, the final circuit can be monitored even further, by e.g. setting a limit value that sends a warning when a certain current or voltage value is exceeded. This predictive error detection ensures increased system availability. In addition to the electrical measured values (current, voltage, frequency, power, energy) of the circuit, values such as tripping type, temperature, switching cycles or operating cycles are also communicated.

Even here, the 1+N pole design of the switch offers the complete scope of protection, without additional connections for the communication function. As a result of the compact size of 1 TE, the 5SV6 COM arc fault detection devices offer a simple replacement option for conventional arc fault detection devices or miniature circuit breakers. Devices with a compact structure (1+N) can be easily exchanged, for the single-pole devices the neutral conductor must also be connected. The 5SV6 COM is available for nominal currents of 6 A to 32 A and in tripping characteristics B and C.

3.5 3NA COM fuse

The 3NA COM fuses with communication and measuring function not only protect the circuit, but also enable early error detection by measuring the current and temperature.

Monitoring of the circuit makes it possible to combat the cause even before the fuse trips by being able to generate warning messages when the set over-current limit or even the temperature limit has been exceeded. This contributes towards the avoidance of power outages, or a reduction of power failures and thus, increases the availability.

The 3NA COM fuse is available in size NH2 and operating class gG or gFF. It can be easily retrofitted in the existing fuse-disconnector due to its standard-compliant dimensions and auxiliary power. The whole fuse module is composed of an electronic module and a fuse link with nominal currents between 80 ... 315 A. The fuse link can be easily replaced once the fuse has been tripped. It is not imperative to renew the electronic module, however, the functions should be checked after re-commissioning. A test must be performed with a suitable reference measuring instrument and the exchanged components must be documented in an appropriate manner (e.g. in the form of a test label and electronic recording).

The electronic module provides the communication and measuring function with an integrated instrument and supply transformer, where an additional connection for the supply voltage is not required. A min. current flow of 5 A is required in order to ensure the communication and measuring function (min. 10 A for a firmware update). Together with the fuse link, the electronic module forms the complete system of the 3NA COM fuse.

3.6 3RV2 COM wireless auxiliary and signaling switch for 3RV2 motor starter protectors

Wireless auxiliary switches and signaling switches are ideal for retrofitting motor starter protectors that are not available as communication-capable versions.

The devices (3RV2921-5M) can be mounted as an accessory on the electromechanical 3RV2 motor starter protector (size S00 - S3); the width is 18 mm.
The measured values and statuses of the basic unit are wirelessly transmitted via the integrated communication and measuring function. In this way, the temperature and the number of shutdowns are transmitted in addition to the switching statuses of the motor starter protector. Apart from the ON/OFF indication, a tripping operation is treated differently depending on whether it was caused by an overload or a short-circuit.

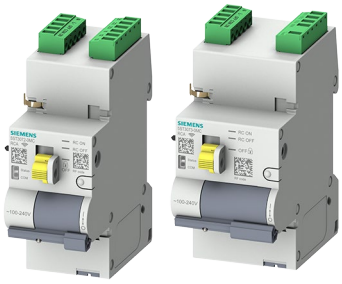
The supply voltage of 24 V DC (SELV) can be bridged to other devices via the screwless plug-in terminals. This device is supported in the Powercenter 1000 from firmware version 3.0.

3.7 5ST3 COM remote control auxiliary (RCA)

Note

Remote control auxiliary

(RCA)



5ST3 COM remote control auxiliaries not only enable monitoring of the system/the attached main devices, they also allow remote switching. These devices are supported in the Powercenter 1000 from firmware version 3.0.

Further functions are provided in addition to the standard measuring functions for device temperature, operating hours and the number of shutdowns, e.g. exact details of the switch position - manual, automatic or remote switching, or the switching command, an automatic reclosing function (ARD) after a tripping operation and its parameterization.

The RCD test version of the remote control auxiliary (5S3073-0MC) also allows one-off or cyclical FI (RCD) or insulation resistance (IR) tests to be performed in accordance with IEC 63024, depending on the configured mount-on device. The time and date and the test results are stored and can be exported later.

Instead of the test function, the standard version (5S3072-0MC) provides wired connections for auxiliary and fault signal contacts.

Both versions are supplied with 100-240 V AC line voltage.

3.8 5TY1 COM electronic circuit protection device (ECPD)

Note

Electronic circuit protection device

Electronic Circuit Protection Device = ECPD

The new concept underlying the 5TY1 COM electronic circuit protection devices allows them to combine familiar protection and convenience functions in a way that has not previously been possible. The functions - with the exception of the basic functions - can be actively enabled/disabled and parameterized thereby permitting application-specific customization. Although these devices are supported in the Powercenter 1000 from firmware version V3.0, no functional expansions are possible. A Powercenter 1100/2000 must be used in order to support the device functions, as these are supplied subsequently by means of firmware updates.

In addition to the familiar measurement functions, it is now possible to change protected parameters, which means that the downstream behavior of the device can be defined more precisely depending on the cause of the trip (e.g. short-circuit/overload). The device features a new Standby (STBY) status for this purpose. This makes it possible to use power semiconductors to switch between ON (conducting, like modern circuit protection devices) and STBY (non-conducting/high-impedance) in order to avoid unwanted losses by standby loads, for example, or to reconnect following an overload trip.

In the case of another protected parameter, the sensitivity of the RCD trip can be changed from standard (22.5 mA) to sensitive (18.0 mA) or robust (27.0 mA) to suit the particular application.

The device also features an integrated self-test which cyclically monitors the device for anomalies and switches the device off when this is necessary in order to achieve a safe state.

Although versions for different currents exist, the current can also be set on each individual device.

The rated voltage is 230 V AC, however the device is capable of operating in the range from 85 to 255 V. In addition to this, the integrated POP function (Power Overvoltage Protection) can be activated (default = active) in order to protect connected loads against overvoltages.

3.9 Residual current measuring devices and 5SV8 COM MRCD

5SV8 COM RCM residual current measuring devices make it possible to monitor system status and faults in the circuit by means of transformer measurement. The signal evaluators and associated residual-current transformers can be combined in accordance with IEC 62020-1 as Type A or F (sinusoidal alternating current, pulsating alternating current) or as Type B (sinusoidal alternating current, pulsating alternating current, pure and pulsating direct currents and alternating currents up to 20 kHz). There are also versions of the RCM signal evaluators that have a residual-current transformer connection and versions with which up to four transformers are connected. These are referred to as 1-channel and 4-channel devices respectively.

MRCDs (Modular Residual Current protective Devices) are combinations of residual current measuring devices and tripping units/circuit breakers that represent a protective device in accordance with DIN EN 60947-2 Annex-M. Circuit monitoring in this case results in the circuit breaker being switched off by floating contacts and the tripping unit if the defined response value is reached.

They communicate their measured values wirelessly to the higher-level SENTRON Powercenter 1100/2000 and can be configured easily from there (not suitable for connection to the Powercenter 1000). Monitoring of the electric circuit enables predictive error detection by reporting pre-warnings.

The monitoring devices can be operated with 24 V DC or, alternatively, with 100-240 V AC.

3.10 5TT4 COM digital input/output module

The 5TT4 COM digital input/output module permits monitoring and control of systems and equipment via 2 digital inputs and 2 digital outputs.

The input and output signals can be gated in function blocks for this purpose. All the status information of the inputs and outputs is displayed via LEDs on the front and is also made available on the Powercenter 1100/2000 via wireless communication.

In addition to the standard measuring functions for device temperature and operating hours, the number of operating cycles is counted at the outputs.

The outputs can be set to a state for a defined time via the front button. Loads with 230 V / 5 A can be switched directly via the outputs.

The inputs can be operated with 24 V AC/DC.

The supply voltage of 24 V DC (SELV) can be bridged to other devices via the screwless plug-in terminals.

This device is only supported in the Powercenter 1100/2000 from firmware version V7.1.

3.11 Overview of compatibility

The table below provides an overview of the terminal device types that are compatible with the SENTRON Powercenter 1000/1100/2000 versions. The firmware version of the Powercenter which is the minimum requirement to fully support the terminal devices is specified. It is always recommended to keep the entire system up to date at all times. For more information, see the section Firmware update (Page 115).

Version V5.0 of the SENTRON Powercenter 1100 is the first basic version to support all the previous terminal device types. This also applies to version V7.1 of the Powercenter 2000.

Terminal device type	POC1000	POC1100	POC2000
5ST3 COM auxiliary switch/fault signal contact	V1.0	V5.0	V7.1
5SL6 COM miniature circuit breaker	V1.0	V5.0	V7.1
5SL6 COM miniature circuit breaker with RCM function	V2.0	V5.0	V7.1
5SV6 COM arc fault detection device	V1.0	V5.0	V7.1
3NA COM fuse	V1.0	V5.0	V7.1
3RV2 COM auxiliary and signaling switch	V3.0	V5.0	V7.1
5ST3 COM remote control auxiliary (RCA)	V3.0	V5.0	V7.1
5TY1 COM ECPD	(V3.0) [1]	V5.0	V7.1
5SV8 COM RCM and MRCD	---	V6.0	V7.1
5TT4 COM digital input/output module	---	V7.1	V7.1

[1] Although a basic connection is possible, new device functions of the 5TY1 COM ECPD are not supported with the SENTRON Powercenter 1000. Use of the SENTRON Powercenter 1100 is recommended.

Installation and connection

4

Note

Only qualified personnel are permitted to install, commission or service the devices.

- Wear the prescribed protective clothing. Observe the general equipment regulations and safety regulations for working with high-voltage installations (e.g. DIN VDE, NFPA 70E as well as national or international regulations).
- The limits given in the technical specifications must not be exceeded even during commissioning or testing of the device.
- Before connecting the device, make sure that the line voltage matches the specifications on the type plate.
- Before you start up the device, check that all the connections have been made correctly.
- Before power is applied to the device for the first time, it must have been located in the operating area for at least two hours in order to reach temperature balance and avoid humidity and condensation.
- Condensation on the device is not permissible during operation.
- Perform regular checks during operation in accordance with the applicable national and international regulations.

Note

During installation and connection, please note the five safety rules for work in or on electrical systems (Page 14).

Note

Prior to purchase or installation, it is necessary to check whether the equipment has the appropriate radio approval for the target country in which it will be operated.

The country radio approvals (https://support.industry.siemens.com/cs/de/de/view/109801197/en) can be found in the SiePortal (https://support.industry.siemens.com/cs/de/en/ps). Simply search for the product or the order number and select the Certificates option as the entry type.

4.1 Preparing installation

4.1.1 Checking delivery

Procedure

1. When you receive the delivery, check the packaging for visible damage in transit.
2. If you discover damage in transit, lodge a complaint with the carrier responsible. Have the carrier confirm the damage in transit immediately.
3. Unpack the device at its destination.
4. Keep the original packaging for reshipping the device. See information on damage.

NOTICE
Damage to the device during transportation and storage If a device is transported or stored without packaging, shocks, vibrations, pressure and humidity act on the unprotected device. Damaged packaging is an indication that the environmental conditions have already had a large impact on the device. The device may be damaged. Do not dispose of the original packaging. Pack the device for transportation and storage.

5. Check that the package contents are complete and undamaged.
6. If the package contents are incomplete or damaged, or not exactly what was ordered, inform the responsible delivery service immediately.

NOTICE
Damaged device • Ensure that the damaged device is not installed and commissioned. • Label the damaged device and keep it locked away. • Send the device for repair immediately.

NOTICE
Damage due to condensation If the device has been exposed to low temperatures or extreme temperature fluctuations during transportation, e.g. in cold weather, moisture may have formed as condensation on or inside the device. Moisture causes short-circuits in electrical circuits and damages the device. To avoid damage, proceed as follows: • Store the device in a dry place. • Equalize the temperature of the device with room temperature before starting it up. • Do not expose the device to the direct radiated heat of a heater. • In the event of condensation, only switch on the device when it has completely dried or after a delay of approx. 12 hours.

7. Also keep the supplied documentation in a safe place. It forms part of the device. When you commission the device for the first time, you will require the documentation.
8. Note the identification data of the device.

4.1.2 Identification of circuit protection devices

These circuit protection devices are usually used for final circuits and to secure individual phases and thus, a large number is used in a system. This is why quick recording and reliable archiving of the identification data is all the more important.

Identification of a circuit protection device is composed of two parts. The

1. Manufacturer identification
2. User identification

The electronic type plate is generated from both identification components.

4.1.2.1 Manufacturer identification

Manufacturer identification provides information on device-specific data such as:

- Device type
- Order number
- Serial number

These data are printed on the front or side of the device.

If there is a QR code on the device, it can be used to directly access the device information.

If there is an unlabeled Data Matrix Code on the device, this must be scanned using the Siemens Industry Online Support (SIOS) app (https://new.siemens.com/global/en/products/software/mobile-apps/industry-online-support.html) to obtain the data.

Example:

① SiePortal code for product information
② RF code for commissioning the communication function

The Data Matrix Code (DMC), which is marked with "RF Code", contains the following communication data in encrypted form:

- Device type
- MAC address
- Installation code

This communication information is necessary for commissioning so that the devices can connect to the SENTRON Powercenter 1000/1100/2000.

The RF code of the SENTRON Powercenter 1000/1100/2000 contains only the Bluetooth® PIN code that is required for connecting to the mobile device.

See also

Installation Manual - SENTRON circuit protection devices with communication and metering function (https://support.industry.siemens.com/cs/ww/en/view/109791805)

4.1.2.2 User identification

User information is used to identify or locate and distinguish the devices from each other. Usually this consists of:

- Plant identifier
- Location identifier
- Installation date

This information is noted by the customer, usually as an adhesive strip, on the device and identically in the system plan. With communication-capable circuit protection devices, this information can be set in parameters and read out using software.

With SENTRON COM circuit protection devices, it must be ensured that the DMC code labeled "RF code" is always clearly visible for the purposes of commissioning using SENTRON Powerconfig mobile. If the code is not legible or accessible, commissioning can also be performed "offline" prior to installation.

You can find more information on this subject in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109791805).

Note

This is particularly necessary for 3NA COM fuses because after installation, these are no longer accessible without shutting down the main circuit.

In addition, the communication function offers a possibility of allowing each communication-capable device to flash with an LED for a certain time, which can facilitate the locating of a device during maintenance.

Note

If the Data Matrix Code is no longer legible because it has been covered or scratched during cleaning, this does not constitute a reason for a complaint.

4.1.3 Installation conditions

The devices can be mounted on a DIN rail in any installation position. The direction of incoming supply is arbitrary for communication-capable miniature circuit breakers and arc fault detection devices and must be set as a parameter in line with the physical direction of incoming supply.

In the case of the SENTRON Powercenter 1000/1100/2000 data transceiver, care must be taken to ensure that there is enough space for the Ethernet plug, pullout and the cable bending radius.

Furthermore, it is necessary to make sure that the data transceiver is mounted with a small distance to metallic surfaces in all directions (apart from the DIN rail) so that the efficiency of the integrated antenna is not impacted too much.

For the 3NA COM fuse, the usual installation position is vertical, as for the other LV HRC fuse links. The current load does not need to be reduced under normal ambient conditions. However, there are devices and applications, where the LV HRC fuse links are arranged horizontally. As per usual, the instructions of the device manufacturer, especially the maximum current-carrying capacity, must be observed in this case.

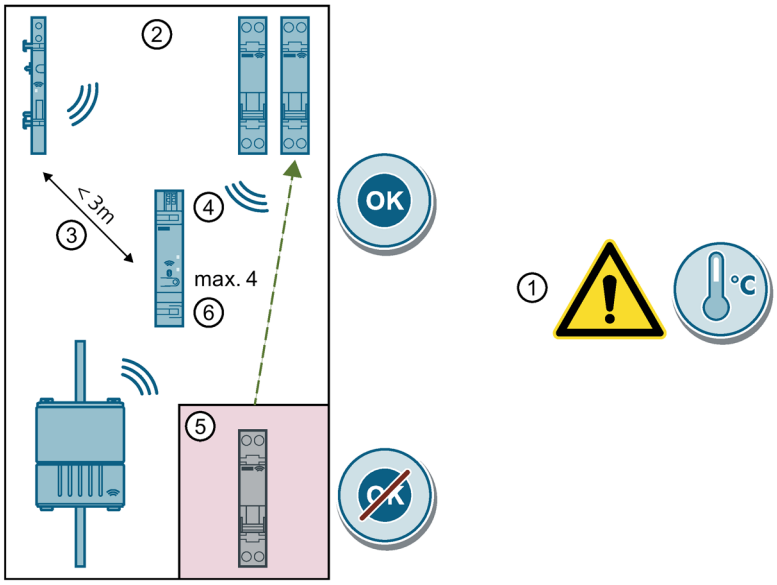
Note

Overhead installation

The upside down installation of the 3NA COM LV HRC fuse links, i.e. with the electronic module above the fuse unit is not permitted. It is possible to overheat the electronic module.

The ventilation slots must not be covered or closed. Follow the ESD guidelines (Page 149) and the mounting instructions of the operating instructions of the electronic module.

The spatial arrangement of the communication-capable circuit protection devices one below the other corresponds to the following recommendations:



(1) Prior to setting up the distribution board, pay attention to devices with a high temperature development. As usual, these are positioned away from smaller, more sensitive devices.

(2) The SENTRON Powercenter 1000/1100/2000 and the associated terminal devices should be installed together in one control cabinet or panel so that wireless communication is less disturbed by other devices or obstacles.

(3) The maximum recommended distance between the terminal devices and the SENTRON Powercenter 1000/1100/2000 should not exceed 3 m. The radio transmit power can be changed as a parameter, which can either decrease or increase the permitted distance between the devices. The default setting of the transmit power of 0 dBm allows a distance of over 10 m without any other disturbances.

Important: The transmit power of each device in the system must be set the same so that the distance to another system can be reduced.

(4) If possible, the SENTRON Powercenter should be placed equally far away from all terminal devices. Therefore, a centrally located place is recommended.

(5) No metallic partitions or other RF devices that use the same radio frequency should be installed between the individual terminal devices and the SENTRON Powercenter data transceiver so that radio transmission can be permanently ensured.

(6) If more than 24 communication-capable circuit protection devices are installed, further SENTRON Powercenter 1000/1100/2000 devices will be required. An equal distribution of the terminal devices between the different SENTRON Powercenter devices is recommended.

If several SENTRON Powercenter 1000/1100/2000 devices share the same radio channel, interferences may occur between the devices. To ensure that this does not happen, the expansion of the radio range can be reduced by lowering the transmit power of all devices in the system. The minimum transmit power amounts to -18 dBm. This allows the devices to be positioned closer together (< 10 m for metallic housings, approx. 50 m in the free field without obstacles).

For more information, see the section Commissioning several SENTRON Powercenter 1000/1100/2000 devices (Page 60).

In security-critical systems, it is important to note that the radio protocols can be disrupted from the outside. Suitable countermeasures such as adequate shielding are recommended for this reason.

4.1.4 Permitted ambient conditions

Communication-capable circuit protection devices must be installed such that the ambient conditions, e.g. temperature, air humidity and pollution, specified in the data sheets are observed.

You can find the data sheets using the SiePortal (https://sieportal.siemens.com).

You can find more information about 5SV8 COM RCM in the Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109975845).

In case of increased ambient temperatures, a correction factor must be applied for the rated current. This applies to the 3NA COM fuse at a temperature of > 40 °C and the 5SV6 COM arc fault detection device or the 5SL6 COM miniature circuit breaker at temperatures > 30 °C according to the respective configuration manual of the product family. You can find more information on this topic in the SiePortal (https://sieportal.siemens.com). Search for the corresponding product.

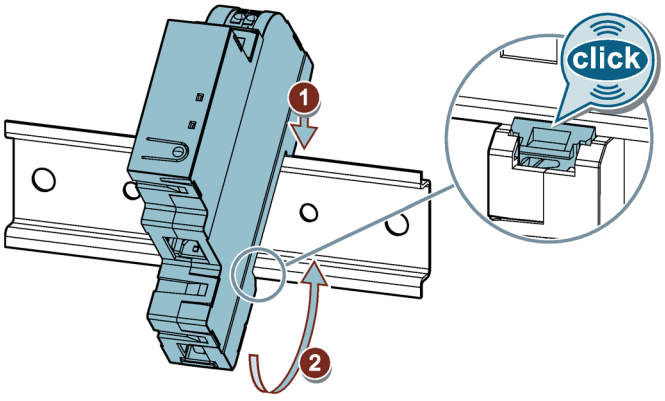
4.2 Device installation

Please refer to the operating and installation instructions of the individual devices to ensure that devices are installed correctly. You can access these in the SiePortal (https://sieportal.siemens.com) or in the section Reference documents (Page 9).

4.2.1 Simple installation on the DIN rail

Most communication-capable circuit protection devices are simply snapped onto the DIN rail. The DIN rail holder must engage.

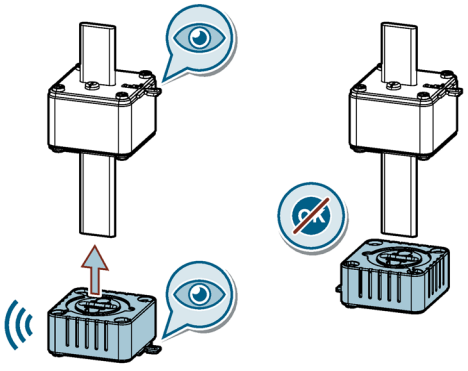
Example for SENTRON Powercenter 1000:



Note

Summation current transformers for 5SV8 COM RCM/MRCD that are larger than 60 mm must be bolted on.

4.2.2 Install 3NA COM fuse



The 3NA fuse link can only be installed in an LV HRC fuse link holder together with the 3NX electronic module pushed on.

The LV HRC 3NA COM fuse link and the appropriate electronic module can be ordered as a unit, however they are delivered in separate packages and still have to be mounted together.

Installation takes place in all common LV HRC fuse bases or fuse switchgears of the appropriate size similar to the installation of a normal LV HRC fuse link according to IEC 60269-2 without the electronic module.

The 3NA COM electronic module does not require a separate power connection. It supplies itself from the primary current via the current transformer according to the Energy Harvesting principle, however, it requires a minimum current of 5 A for this purpose.

Note

The gFF operating class is only approved for the Netherlands. The relevant installation specifications apply.

In the event that the fuse link has switched off following a short-circuit or an overload, the fuse link must be replaced. Remove the LV HRV 3NA COM fuse link and the electronic module out of the device, pull the electronic module down off the contact blade and re-insert the electronic module on to the new 3NA COM fuse link in reverse order. The LV HRV 3NA COM fuse link can also be ordered separately.

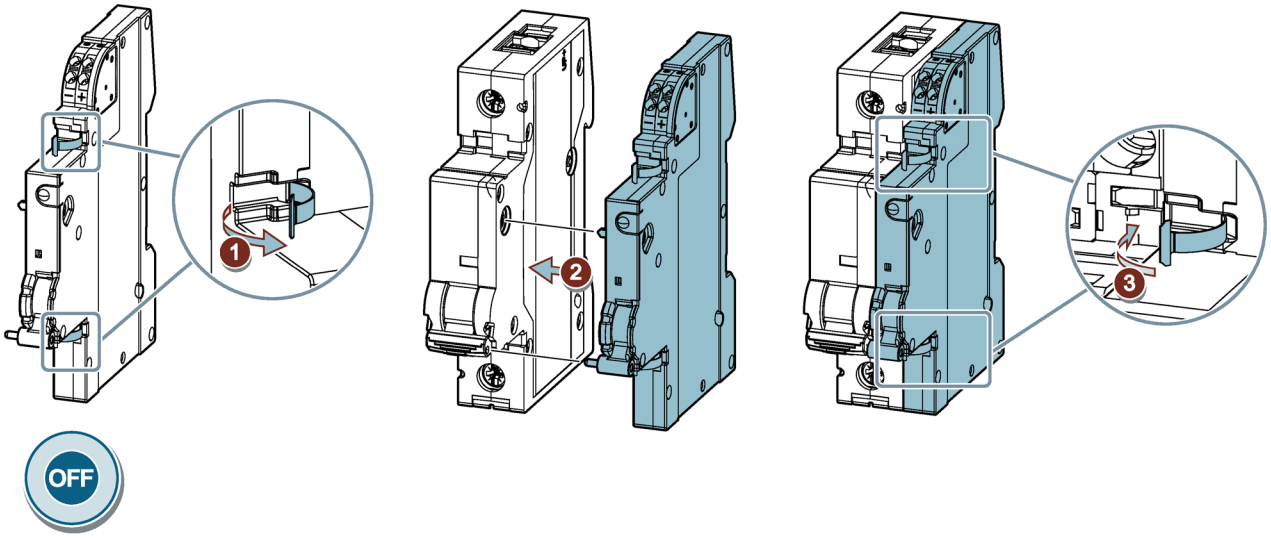
The electronic module can be reused under certain circumstances, but this must be checked after recommissioning.

4.2.3 Auxiliary switches and mount-on devices

Auxiliary switches for attaching to main devices must first be mounted on the main device before the two devices together are mounted on the DIN rail. This reduces the risk of injury.

The supply voltage lines must be connected or disconnected in the assembled state.

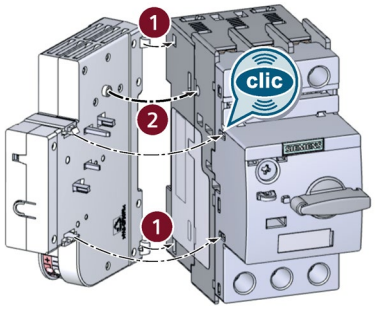
5ST3 COM auxiliary switch/fault signal contact:



The 5ST3 COM auxiliary switch/fault signal contact can be attached to the following main devices:

Designation	Article numbers
Device protection switches or miniature circuit breaker	5SL, 5SY, 5SP
Residual current operated circuit breaker or RCBO	5SU1, 5SV
Other switching devices	5TL, 5ST30

3RV2 COM auxiliary and signaling switch:

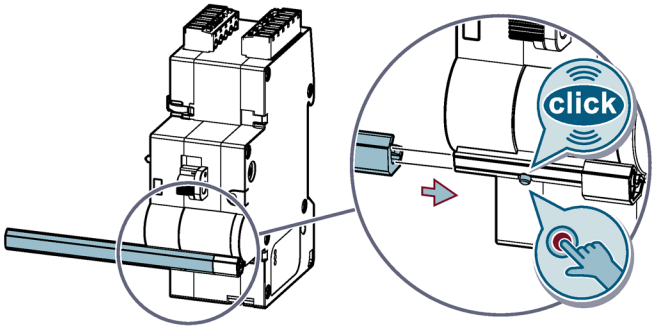


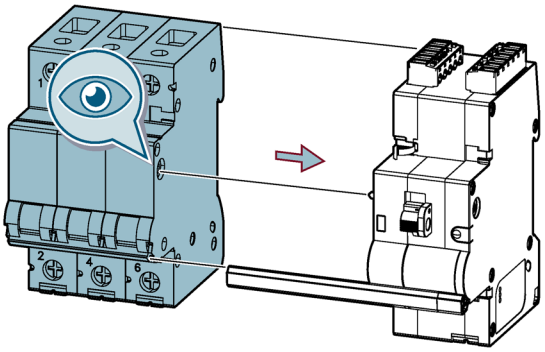
① Attach the wireless auxiliary and signaling switch to the rear of the motor starter protector.
② Press the wireless auxiliary and signaling switch to the motor starter protector until you hear it engage (the motor starter protector must be switched off).

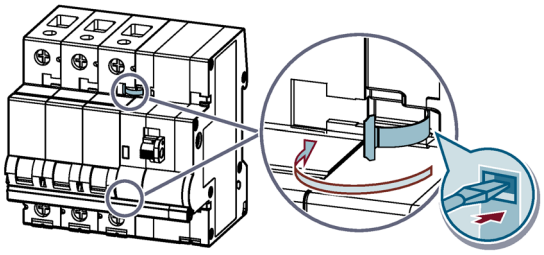
5ST3 COM remote control auxiliary (RCA):

Mount the 5ST3 COM remote control auxiliary on the main device. A handle adapter suitable for the main device must be used.

	Suitable for	
5ST3820-1	5SY4/5/6/7/8 - 1/2 pole, 5SP4 - 1 pole	5SY60...CC
5ST3820-2	5SY4/5/6/7/8 - 3/4 pole, 5SP4 - 2/3/4 pole	
5ST3820-3	5SM2	
5ST3820-5	5SU1 (max. 3 width units)	
5ST3820-6	5SL6/4 - 1/2 pole, 5SY...CC, 5TL1 - 1/2 pole	5SV1/3/4/9, 5SL60, 5SV60
5ST3820-7	5SL6/4 - 3/4 pole, 5SY...CC, 5TL1 - 3/4 pole	







See also

5ST3 COM operating instructions
(https://support.industry.siemens.com/cs/ww/en/view/109823192)

4.3 Connecting the devices

The communication-capable 5SL6 COM miniature circuit breaker and 5SV6 COM arc fault detection device have an integrated power supply unit for the electronics, as do the 5ST3 COM remote control auxiliary and the ECPD (5TY1 COM). Therefore, the phase and N conductor (230 V AC) must be connected.

The SENTRON Powercenter 1000/1100/2000, the 5ST3 COM auxiliary switch/fault signal contact, the 5TT4 COM digital input/output module, and the 3RV2 COM wireless auxiliary and signaling switch are supplied using an extra-low voltage of 24 V DC (SELV). The screwless connection terminals of the devices enable a loop-through (daisy chain) of the supply voltage.

The 3NA COM fuses are supplied via Energy Harvesting from the main circuit and therefore do not require any additional wiring to the connections made as standard.

The 5SV8 COM RCM monitoring devices can operate with 24 V DC or, alternatively, with 100 - 240 V DC/AC.

⚠ WARNING
Danger due to fire or electric shock. **May cause death, serious personal injury, or equipment damage.** Only use leads that correspond to the local safety regulations.

The operating and installation instructions of the individual devices describe how to connect the devices correctly. You can access these in the SiePortal (https://sieportal.siemens.com).

You can also find the instructions in the section Reference documents (Page 9).

The connection of the 5SL6 COM miniature circuit breaker with power measurement (without RCM function) is a special case: Here the neutral conductor can be dispensed with on the outgoing side. With all other circuit protection devices, the neutral conductor must

also be connected on the outgoing side in order to ensure that the device functions are fully operational.

NOTICE
DIN-rail mounting To avoid material damage, mount the devices for connection firmly on the DIN rail.

4.4 Interfaces of the SENTRON Powercenter 1000/1100/2000

4.4.1 Ethernet interface

After mounting, the protection of the Ethernet plug must be removed in order to insert an Ethernet cable (Cat5 F/UTP or better). This connection enables IP communication of the SENTRON Powercenter 1000/1100/2000. If the data transceiver is connected to an Ethernet switch or a router, the data or parameters can be viewed or set in the whole local network via LAN or WLAN. Only the IP parameters, such as a static IP address, can be changed in the app via Bluetooth®.

A VPN connection or another gateway can be used for advanced access beyond the local network. For more information, see the chapter Application examples (Page 99).

The secure, encrypted protocol https via REST API is used as standard for commissioning with the SENTRON Powercenter 1100/2000. The unencrypted Modbus TCP connection can be switched on and off separately.

Both Ethernet sockets of the SENTRON Powercenter 1100/2000 have a switch function. This allows additional devices in the same network to be connected.

Note

Network scan

The use of vulnerability scanners can affect the SENTRON Powercenter 1100 (firmware version V5.0). The use of such tools is not currently recommended, as it would necessitate restarting the Powercenter 1100.

The SENTRON Powercenter 2000 additionally features an MQTT connection that is provided via the same Ethernet interface. This MQTT connection allows the device to be directly connected to a cloud solution. The Powercenter 2000 also features an integrated web server which can be accessed in the browser via the set IP address if the browser is in the same network.

See also

Secure protocol – https via REST-API (Page 91)

Modbus TCP connection (Page 84)

Cloud connection via MQTT (Page 92)

4.4.2 Bluetooth® interface

The Bluetooth® interface enables local access to the data of the SENTRON Powercenter 1000/1100/2000 on site. This is the Bluetooth® Low Energy 4.2 standard. However, data transmission performance can be significantly improved with Bluetooth® Low Energy 5.1.

In order to establish the connection, the data transceiver must first be set to Bluetooth® mode. This is either done after restarting the device or after a short button press (< 3 s). To do so, the mobile terminal device must be located near an active Bluetooth® (approx. 5 m – 10 m). Only one active connection is supported. As of firmware version 1.1.0, the plant identifier, if entered, is displayed in addition to the device type. This makes it easier to distinguish between multiple devices.

The 6-digit Bluetooth® PIN of the data transceiver must be entered to complete the connection and to establish an encrypted connection between the SENTRON Powercenter 1000/1100/2000 and the mobile terminal device (encryption: AES CCM algorithm with 128 bits). This can either be scanned using the Data Matrix Code or manually typed in using the information printed on the side of the device. The PIN code can be changed for increased security after commissioning. The data transceiver must be reset in order to reset the PIN to the factory setting (button press ≥ 10 s). Similarly, the reception strength for Bluetooth® can be decreased or increased so that remote access can be prevented or the range can be increased.

The Bluetooth® mode of the SENTRON Powercenter 1000/1100/2000 is switched off again if left unused for a period of 180 seconds. The LED will flash as long as the device is in the Bluetooth® search mode. If the time without active connection has expired, the function is switched off or if a connection has been successfully established, the COM LED will stop flashing at 2 Hz.

If a mobile device is connected to the SENTRON Powercenter 1000/1100/2000 via Bluetooth®, this connection can be disconnected by terminating the connection on the mobile terminal device or by pressing the button on the SENTRON Powercenter 1000/1100/2000 once again (< 3 s). The Bluetooth® mode of the data transceiver is also switched off if the PIN is entered incorrectly three times.

Note

Due to the performance, larger data packages such as Trends in SENTRON Powerconfig mobile are not displayed via the Bluetooth® interface. Commissioning should only be carried out once in this manner.

Because the SENTRON Powercenter 1000/1100/2000 provides radio communication for the circuit protection devices and Bluetooth® communication for the mobile devices using the same radio module, the performance of the Bluetooth® connection is restricted. Therefore, the Modbus/TCP-connection via Ethernet is recommended for faster data transmission.

4.4.3 Radio interface to the devices

The circuit protection devices with communication and measuring function provide the SENTRON Powercenter 1000/1100/2000 with their data via radio. Data can be read from the devices and changed parameters can be sent to the devices.

Communication is possible via radio as soon as the devices are connected and supplied with power (minimum 5 A for the 3NA COM fuse).

A SENTRON Powercenter 1000/1100/2000 can communicate with up to 24 terminal devices. Each of these circuit protection devices must join the secure radio network of the Powercenter, which means each terminal device must be paired with the SENTRON Powercenter. The terminal devices do not communicate among one another, rather communication with the data transceiver is bidirectional/in a star configuration (no mesh-network).

In order to pair the devices, the RF code of the terminal devices must be scanned; this transfers the device type, MAC address and installation code of the device. Alternatively, this information can be entered manually. A description of the procedure can be found in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109791805).

Note

Once the terminal device has been paired with the data transceiver, the installation code is encrypted and replaced so that each communication connection is separately encrypted (encryption: AES CCM algorithm with 128 bits). Therefore it is necessary to reset the communication information in order to be able to carry out another pairing.

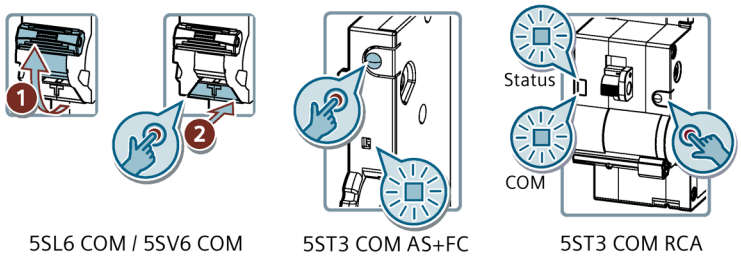
If radio transmission is disturbed or interrupted, no data are transmitted. This can be checked via the offline status of the terminal devices. Radio transmission can be significantly influenced by other transmitting devices. It can result in losses of individual data packages. A recommendation for installation is provided in the section Installation conditions (Page 34).

4.5 Operation of circuit protection devices

4.5.1 Standard operator controls - levers and buttons

The circuit protection devices with measurement and communication function have different operating options in addition to the communication function. Most devices have at least one button and/or one lever.

Examples:



5SL6 COM / 5SV6 COM 5ST3 COM AS+FC 5ST3 COM RCA

Only the 3NA COM fuse has neither LEDs for status display nor operating options on the device itself. The operation for this only works via the communications interface and a corresponding software, such as SENTRON Powerconfig mobile.

The following operating options are provided:

Table 4- 1 Powercenter 1000/1100/2000:

Description	Action	POC 1000	POC 1100	POC 2000
Activation of Bluetooth® mode (COM LED flashes at 2 Hz as long as no smartphone is connected)	Button press < 3 s	✓	✓	✓
Disconnection of active Bluetooth® connection	Short button press < 3 s	✓	✓	✓
Reset of the Bluetooth® PIN	Button press ≥ 10 s	✓	✓	✓
Reset of the local login data (user name, password)	Button press ≥ 20 s with repeated brief confirmation using the button within the next 10 s	---	✓	✓

Table 4- 2 Subordinate circuit protection devices

Description	Action	5ST3 / 3RV2	5SL6 MCB	5SV6 AFDD	5TY1 ECPD	5SV8 RCM	5TT4 DIDO
Switching the device on or off	Lever in Open or Closed position	---	✓	✓	✓	---	---
Confirmation of a tripping operation if the LED flashes red	Short button press < 3 s	---	✓	✓	✓	---	---
Execution of a self-test incl. triggering of test button if no other fault is active	Short button press < 3 s	---	---	✓	✓	---	---
Confirmation of an RCM alarm if alarm auto-reset is deactivated	Short button press < 3 s	---	✓[1)]	---	---	✓	---
Execution of an RCM function test if no other fault is active	Short button press < 3 s	---	✓[1)]	---	---	✓	---
Confirmation to allow setting of protected parameters (device protection functions)	Short button press < 3 s within specified settable time	---	---	---	✓	---	---
Reset of the RF communication information, i.e. unpairing from Powercenter	Button press ≥ 10 s	✓	✓	✓	✓	✓	---
Toggle outputs for 60 s	Button press < 3 s but > 0.3 s	---	---	---	---	---	✓

[1)] Only for RCM versions

If a 5SL6 COM miniature circuit breaker or a 5SV6 COM arc fault detection device has tripped (overload, short-circuit or arcing fault), the device is switched off and the lever is in the OFF position. Communication is not possible in this state. In order to switch on the device again, the lever must be moved up to the ON position. Communication is then possible and the LEDs indicate that the device has tripped via its protection function by flashing red. In order to acknowledge this flashing, the tripping operation has to be confirmed with a short button press.

For the 5SL6 COM miniature circuit breaker with RCM function, the internal RCM measuring function can be tested with a short button press. Each activated RCM alarm is tested, including LED activation, alarm and stored message. Devices with the RCM function have a function that allows an RCM alarm to be displayed until it is acknowledged with a short button press or software command. This function is deactivated by default, i.e. an RCM alarm is no longer displayed after the measured value falls below the set limit.

The 5TY1 COM electronic circuit protection device (ECPD) also retains a communication function in the mechanical OFF state, as the direction of incoming supply is specified (labeled LINE on the device, from below). A trip can also be indicated in the STBY or OFF state as a result (depending on the setting in the trip configuration) and can also be acknowledged. An LED is also integrated in the handle of the ECPD and is visible when the handle is in the top end position (mechanically closed). The semiconductor status of the device is indicated on this LED (ON = red / STBY = yellow), as is ARD reclosing (flashing red).
The ECPD features an integrated self-test which is either performed cyclically (once a day) or via the app or by pressing a button on the device. If the test button is pressed on the device, the device confirms that the test has been performed successfully by a trip to the OFF position. When the device performs its cyclic self-test or a remotely triggered test, the device is not tripped to OFF. The results of both the RCD and the device tests are displayed and stored in the SENTRON Powerconfig mobile app.

With 5SV8 COM RCM versions, the reset must be confirmed on the display after pressing the Reset button.

The communication information of the 3NA COM fuse can only be reset if the fuse is capable of communication but is unable to establish a connection to the SENTRON Powercenter 1000/1100/2000 for more than 24 hours. For this purpose, the fuse must be operated with sufficient load current but the SENTRON Powercenter 1000/1100/2000 data transceiver must be switched off.

Following first commissioning of the SENTRON Powercenter 1100, at least one user must be created with the "Superuser" role so that commissioning can be completed and new users can be created. All users are reset with a very long button press (20 s) followed by a brief confirmation within 10 s while the LEDs are lit yellow. The initial Superuser can be created again once this has been done. For more information on this subject, see the section Role-based access control (Page 91).

See also

Bluetooth® interface (Page 42)

Decouple (Page 56)

4.5.2 Other operator controls

Other operator controls exist in addition to the standard operator controls which are present in most of the communicative circuit protection devices.

Remote switching on 5ST3 COM remote control auxiliary

Yellow slide switch to block the remote switching function and to reset various error/status messages.

To reset a message, move the slide switch to the OFF position (the operating lever must also be switched off) and then back to "RC ON".

The 5ST3 COM remote control auxiliary can be operated remotely either via the wired connections on the plug-in terminal block (default) or via the communications interface. The communications interface must first be activated for security reasons.

You can find more information on this subject in the Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109823192) and also in the section Switching operation (Page 78).

Write protection on SENTRON Powercenter 1100/2000

A tool is required to operate the slide switch on the SENTRON Powercenter 1100/2000.

If the switch is in the lower position, the device can be configured as required by any user logged in who has the appropriate user roles. Write protection is deactivated.

If the slide switch is in the upper, locked position, no data points/parameters/commands can be sent to the data transceiver. This means that terminal device pairing is also deactivated. The purpose of this setting is to prevent any changes after configuration in security-critical systems.

5SV8 COM RCM residual current monitors

Rotary selector switch for selecting the rated residual current/threshold value for the RCM alarm and the delay time for the RCM alarm. If the COM position is selected, all the values set via the communications interface/software apply. Both selector switches must be set to COM for configuration using SENTRON Powerconfig.

The devices that have a display can be configured using the menu structure or via communications interface and SENTRON Powerconfig software.

You can find more information on this subject in the Operating Instructions:

- 5SV8 COM RCM residual current monitor (https://support.industry.siemens.com/cs/ww/en/view/109973379)
- 5SV8 COM MRCD modular residual current device (https://support.industry.siemens.com/cs/ww/en/view/109973380)
- Configuration Manual – 5SV8 residual current measuring devices and modular residual current protection devices (https://support.industry.siemens.com/cs/ww/en/view/109975845)

4.6 LED signaling of the SENTRON circuit protection devices

Circuit protection devices with measuring and communication function use LEDs to display different statuses.

The status of the 3NA COM fuse can only be displayed via the communications interface, as no LED is available for this purpose.

You can find the exact status displays of each device in the operating and installation instructions of the individual devices (see Reference documents). A detailed description is especially important if several LEDs are available on a device.

General statuses that are supported by almost all devices exist, but also specific statuses that are only displayed by certain devices. See the tables below for further details.

A flashing frequency of 2 Hz means that the LED flashes twice per second. Similarly, flashing at 5 Hz (5 times per second) is faster.

Table 4- 3 General statuses

Description	LED	LED response	Note
Function not available or device has no power supply		Off	
Device in working condition, function possible without restrictions		Permanently green	
No radio connection to the Powercenter (for terminal devices) or no radio connection to terminal devices (for Powercenter)		Slow green flashing at 0.75 Hz	Usual display via COM LED, if available
Internal process running, e.g. connection setup, firmware update		Flashing green at 2 Hz	Usual display via COM LED, if available
Unpairing from Powercenter (for terminal devices) or reset of Bluetooth® PIN (for Powercenter)		Flashing green at 2 Hz with a change to very fast flashing at 10 Hz after 10 s when the action is complete.	Usual display via COM LED, if available
Device localization via software active for 10 s		Fast green flashing at 5 Hz	Usual display via COM LED, if available
Communication error. Fault rectification with a long button press (≥ 10 s) and re-pairing.		Flashing yellow at 2 Hz	Usual display via COM LED, if available
Warning about the upper limit violation of a measured value (e.g. temperature, current or voltage). Warning disappears automatically when the measured value leaves the set limit.		Flashing green/yellow at 2 Hz	Usual display via devices/ON/Act/status LED, if available
Warning about an upper limit violation of service life parameters (e.g. operating hours, operating cycles, tripping operations) This warning remains active until it is switched off or until the limit is increased.		Flashing yellow/red at 2 Hz	Usual display via devices/ON/Act/status LED, if available
Device error, e.g. self-test failed. If the error remains active after a device restart, the device must be replaced.		Fast red flashing at 4 Hz	Usual display via devices/ON/Act/status LED, if available
Tripping of the circuit protection device or of the attached circuit protection device (does not apply to Powercenter)		Flashing red at 2 Hz	Usual display via devices/ON/status LED, if available

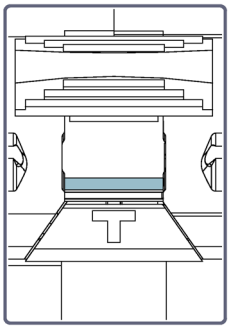
Table 4- 4 Device-specific flashing patterns

Description	LED	LED response	Note
Powercenter 1000/1100/2000			
Bluetooth® mode is active and searching for mobile devices		Flashing at 2 Hz green	COM LED
Powercenter 1100/2000			
Bluetooth® mode is active, Powercenter is connected to the mobile device		Permanently green with short flashing every 2 s	COM LED
Reset of all login data (users and passwords)		Yellow light after button is pressed for 20 s. Confirm with a short button press within the next 10 s.	COM and ACT LEDs
5ST3 COM and 3RV2 COM auxiliary switches			
Manual switching off of the main device		Flashing yellow/red at 2 Hz	
5SL6 COM miniature circuit breaker with RCM function and 5TY1 COM ECPD			
RCM advance warning		Flashing green/yellow at 2 Hz	Display via RCM LED (5SL6) or device LED (5TY1)
RCM alarm		Flashing yellow at 2 Hz	Display via RCM LED (5SL6) or device LED (5TY1)
5SV8 COM RCM/MRCD			
Malfunction, can be resolved by user, for example connection error		Fast flashing at 4 Hz yellow	ON LED
RCM advance warning		Permanently yellow	Display via RCM alarm LED(s). Accompanied by display of filler value depending on version.
RCM alarm		Flashing yellow at 2 Hz	Display via RCM alarm LED(s). Accompanied by display of filler value depending on version.
5ST3 COM remote control auxiliary (RCA) (status LED)			
1) Device switched off manually or: 2) Remote switching function off (RC off)		Slow green flashing at 0.75 Hz	
Device charging for reclosing (ARD)		Flashing green at 2 Hz	
1) Warning (see table above) or: 2) IR test warning or: 3) Closing operation failed (e.g. ARD unsuccessful after 3 attempts)		Flashing green/yellow at 2 Hz	2) and 3) can be reset with the yellow slide switch (OFF → RC ON)
1) Warning (see table above) or: 2) Reset of errors via yellow slide switch was unsuccessful		Flashing yellow/red at 2 Hz	2) can be reset with the yellow slide switch (OFF → RC ON) After 5 failed attempts: device error.
Performing test (RCD and/or IR test)		Fast green/red flashing at 5 Hz	Applies only to version with RCD test function.

Description	LED	LED response	Note
1) Attached protection device has tripped. or: 2) RCD/IR test has failed. Can be reset using the yellow slide.		Flashing red at 2 Hz	2) Applies only to version with RCD test function. It can be reset with the yellow slide switch (OFF → RC ON).
5TT4 COM DIDO status LEDs for inputs and outputs			
DI1/DI2		Permanently green	Input 1 (high)
		Off	Input 0 (low)
DO1/DO2		Permanently green	Contact closed
		Off	Contact open

4.6.1 5TY1 COM ECPD handle LED

For the first time ever in the case of circuit protection devices, the switching status is indicated by an LED in the handle.



LED	Status
	No LED / green marking Mechanical OFF
	LED permanently yellow Standby
	LED permanently red ON
	LED flashes red at 2 Hz ARD (automatic reclosing) active

Commissioning

5

Note

Only qualified personnel are permitted to install, commission or service the devices.

- Wear the prescribed protective clothing. Observe the general equipment regulations and safety regulations for working with high-voltage installations (e.g. DIN VDE, NFPA 70E as well as national or international regulations).
- The limits given in the technical specifications must not be exceeded even during commissioning or testing of the device.
- Before connecting the device, make sure that the line voltage matches the specifications on the rating plate.
- Before you start up the device, check that all the connections have been made correctly.
- Before power is applied to the device for the first time, it must have been located in the operating area for at least two hours in order to reach temperature balance and avoid humidity and condensation.
- Condensation on the device is not permissible during operation.

5.1 Commissioning with SENTRON Powerconfig mobile

The measurement and communication-capable SENTRON circuit protection devices are put into operation with the SENTRON Powerconfig commissioning app for mobile devices, also known as Powerconfig mobile.

Note

You can find a detailed description of how to proceed using the app in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109791805).

First the SENTRON Powercenter 1000/1100/2000 data transceiver must be added. This can happen in the following ways:

- WLAN search if the SENTRON Powercenter 1000/1100/2000 and the mobile device are located in the same network.
- Bluetooth® search of all available devices. To do so, Bluetooth® mode must be activated with a short button press and the Bluetooth® PIN code must be entered after scanning the Data Matrix Code. The PIN code can also be entered manually with the code printed on the side of the device.

- Manual entry of the IP address of the SENTRON Powercenter 1000/1100/2000. This may be necessary if at first all devices are to be added offline or in case of a VPN connection the IP address must be entered manually for security reasons. In order for the data transceiver to set up a communication with the smartphone or tablet, it must be connected to the 24 V DC-power supply. After the supply voltage has been applied and the IP address has been determined, it can be subsequently changed in the app.

Then the individual communication-capable terminal devices must be added. To do so, the DMC must be scanned with the "RF code" marking of the individual devices; this contains the device type, MAC address and the installation code. Alternatively the scanning step can be skipped and the aforementioned information can be entered manually. These are printed on the side of the device.

A unique name or plant identifier must be provided when adding the communication-capable terminal devices so that the devices can be distinguished from one another.

Note

Scanning can also be performed without powering the devices. This is necessary if the RF codes are not accessible when fully installed (e.g. possible with the 3NA COM fuse) or the devices are not allowed to be switched off to scan the RF code. The RF code of the 5SL6 COM miniature circuit breakers and 5SV6 COM arc fault detection devices can only be scanned if the operating lever is set to the Off position.

Two Data Matrix Codes need to be scanned for the 3NA COM fuse. First the one of the electronic module and then the one of the fuse link

The 3NA COM fuse link and the electronic module can still be scanned when installed, e.g. in a 3NP fuse switch disconnector, if necessary, the flashlight function of the mobile device must be used to illuminate the code.

Then the communication-capable devices must be paired with the SENTRON Powercenter 1000/1100/2000. This is only possible if the devices are powered, contrary to the previous steps, which can also be carried out offline. Pairing can be carried out for each individual device or simultaneously for several devices. Here, the terminal devices are connected one after the other in groups.

⚠ DANGER

Hazardous voltage

Will cause death, serious personal injury, or equipment damage.

In order to be able to establish communication, the devices must be switched on and supplied with power. In doing so, attention must be paid to sufficient safety measures (among other things, touch protection).

The measured values can be examined if the devices are paired. The trends are only displayed with an existing WLAN (Ethernet) connection. Similarly, the parameters of the individual devices can now be adapted, for example, the plant identifier which is required for the identification of the devices. For example, the various alarm messages (see the section Messages (Page 72)) can be changed, switched on or off, or the cyclic time synchronization of the SENTRON Powercenter 1000/1100/2000 (see the section Time synchronization

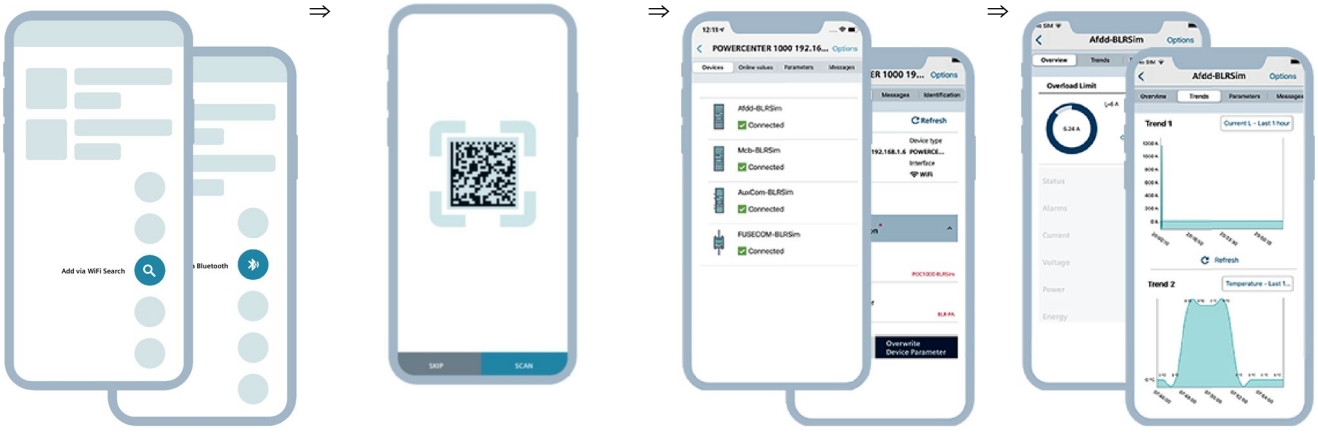
(Page 83)) can be activated. In addition, there are also views of the device identification and the stored messages such as exceeding an alarm limit or the tripping of a device.

Note

The communication parameters for the IP connection (DHCP and static IP address) can only be changed in SENTRON Powerconfig mobile via Bluetooth®. Alternatively, the SENTRON Powerconfig PC version can be used via Ethernet.

During commissioning, the devices display different statuses on the LEDs; these were explained in the section LED signaling of the SENTRON circuit protection devices (Page 47). Upon completion of the commissioning process, all LEDs should be static green, i.e. the commutative circuit protection devices are fully functional.

1. Adding the Powercenter (Bluetooth® or Ethernet) ⇒ **2. Adding and pairing the communicative circuit protection devices** ⇒ **3. Display and parameterization of the connected devices** ⇒ **4. Visualization of the recorded values**



If a SENTRON Powercenter 1000/1100/2000 is added to another project with another mobile device, the terminal devices do not need to be scanned and paired again if they have already been paired.

5.2 Commissioning with SENTRON Powerconfig for PC

Alternatively, the circuit protection devices with communication and measuring function can also be (re)configured with the SENTRON Powerconfig PC software. First the SENTRON Powercenter 1000/1100/2000 must be added from the same network. Then the individual terminal devices that have already been paired must be added in the online view "Overview": Unpaired terminal devices can be added from the library and paired by entering the device address, the MAC address and the installation code in the "Communication" view after the fields have been enabled.

An alternative is to export an existing project from SENTRON Powerconfig mobile once commissioning has been completed. In doing so, a .splx file is stored on the smartphone, which can be imported as a PC version. In addition, the project data and parameters can be easily viewed and further processed on the PC. The extended range of functions of the SENTRON Powerconfig PC version also enables a firmware update of the entire system via the SENTRON Powercenter 1000/1100/2000.

Similarly, a .splx file could be exported from the PC version, archived on the PC and imported in SENTRON Powerconfig mobile.

5.3 Setting of parameters

All devices have parameters that can be set. Some parameters are found on different device types, others only on specific ones. See the section Data points and Modbus registers (Page 89) for details on the availability of parameters on each device.

Important parameters that can be set are:

- The plant identifier, as a unique name of each device
- The system time on the SENTRON Powercenter 1000/1100/2000
- The Ethernet settings on the SENTRON Powercenter 1000/1100/2000 (static IP address can be set only via Bluetooth® or Powerconfig PC)
- The order number of the fuse link for the 3NA COM fuse, without which the rated current of the device is not known
- The direction of incoming supply for the 5SL6 COM and 5SV6 COM. This influences the counters for exported energy and imported energy and the sign of the power factor. If the set and physical direction of incoming supply match, the sign is positive
- The radio transmit power, which must match for all devices in the system if changes are necessary
- The automatically selected radio channel of the SENTRON Powercenter 1000/1100/2000
- All alarm settings that must be selected depending on the application
- Parameters for remote control (wired or via radio frequency), for the reclosing function (ARD) and for the RCD/IR test with the 5ST3 COM remote control auxiliary.
- The protection parameters for configuring the tripping behavior on the 5TY1 COM ECPD

Note

Not all alarms are activated by default.

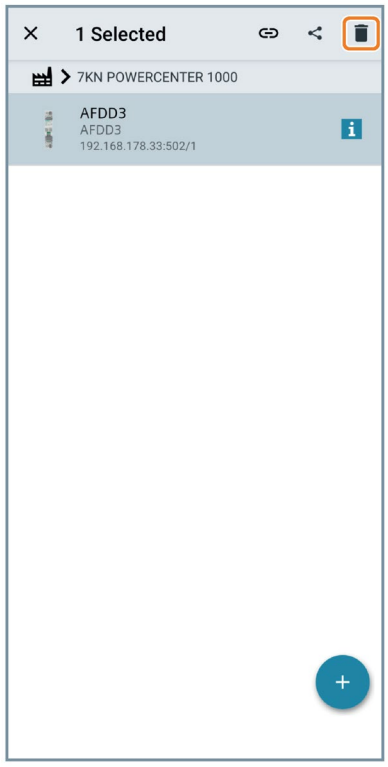
Once the parameters have been changed, it is important to save these to the device. If it is necessary to check which parameters are current in the device, the parameters must be downloaded so that the values in the project are overwritten.

5.4 Removing devices

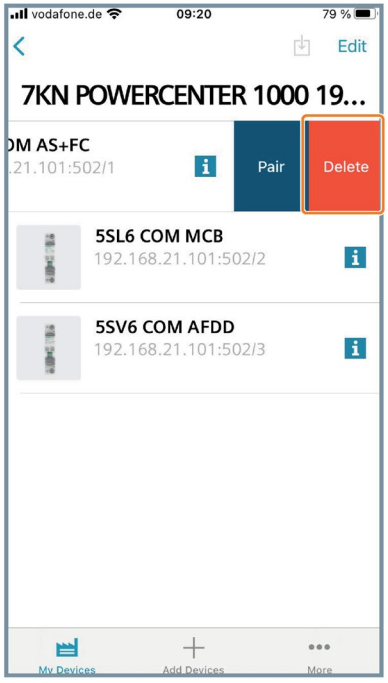
5.4.1 Delete

Added devices can be deleted from the list view of the project in the software. In the app, this can only take place in the project view via the gear icon to the right of a SENTRON Powercenter 1000/1100/2000. This means that this can no longer be displayed in the project. If the SENTRON Powercenter itself is selected, the devices continue to be paired and are displayed in the list of connected devices. To disconnect a subordinate terminal device from the Powercenter, the unpair command must be sent via the device options (see Unpairing (Page 56)). Alternatively, a terminal device can be unpaired with a long button press (≥ 10 s).

If a device has been deleted, there is no need to rescan it. Selecting it in the SENTRON Powercenter view of paired devices is sufficient. This device is then displayed in the project view once again.



Android



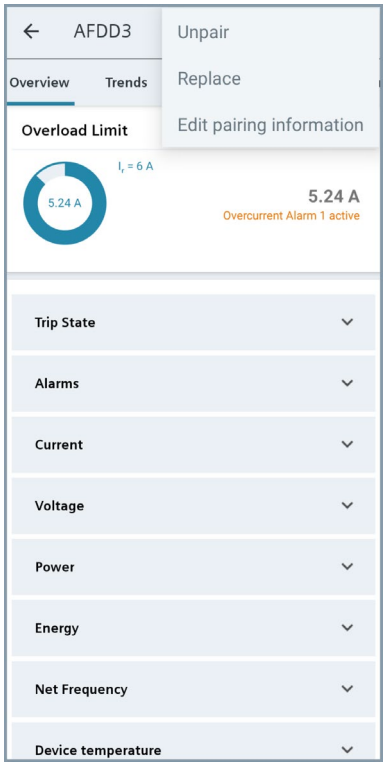
iOS

5.4.2 Decouple

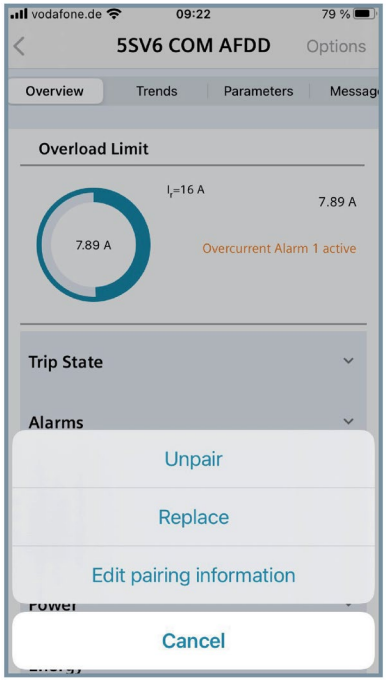
The Unpair function can be used in the detailed view of the individual devices. This causes the terminal devices to be unpaired from the SENTRON Powercenter 1000/1100/2000, similar to a long button press on the terminal devices. To ensure that both the terminal device and the Powercenter 1000/1100/2000 are unpaired on both sides, both devices must first be switched on and communicating with each other. This applies both for the command via the app and for the button press.

Example 1: If the terminal device is unpaired using the app when it is switched off, the Powercenter 1000/1100/2000 will "forget" the terminal device. Following a restart, however, the terminal device will attempt to reconnect to the Powercenter 1000/1100/2000 and then returns a communication error. A long button press must then be performed on the terminal device.
Example 2: If the button on the terminal device is pressed for ≥ 10 s while the Powercenter 1000/1100/2000 is switched off, the Powercenter will continue to search for the terminal device following a restart and to display it in the list. The terminal device must then be removed in the app.

A terminal device that has been unpaired will no longer be displayed in the list of connected devices of the Powercenter 1000/1100/2000. In the app's project list, which can be accessed via the gear icon, the device is still displayed and can either be re-paired or simply deleted.



Android



iOS

5.4.3 Replace

In addition to unpairing, the Replace function can also be selected in the detailed view of the individual devices. To do so, a new device of the same type must be scanned, which then replaces the current devices. In addition, the old device is removed from the radio network, the new device is added, and the parameters included in the app project at this time are transferred to the new device. If the device to be replaced is no longer communication-capable and the last parameters are not known to the project in the app, then only the default parameters are used.

The Replace function only works if the same type of device is scanned and SENTRON Powercenter 1000/1100/2000 is online. If the new device has already been added to the project, it must be deleted if the Replace function is to be used.

For the 3NA COM fuse there are different possibilities available to replace the device. On the one hand, only the fuse link can be replaced by inserting a fuse link with the same rated

current together with the previously paired electronic module. A change in the software is then no longer necessary.

Note

If another rated current is used, the system must be adjusted to the new rated current and the new rated current must be set in the software.

If it is only the electronic module or the electronic module and the LV HRC fuse link being replaced, the Replace function in the software can be used by scanning the new Data Matrix Code.

5.4.4 Change communication information

The third function, which can be selected in the device detailed view is changing the communication or pairing information. Here, the MAC address or the installation code can be adapted as long as the devices have not yet been paired with the SENTRON Powercenter 1000/1100/2000. This may be necessary if the information was entered manually and an error occurred, whereby pairing is not possible.

Similarly, the IP address can also be changed if a SENTRON Powercenter 1000/1100/2000 is added manually. This can be useful if the Powercenter was added offline, for example.

5.5 Special features of the 3NA COM fuse

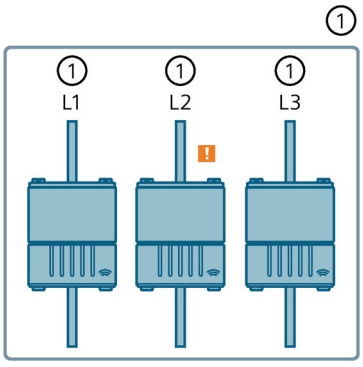
If several fuses are added, these are displayed together in the app. This is referred to as "Device Group".

In order to summarize fuses in a device group, the plant identifier of the devices must match. The respective installation position / phase should be specified for each fuse. As soon as the plant identifier no longer matches, the devices are no longer displayed as a device group.

Note

A name can be given when adding the fuses. If this is not done, the default designation of the devices remains. The unnamed devices are also summarized.

The representation in the app includes the number of grouped fuses (2 to max. 3 pieces), the status (connected or not connected) and a possible indication of at least one present alarm.



① Line

If a red circle is displayed in the overview, the rated current of the fuse link is not known to the project and/or the electronic module. This problem can be resolved by saving the order number of the fuse link in the parameters.

Note

If the rated current is not known to the electronic module, no alarm can be generated if the upper limit for the current is violated.

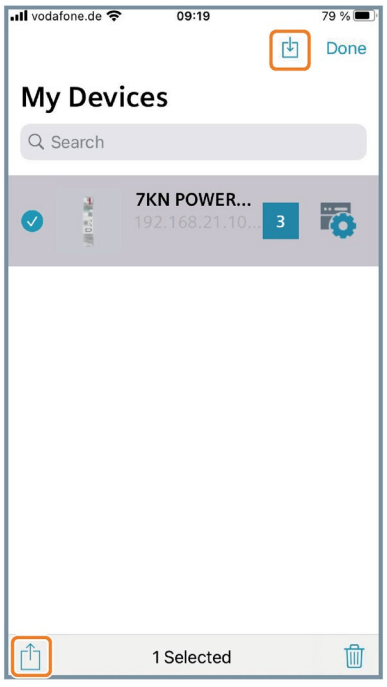
5.6 Import and Export

Several devices can be added in SENTRON Powerconfig mobile and displayed in a project. If it is necessary to summarize devices in different projects, it is recommended to export the .splx file to the mobile device for each project after commissioning. Several projects can be stored with different names in this manner and can be imported again at a later time.

During import, it must be ensured that the imported devices do not overwrite the existing ones. If only the imported project is to be displayed, it is recommended to export the existing project and then delete the devices. Alternatively, the different devices can also be distinguished with a specific name.

The PC version of SENTRON Powerconfig must be used to get an overview of different projects or to move devices to different projects. The mobile app only supports a listing of all added devices.

Android



iOS

5.7 Commissioning several Powercenter 1000/1100/2000 devices

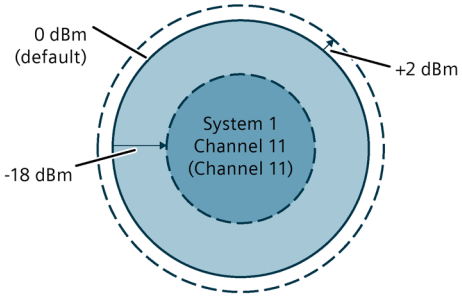
5.7.1 Automatic radio channel selection

Note

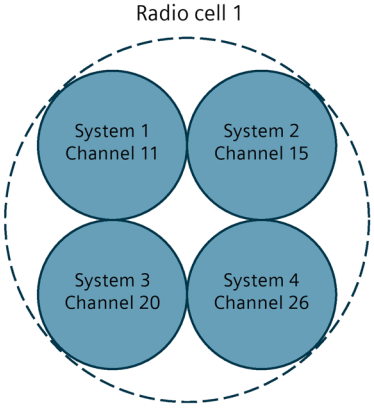
Only qualified personnel are permitted to install, commission or service the devices.

It is recommended to operate a maximum of four SENTRON Powercenter 1000/1100/2000 devices simultaneously in order to avoid overlaps. Additional data transceivers can be used by increasing the distances between the devices (or reducing the signal strength) so that the devices do not disturb each another. It makes sense to distribute all communication-capable circuit protection devices as equally as
possible between the various data transceivers.

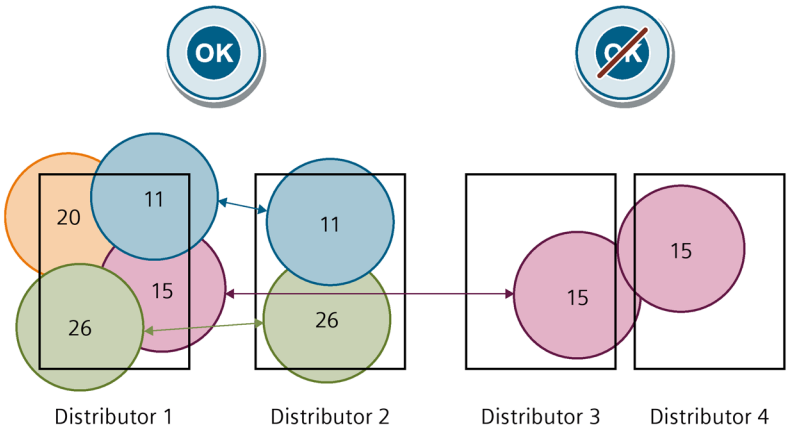
The signal strength must be set in both the SENTRON Powercenter and the associated terminal devices. This can be set between -18 ... +2 dBm.



In the used frequency band between 2400 MHz and 2483.5 MHz there are 16 individual channels (11-26) with separate bandwidths. Each Powercenter independently selects the channel with the lowest capacity utilization. The selected radio channel is visible in the parameters. The following four channels can be automatically selected: 11, 15, 20 or 26.



If only one Powercenter is used per radio channel, the devices will not disturb each other. If several Powercenter devices are required however, interference between these systems is possible. In the worst case, this entails the loss of data in the radio connection. The maximum number of Powercenter 1000/1100/2000 devices depends on the utilization of the radio channel, the ambient conditions and the types of lower-level terminal devices. Normally up to 4 Powercenter systems each with 24 5ST3 COM auxiliary switches/fault signal contacts are capable of operation, as these devices generate a low volume of data. In the case of devices with a large volume of data, such as the 5SV8 COM RCM, only one maximum configuration with 24 devices is recommended. If additional systems are required despite this, the distance between them must be increased (> 10 m) or the systems must be isolated accordingly.



Note

A specific sequence must be observed during commissioning so that not all Powercenter 1000/1100/2000 devices transmit radio signals on one channel simultaneously, thus putting too much strain on the channel and causing data to be lost. Because the greater the number of radio nodes, the greater the risk that individual data packages from the different nodes will be lost.

During the entire commissioning process, all Powercenter 1000/1100/2000 devices and the associated circuit protection devices can either be switched all at once or sequentially. Channel selection takes place as soon as the first communication-capable circuit protection device is paired with the SENTRON Powercenter. All of the devices can be added to the app when switched off, only then is the sequential switching on of the terminal devices required and commissioning can be shortened by pairing 24 terminal devices at the same time.

The following steps should be followed in sequence:

1. Switch on all SENTRON Powercenter devices
2. Switch on the circuit protection devices that are paired with the first Powercenter. The fewer other, unpaired circuit protection devices are active, the faster the initial pairing process will be.
3. Pair the circuit protection devices with the SENTRON Powerconfig mobile app.
4. Once all devices for the first Powercenter 1000/1100/2000 have been successfully paired, they must be left in operation during the next step so that the previously busy channel does not appear to be free/unused for the next data transceiver.
   Recommendation: Restart the devices that have just been paired so as to ensure reliable connection to the wireless network.
5. Only now should the next group of communicative circuit protection devices be switched on with a view to pairing them with the second SENTRON Powercenter 1000/1100/2000.

Repeat steps 2 to 4 until all devices have been paired with the various SENTRON Powercenter devices.

Note

Due to the conditional disconnection possibility of 3NA COM fuses and 5ST3 COM auxiliary switches/fault signal contacts and the 3RV2 COM wireless auxiliary and signaling switch, it is recommended to pair these with the first Powercenter. If necessary, an additional switch must be placed for the power supply of the auxiliary switch.

5.7.2 Manual radio channel selection

As of Version 2.0 of SENTRON Powercenter 1000 or with Powercenter 1100/2000, it is possible to switch off automatic radio channel selection via the parameters. As a result, it is necessary to make a manual selection between channels 11-26. This setting must be made before the first terminal device is paired. Once a subordinate terminal device has been paired with the SENTRON Powercenter, the radio channel will not be changed on the device even if a different setting is stored. If a different radio channel is required, all terminal devices must first be unpaired. This function is supported for all terminal devices as of Version 2.0. Older device versions can only be paired on the 4 standard channels.

Important:

- Radio channel selection must take place before the first terminal device is paired
- Manual radio channel selection is possible only for devices as of Version 2.0

Manual radio channel selection makes it possible to operate a larger number of SENTRON Powercenter devices simultaneously. The exact number depends on the real ambient conditions (e.g. interference with WLAN). Before selecting the channel, it is recommended that the capacity utilization of the radio channels be determined by means of spectrum analysis so that the smooth transmission of data can be ensured. It is recommended that a radio spectrum analysis be carried out so that the radio channels having the lowest capacity utilization are selected. The commissioning of several systems must be carried out in a particular sequence as described in the section Automatic radio channel selection (Page 60).

See also

Firmware update (Page 115)

5.8 Time-Outs

5.8.1 Reclosing

All subordinate circuit protection devices automatically reconnect to their Powercenter after they are switched on.

The more device to be connected, the longer the wait time.

5.8.2 Pairing

The simultaneous pairing process of multiple circuit protection devices with one SENTRON Powercenter takes place sequentially inside the device. Due to the increased data volume, the pairing of 24 terminal devices can take longer compared to a single device.

During the pairing of one or several devices, a pairing timeout can be displayed in the app after 60 seconds. However, the devices will continue (unlimited) to try to pair even after this timeout provided the process is not terminated by the software.

5.8.3 Unpairing

As with the pair command, the unpair command is followed by a timeout of 60 s. If this is exceeded, the SENTRON Powercenter will attempt to unpair the terminal device indefinitely.

If the operation is still not possible, e.g. because the terminal device is irreparably damaged or no longer available, the unpair operation can be terminated, causing the device to be removed from the Powercenter without the knowledge of the terminal device. The terminal device will display a communication error if it becomes available again, as no response will be received from the associated Powercenter.

5.9 Use of third-party software

Both the SENTRON Powerconfig, SENTRON Powerconfig mobile and the SENTRON circuit protection devices with communication and measuring function use third-party software licenses.

The OSS licenses of Powerconfig are displayed via the Info and Help menu items. You can find the OSS licenses of the SENTRON circuit protection devices here (https://support.industry.siemens.com/cs/de/en/view/109797242).

Functions

6

The SENTRON circuit protection devices with communication and metering function offer different functions depending on the respectively recorded measured values and setting options.

6.1 Recorded measured values and storage

6.1.1 Measured value acquisition

The measured values listed below are recorded by the SENTRON COM system. They are then displayed in the device overviews of the SENTRON Powerconfig mobile app, for example. Not all device types support all measured values. See the section Data points and Modbus registers (Page 89) for a detailed list of the measured values and parameters supported by the different device types.

- Temperature (incl. mean value)
- Current (incl. mean value and maximum value)
- Voltage
- Line frequency
- Apparent, reactive, active power and power factor
- Reactive, active energy
- Residual currents in several frequency ranges
- Switching status or switching status of the attached main device
- Status of the inputs/outputs
- Operating hours
- Operating hours with load current
- Mechanical operating cycles
- Number of short-circuit tripping operations
- Number of tripping operations in general
- Number of test executions
- Status for ARD function
- Status of test execution
- Detection of trip cause

Measured values are displayed in the software as invalid, if they are not received for a specific period of time.

All pairable terminal devices also have a value specifying the radio received signal strength (RSSI). This indicates the quality of the radio communication with the SENTRON Powercenter 1000/1100/2000. If the value is greater than -90 dBm (e.g. -60 dBm), a stable connection can be assumed. At values below -100 dBm, dropouts and interruptions can occur.

6.1.2 Accuracy

The accuracy and measuring range of the individual measured values with a reference temperature of 23 °C are described as follows:

Measured value	5ST3 COM, 3RV2 COM, 5TT4 COM DIDO	5SL6 COM MCB, 5SV6 COM AFDD	3NA COM	5TY1 COM ECPD	5SV8 COM RCM
Temperature	±2 °C from -25 °C ... 100 °C	±2.5 °C from -25 °C ... 100 °C	±2.5 °C from +20 °C ... 120 °C	±2.5 °C from -40 °C ... 100 °C	±2 °C from -25 °C ... 100 °C
Current	---	0.5% of 0.02 ... 2 x I_n	2% of 2.5 A ... < 8 A and 1% of 8 A ... 440 A[1)]	±0.5% from 2.5 A ... 1.2*I_n	---
Voltage	---	0.5% at U_n and 1% of 0.9 ... 1.1 x U_n	---	±0.5% from 85 ... 275 V AC	---
Line frequency	---	0.5% of 45 Hz ... 60 Hz	---	±0.5% from 48 ... 52 Hz	---
Power values	---	1% at 0.9 ... 1.1 x I_n and U_n	---	±1% at 1.6 A ... 1.2*I_n and 85 ... 275 V	---
Power factor	---	±0.1 of -1 ... 1	---	---	---
Energy	---	1% at 0.9 ... 1.1 x I_n and U_n	---	---	---
Residual current	---	5SL6 COM RCM version: ±15% of 3 ... 3000 mA	---	±1% of 5 ... 50 mA	± 10% in the range 0.5x ... 5x I_{dn}

[1)] Reference temperature here 25 °C relative to mean value

The accuracy classes are in accordance with the IEC 61557-12, IEC 62053-22 and IEC 62053-23 standards.

6.1.3 Measured value transmission frequency

The measured values are transmitted to the SENTRON Powercenter 1000/1100/2000 on different transmission frequencies.

This leads to the fact that not every measured value is updated equally as fast as in the software.

The following measured values are transmitted every x seconds:

- Temperature: 2 s
- Temperature mean value: 60 s
- Current: 2 s
- Current mean value: 2 s
- Current maximum value: 60 s
- Residual current (all measurement channels): 2 s
- Voltage: 60 s
- Line frequency: 60 s
- Active, reactive and apparent power: 2 s
- Power factor: 60 s
- Active and reactive energy: 60 s
- Operating hours counter with/without load current: 60 s
- Operating cycles counter, test execution counter: 10 s and in the event of a change
- Counter for tripping operations: 60 s and in the event of a change
- Number of short-circuit tripping operations: 60 s
- Switching status: 10 s and in the event of a change
- Alarm status: 60 s and in the event of a change
- Radio RSSI: 60 s

6.1.4 Saving measured values in the SENTRON Powercenter 1000

The different measured values are stored in the SENTRON Powercenter and can be displayed in the trends of the respective devices in SENTRON Powerconfig mobile (not via Bluetooth®). A distinction can be made between the following trends depending on whether the aforementioned measured value is supported by the respective device.

Stored measured value	Storage duration	Interval	Representation type
Temperature mean value	1 hour	1 minute	Line diagram
Temperature mean value	7 days	15 minutes	Line diagram
Current mean value	1 hour	10 seconds	Line diagram
Current mean value	7 days	15 minutes	Line diagram
Imported active energy	7 days	15 minutes	Line diagram
Imported active energy	30 days	1 day	Bar diagram
Voltage min/max	10 days	1 day	Bar diagram
Line frequency min/max	10 days	1 day	Bar diagram
Active power min/max	10 days	1 day	Bar diagram
Apparent power min/max	10 days	1 day	Bar diagram
Temperature min/max	10 days	1 day	Bar diagram

As of Version 2.0, the stored measured values can be adjusted individually for each trend. The storage duration and the intervals remain unchanged.

6.1.5 Storing measured values in the SENTRON Powercenter 1100/2000

The measured values from the connected terminal devices are stored separately for each device in the SENTRON Powercenter 1100/2000. This provides enhanced flexibility. The measured values stored in the historic trends can be adjusted.

The default setting is:

		Supported device					
Stored measured value	**Trend type**	**5ST3 COM AS+FC, 5ST3 COM RCA, 3RV2 COM, 5TT4 COM DIDO**	**3NA COM fuse**	**5SL6 COM MCB with EM, 5SV6 COM AFDD**	**5SL6 COM MCB with RCM**	**5TY1 COM ECPD**	**5SV8 COM RCM**
Temperature	Minimum, maximum and mean value for the last 19 days	✓	✓	✓	---	✓	✓
Current		✓	✓	✓	✓	✓	---
Voltage		---	---	✓	✓	✓	---
Active power		---	---	✓	✓	✓	---
Apparent power		---	---	✓	✓	✓	---
Residual current low pass		---	---	---	✓	✓	✓
Residual current base frequency		---	---	---	✓	---	---
Special trends:							
Mean current	Last 1 hour at 10 s intervals	---	✓	✓	---	---	---
Active energy export	30 days at 1 day intervals	---	---	✓	✓	---	---
Active energy import	30 days at 1 day intervals	---	---	✓	✓	---	---
Residual current low pass	Snapshot 3 min before and 3 min after alarm at 2 s intervals	---	---	✓	---	---	---

6.1.6 Special considerations relating to power factor

The sign of the power factor and the counting of the exported or imported energy are dependent on the set and physical direction of incoming supply.

The rms value of the current is measured even if the current curve does not exhibit true sinusoidal behavior. In this case, the standard relationship ($S^2=P^2+Q^2$) between apparent, reactive and active power cannot be used.

6.1.7 Special considerations relating to energy counters and direction of incoming supply

When devices feature a settable direction of incoming supply (5SL6 COM miniature circuit breaker and 5SV6 COM arc fault detection device), the actual direction must be entered as the settable direction. The default setting is: infeed from top to bottom. The correct setting is necessary for the leading sign of the power factor and the energy counters.

If the physical incoming supply is from above, the intrinsic consumption of the device is also counted in the energy counter.

The threshold value from which the energy counter starts to accumulate is 1.5 Wh or 1.5 varh.

The energy counters can only be reset together.

6.2 Residual current measurement (RCM)

Residual current measurement, also called the RCM function, is supported by some SENTRON COM circuit protection devices.

6.2.1 5SL6 COM miniature circuit breaker with RCM function

The 5SL6 COM miniature circuit breaker with RCM function corresponds to the IEC 62020-1 standard. This is a type F device and determines sinusoidal residual currents (AC) up to 100 kHz and residual currents from pulsating DC current. The measuring range is between 3 mA and 1000 mA for AC residual currents or between 3 mA and 300 mA for pulsating DC residual currents.

The measured value of the residual current is measured in several frequencies simultaneously and distributed over the following measurement channels:

- Line frequency (50 Hz)
- Harmonic of line frequency
- Low-pass - AC
- Low-pass - AC and pulsating DC (also referred to as "RMS", i.e. AC and DC combined)
- Band-pass
- High-pass

All ranges of the measurement channels can be set except for the base frequency, which is determined by the device itself. You will find more detailed information about setting options in Chapter RCM measured values and parameters.

By subdividing the residual current into different frequency ranges, it is possible to identify different error causes, such as defective insulation and humidity in the low frequency range or electromagnetic interference at high frequencies.

The two low-pass channels also have a configurable alarm and pre-alarm, including threshold value, hysteresis, ON and OFF-delay. Here, the pre-alarm is set as a percentage of the main alarm.

A general ON-delay of the RCM alarms after a restart of the device can also be set, for example to wait until a motor has ramped up before the measurement or alarm is once again active.

In addition, the automatic resetting of alarms can be switched off if the measured value is below the threshold value, so that an RCM pre-alarm / alarm can be confirmed only by a button press or via a remote command. This is useful so as not to miss an upper limit violation of the RCM measured value.

Here, too, all setting options can be found in RCM measured values and parameters.

6.2.2 5SV8 COM residual current monitors

The signal evaluators and associated transformers can be combined in accordance with IEC 62020-1 as Type A or F (sinusoidal alternating current, pulsating alternating current) or as Type B (sinusoidal alternating current, pulsating alternating current, pure and pulsating direct currents and alternating currents up to 2 kHz).

For the Type A devices, the RMS value is captured and output for each channel. For the Type B devices, AC, DC and RMS values (= AC + DC) are captured and output for each channel. The filter frequencies of the measurement channels can be configured.

The devices are equipped with one or two changeover relays for pre-alarm/alarm output depending on type. The relays can be configured to match the device. Certain variants also have two digital outputs DO and one digital input DI available to be configured.

Warning thresholds, startup delays and ON delays can also be configured. Alarms can be configured on a channel-dependent basis to be reset automatically or by a button push or COM command.

The setting options vary from device to device and are set out in the Modbus register table (Page 84).

6.2.3 5TY1 COM electronic circuit protection device (ECPD) with RCD and RCM function

In addition to the residual current protection function (RCD) in line with IEC/EN 61009-1 (IEC/EN 62423), the 5TY1 COM electronic circuit protection device (ECPD) includes a residual current monitoring function (RCM) in line with IEC 62020-1.

This is a type F RCM device and detects sinusoidal residual currents (AC) up to 1 kHz and residual currents from pulsating DC current. The RCM measuring range is between 3 mA and the RCD tripping threshold. See the Modbus register table (Page 84) for the settable parameters.

6.3 Messages

6.3.1 Measured values and upper limit violation

Circuit protection devices with measuring function detect many statuses. Some of these statuses are stored directly in the device and can be read out using the "Messages" tab in SENTRON Powerconfig. Up to 126 messages can be stored per device. After this, the oldest entries are overwritten. Each message is tagged with the time stamp of the device (system time can be set on the Powercenter). In some cases, additional message details are displayed in the software.

The messages listed below based on measured values are available. Whether a message is available or can be set for a particular device type depends on whether the measured value is available. For more information on this subject, see the section Measured value acquisition (Page 65).

Description	Default alarm setting	Note
Upper limit violation of operating hours with load current	Not active	
Upper limit violation of operating hours	Not active	
Upper limit violation of number of mechanical operating cycles	Not active	
Upper limit violation of number of tripping operations	Not active	
Upper limit violation of number of short-circuit tripping operations	Active	
Upper limit violation of device temperature	Active	The average temperature is considered here
Upper current limit violation, alarm 1	Active	
Upper current limit violation, alarm 2	Not active	
Lower current limit violation, alarm 1	Not active	
Lower current limit violation, alarm 2	Not active	
Upper voltage limit violation, alarm 1	Not active	
Upper voltage limit violation, alarm 2	Not active	
Lower voltage limit violation, alarm 1	Not active	
Lower voltage limit violation, alarm 2	Not active	
Lower voltage limit violation, AFDD trip	Active	The base line is the measured voltage value, which according to the standard is fixed at a constant 195 V with a hysteresis of 10%.
Upper limit violation of RCD test counter	Not active	
Upper limit violation of residual current RCM AC pre-alarm	Not active	
Upper limit violation of residual current RCM AC alarm	Not active	
Upper limit violation of residual current RCM RMS pre-alarm	Active	
Upper limit violation of residual current RCM RMS alarm	Active	
Upper limit violation of residual current RCM DC alarm	Not active	
Upper limit violation of residual current RCM DC pre-alarm	Not active	
Upper limit violation of number of delayed tripping operations	Active	

Note

Not all alarms are activated by default. All alarms can each be switched on or off.

The respective alarms can be activated or even deactivated. A message is not displayed if they are deactivated and the device LEDs do not flash according to the pattern described above (see the chapter LED signaling (Page 47)). Furthermore, there are adjustable threshold values that generate messages when they are exceeded. In addition, a hysteresis value can be set for the alarms for current, voltage and temperature. An alarm is activated if a threshold value is exceeded. If the measured value drops below the threshold value including the set hysteresis, the alarm status is exited again. As of firmware version 1.1.0, exiting an alarm when the limit is no longer exceeded is also stored as a message.

In order to avoid an unnecessary flood of messages and the loss of important messages, the limits for the alarms must be set in an expedient manner according to the application.

For measured values relating to service life (e.g. operating cycles counter, operating hours, number of tripping operations), an alarm status that has been reached can only be left if the threshold value is increased or the alarm is deactivated after the device has been tested. If it is no longer possible to ensure that a device is in perfect operating condition (e.g. visible burns after too many short-circuit trips), it is recommended to replace the device.

The parameters that are available with the different units, value ranges and default settings are described in the section Data points and Modbus registers (page 101).

6.3.2 Further messages

The messages listed above are based on measured values and their limit violations. Statuses also exist which cannot be set and are stored as messages.

- Change of device time setting
- Reset of the energy counters
- Different statuses of a firmware update
- DHCP network error
- Device restart
- Error involving summation current transformer
- Status relating to thermal protection shutdown
- Change of MQTT client service
- Confirmation of a tripping operation
- Alarm has been activated/deactivated
- Device switched on/off by manual operation
- Device switched on/off by remote control
- Switching operation
- Setting and status of the ARD function

- Protected parameters on the ECPD have been changed
- Tripping operation detected (see next section)

6.4 Tripping operations in the event of a fault

The circuit protection devices with measuring and communication function have different tripping functions/protection functions. These protection functions are independent of the communication function, i.e. the electromechanical devices continue to provide protection even if there is a communication failure.

The following trip causes are detected and stored in the internal memory. Up to 100 tripping operations are stored. The trip messages are displayed in the SENTRON Powerconfig app/PC version on the "Messages" tab together with the entries listed above.

Trip cause	AS+FC, 5ST3 COM RCA	5SL6 COM MCB, 3RV2 COM	5SV6 COM AFDD	3NA COM fuse	5TY1 COM ECPD
Attached device has tripped (reason unknown)	✓	---	---	---	---
Manual/mechanical shutdown	✓	✓	✓	---	✓
Overload (thermal tripping)	---	✓	✓	---[1)]	✓
Short-circuit	---	✓	✓	---[1)]	✓
Arcing faults	---	---	✓	---	---
Overvoltage	---	---	✓	---	✓
Test tripping operation	---	---	✓	---	✓

[1)] The protection function is provided, but the communication function does not send a trip message

Note

Short-circuit detection in 5SL6 COM and 5SV6 COM

In the case of rapidly rising short-circuits or a reconnection to an existing short-circuit, the short-circuit is not detected by the measuring function. In these situations, the integrated miniature circuit breaker mechanically trips the device so quickly that there is no entry in the messages, there is no alarm and no trip counter is activated.

Note

Short-circuit detection with 5TY1 COM

As the ECPD switches off ultrafast in the event of short-circuits, the RMS value does not yet reflect the short-circuit current value. Depending on the magnitude of the current, the displayed tripping value may be lower than the I_{max} value that has been reached.

The 5ST3 COM auxiliary components communicate the status of the attached device even when the device is switched off. They distinguish between a manual shutdown and a tripping operation due to error. The trip cause is not detected.

The 3RV2 COM wireless auxiliary and signaling switch for motor starter protectors distinguishes between a manual shutdown and a trip caused by short-circuit or overload. The trip cause is detected and can be output. The external power supply means that communication is possible even with the operating lever in the OFF position.

Communication is not possible if the 5SL6 COM miniature circuit breaker and 5SV6 COM arc fault detection device are switched off. If the device is switched off manually, the operating cycles counter is incremented. If the device trips, both the operating cycles counter and the trip counter are incremented. In addition, a message containing more detailed information including the reason for the trip operation and the time is generated. If a trip is detected, it must be confirmed by pressing the button briefly when the devices are reclosed. From version V1.1, the switching status is displayed.

It may happen that a trip message or the change of switching status is not transmitted or received by the SENTRON Powercenter in time before the 5SL6 COM miniature circuit breaker or 5SV6 COM arc fault detection device are switched off.

In order to monitor a trip message or the switching status of the 3NA COM fuse, a commercially available external fuse monitoring system must be installed via an additional device. If the fuse element has tripped, communication can no longer take place and the fuse itself indicates this via a front indicator. The electronic module does not distinguish whether there is a disconnection of faults, a power failure or the deactivation of a load. In any case, the electronic module reports the "Connection disconnected" status.

6.5 Test execution and memory

The execution of test functions is recorded in a further memory area. Up to 60 test entries are stored. They are displayed on the "Test" tab in SENTRON Powerconfig. Here, an entry is created for each test execution and includes the result and the time stamp, among other information. It is possible to export the test results. Regular, internal self-tests of devices (e.g. by the 5SV6 COM AFDD) are only documented in the event of a fault.

The following device tests are stored for each device:

5SL6 COM miniature circuit breaker with RCM function

RCM test:

An internal residual current is simulated here. The internal measuring functions are tested, as is the associated LED flashing when an alarm limit is exceeded. The set parameters for rise and fall delay are not considered in this case.

5SV8 COM RCM residual current measuring devices

RCM test:

An internal residual current is simulated here. The device display indicates the fault accordingly (LED or display). The relays and digital outputs are able to switch, depending on the configured assignment.

Relay test:

It is possible to test the function of the relays present. The relay switches to the defined state for 60 s when the command is sent. No entry is created in the memory for this test. This is simply a manual test of relay output function.

5TY1 COM electronic circuit protection device (ECPD) with RCD function

An internal self-test is started here which tests internal functions and ensures that the device is fully functional. An internal RCD test is also performed by introducing a test signal into the RCD circuit to check whether it is detected. Depending on the test trigger (app, test button, cyclic test), the device will either switch to the OFF state after the test or remain ON. Test results are stored in the relevant test area where they can be viewed by the customer.

5ST3 COM remote control auxiliary with RCD test function

RCD/IR test:

A test procedure normally includes an RCD test and an insulation resistance test (= IR test). Each can be disabled and parameterized individually. The two tests are only available if an RCD, RCBO or RC unit is set as the attached device.
For the RCD/FI test, the correct RCD (30 mA, 100 mA, 300 mA selective or non-selective) must be set. The comparison resistance value for the IR test is defined at the same time. For the IR test, the number of poles must also be set if the IR test is to be carried out.

Note

The IR test is deactivated by default. The IR test is performed at < 2 mA at a rated voltage in accordance with IEC 63024.

The following test results are logged:

- Time of day
- RCD test result
- Set RCD type
- RCD test voltage
- Tripping time and tripping current
- IR test result
- Set resistance value
- Set number of poles
- Insulation resistance values.

Note the following:

Note

- A stand-alone IR test, not following an RCD test, can only be started in the switched-off status. As a result, if an MCB is attached, the switch must first be turned off before a (cyclic) test can be performed.
- An IR test is performed after every tripping operation of the mount-on device unless the IR test is disabled.
- After a successful test execution, the device is switched on again. If an IR test fails, the system must first be checked, the error message reset and the switch turned back on again manually (via the lever or remote switching). The ARD function are not possible in this situation. An IR test error occurs if the measured resistance Rd is below the requirement for the value Rd0 in the IEC 63024 standard (8000 Ω at 30 mA RCD; 2500 Ω at 100 mA RCD; 800 Ω at 300 mA RCD).
- An IR test warning occurs if the measured resistance is below the setting Rd but not yet below the requirement Rd0 in the standard. This improves system safety. After a warning, the device can be switched on remotely, or automatic reclosing (ARD) may be possible depending on the configuration.

An RCD/IR test can be set and executed individually or automatically (cyclically).

Note

The system time of the Powercenter 1000/1100/2000 is used when the test is performed cyclically. It is strongly recommended to configure a time server to ensure that the time is set correctly even after an outage. For more information on this subject, see the section Time synchronization (Page 83).

6.6 Switching command

With devices such as the 5ST3 COM remote control auxiliary, an active switching command can be sent. However, if the device is switched off manually with the lever, it must also be switched on again manually or a separate switch-on command must be sent so that a technician on site is not in any danger.

⚠ WARNING

Death or serious injuries are possible

There is dangerous voltage after an external switching command.

Make sure that a technician on site, for example, is not in any danger from an external switching command.

6.6.1 Switching operation with the 5ST3 COM remote control auxiliary

With the 5ST3 COM remote control auxiliary, a switching command can be sent either via the wired interface at the plug-in terminals or via the software and the Powercenter 1000/1100/2000. Both methods are not possible at the same time. The corresponding setting must be made in the configuration software. To prevent commands such as a switching command or a test execution being skipped, they must not be re-sent within 10 s. It takes at least 1 s to execute a switching command.

Note

The remote switching function can be blocked with the yellow slide switch on the remote control auxiliary (positions "RC OFF" or "OFF").

This block prevents remote switching and also test execution. This is necessary especially if secure, restricted access cannot be guaranteed in the network.

A Modbus TCP command is able to switch the device even unintentionally. Make sure that the system is protected against unauthorized access.

In addition to the remote switching function, the remote control auxiliary supports the automatic reclosing function (ARD) after a tripping operation of the mount-on device. This function can be configured: on/off, three delay times for repeated reclosing attempts and a waiting time after which three new attempts will be made. It is also possible to specify whether the device is automatically reclosed after an IR test warning.

The ARD status is displayed directly after an IR measurement. If no IR measurement has been performed because this was unavailable or deactivated, the display of the ARD status is not updated until 5 minutes have elapsed, as it is assumed that the status is now stable.

If the device cannot be reclosed after three or six attempts, the ARD function is blocked and must first be reset by means of a manual switching operation (via the lever or remote switching) or with the yellow slide switch ("RC ON" → OFF → "RC ON").

6.6.2 Switching operation with the 5TY1 COM ECPD

The 5TY1 COM also features a remote switching function for a variety of cases, e.g. reclosing following a fault. In this case, the integrated ARD (automatic reclosing device) function can be activated or a command can be sent to the device.

The device can also be controlled via the integrated digital input (DI) by switching the semiconductor to the conducting or the non-conducting state. The protection functions continue to be active and take priority over the DI in the event of a fault (e.g. short-circuit).

The device can also be tripped to the OFF state by means of a command that causes the mechanical isolating contact to open. After mechanical opening, remote switching is no longer possible. Mechanical reclosing at the device is necessary.

These functions can be activated and deactivated separately. The factory setting for these functions is set to deactivated.

The functions listed here affect the protection behavior of the device and are set by means of parameters. SENTRON Powerconfig refers to this parameter range as "protected parameters". This range can only be set if the range is unlocked using the padlock symbol and the button on the device is then pressed within the specified time. Alternatively, remote switching can be activated in the role of Superuser.

Other parameters, such as rated current etc., can also be set on the 5TY1 COM ECPD. See the Modbus register map (https://support.industry.siemens.com/cs/de/de/view/109973540/en) for a detailed list of all options.

Changes in protected parameters are stored in the 5TY1 COM ECPD and can be read out under "Messages".

6.6.3 Switching operations on 5TT4 COM DIDO

The outputs of the 5TT4 COM digital input/output module can be switched in two ways:

1. Via software (Powerconfig via Powercenter 1100/2000):
   - Each individual output can be forced into a particular state for a settable time (Force function).
   - An active Force command can be extended or canceled at any time via the software.
   - After the defined time has elapsed or if the command is canceled, the output returns to the state defined in the device configuration.
2. Via the front button:
   - A short button press (between 0.3 and 3 seconds) switches the state of the output for a fixed time of 60 seconds (e.g. from "Off" to "On" or vice versa).

Note

A switching command initiated manually via the button cannot be interrupted or changed via the software. Similarly, commands issued using the software must be changed in the software.

6.7 Logic configurations

The 5TT4 COM DIDO module provides different function blocks for flexible processing of the digital inputs (DI1, DI2) and for manipulating the digital outputs (DO1, DO2).

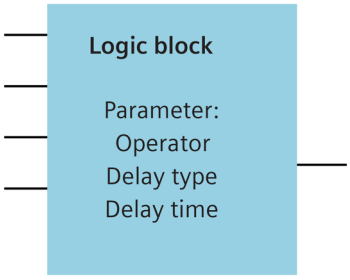
These function blocks make it possible to map complex logic functions directly in the device.

Principle of logic operation:

Each function block has specific inputs which control its behavior. The output signal of one function block can be used as an input signal for other function blocks, thus making it possible to implement versatile logic operations.

6.7.1 Logic operators

The 5TT4 COM DIDO module makes a total of four logic operators available. Up to four input signals can be assigned to each operator.



Configuration options:

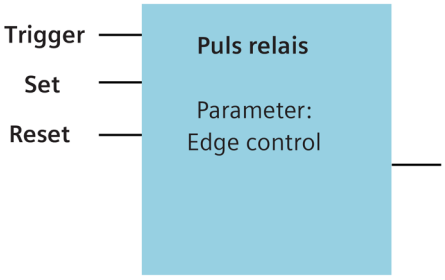
- Delay type: It is possible to define whether the operator reacts to changes in the input signals immediately or whether a configurable ON or OFF delay is active.
- Delay time: The delay time can be set in seconds.

Available operators:

- AND: The output signal is 1 (TRUE) if all the assigned input signals are 1 (TRUE) or if they are not used.
- NAND: The output signal is 0 (FALSE) if all the assigned input signals are 1 (TRUE) or if they are not used.
- OR: The output signal is 1 (TRUE) if at least one assigned input signal is 1 (TRUE).
- NOR: The output signal is 0 (FALSE) if at least one assigned input signal is 1 (TRUE).
- XOR: The output signal is 1 (TRUE) if exactly one assigned input signal is 1 (TRUE).
- XNOR: The output signal is 0 (FALSE) if exactly one assigned input signal is 1 (TRUE).

6.7.2 Pulse relay

The module provides two independent pulse relays.



Each pulse relay has the following inputs:

- Trigger input: Initiates the switching operation.
- Set input: Sets the output signal of the relay.
- Reset input: Resets the output signal of the relay.

Principle of operation:

A parameter can be used to configure whether the pulse relay reacts to the rising edge (change from 0 to 1) or the falling edge (change from 1 to 0) of the trigger input signal.

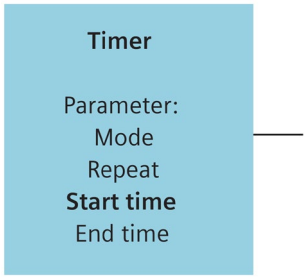
If the set input is active, the output signal of the pulse relay is changed in the event of a signal at the trigger input (toggle function).

Priority:

If the set and reset inputs are active simultaneously, the reset input has priority.

6.7.3 Timer

The 5TT4 COM DIDO module has a total of ten configurable timers.



Each timer can be set independently and four parameters are used to control its behavior:

1. Mode: Defines the operating mode of the timer.
   - Off: The output signal of the timer is 0 at the specified time (FALSE).
   - On: The output signal of the timer is 1 at the specified time (TRUE).
   - Holiday (vacation/random): The output signal changes at random time intervals to simulate presence.
2. Repeat: Defines the days of the week on which the timer should be active.
3. Start time: Defines the start of the active time window for the timer.
4. End time: Defines the end of the active time window for the timer.

6.7.4 Integration of external signals

The data points "External 1" and "External 2" are available for use in the function blocks of the 5TT4 COM DIDO module. These make it possible to integrate additional external signals or statuses in the SENTRON COM system.

Configuration of external signals:

- Via Modbus: The "External 1" and "External 2" data points can be written via Modbus. The available Modbus statuses are described in the section Data points and Modbus registers (Page 89).
- Via the SENTRON Powerconfig software: It is also possible to define the "External 1" and "External 2" data points directly in SENTRON Powerconfig.

6.8 Time switch

Up to three time switch functions can be defined on the 5TY1 COM ECPD. These are set independently. This timer function must first be enabled via the protected parameters.

The following settings must be defined:

- Target status: Should the device switch on (ON) or off (STBY) during the timed switching operation?
- Weekday: On which day(s) of the week should switching be performed?
- Start and end times: Between which times should the target status be switched?

The start and end times of the switching operations are based on the set local device time, which corresponds to the system time of the relevant SENTRON Powercenter 1100/2000. If the system time of the Powercenter is correct (e.g. via SNTP server), no further setting is necessary. Otherwise, the difference between the UTC and the system time can be set, as can the manual or automatic changeover to daylight saving time: DST).

6.9 Time synchronization

The SENTRON Powercenter 1000/1100/2000 can avail of global, cyclic time synchronization via SNTP (Simple Network Time Protocol). This is necessary in order to ensure that trends and messages obtain the correct time stamps. Messages retain the time stamps obtained during generation even if the time changes.

The system time in the Powercenter is displayed in UTC and is adapted to the time zone of the device in the software.

Note

The system time must be synchronized during first commissioning, either once via Powerconfig or regularly via a time server. The latter method is recommended, as the time is automatically resynchronized after the device is switched off. Synchronization via Powerconfig is also possible, but the time is lost when the device is switched off. Time synchronization via an SNTP server is preferred for this reason.

If the SNTP server is selected on the Powercenter, an IP address of a web server must be entered. Routers, the IoT gateway Powercenter 3000 or a time server from the internet can be used as a time server. In the latter case, an existing internet connection is required and the ports must be enabled in the firewall. If the broadcast function is activated on the Powercenter, all network broadcasts are received. A typical SNTP server is the SENTRON Powercenter 3000, but routers or PC systems such as SENTRON Powermanager can also be used.

See also

Equipment Manual - SENTRON Powercenter 3000
(https://support.industry.siemens.com/cs/ww/en/view/109763838)

How do you configure your PC as NTP server?
(https://support.industry.siemens.com/cs/ae/en/view/22144502)

6.10 Modbus TCP connection

The Modbus TCP protocol is based on unencrypted communication. Security measures such as access restrictions must be implemented in the higher-level system/network.

One SENTRON Powercenter 1000/1100/2000 supports up to three Modbus TCP connections simultaneously via the Ethernet interface and one additional Bluetooth® connection in parallel. This means that different software applications would be able to communicate with the data transceiver. This, however, is advised against.

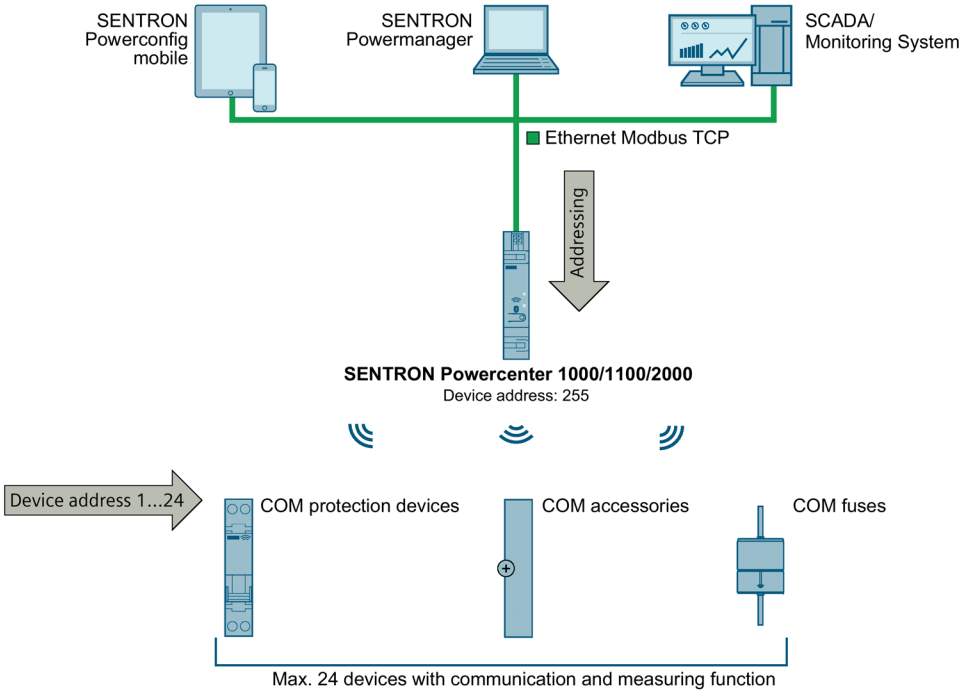
Note

It is recommended to always only use one Modbus TCP connection operatively so that it does not result in an overlap of commands.

Measured values and parameters are requested via Modbus TCP using the relevant register number of the data point.

The correct address must be specified so that the data point is assigned to the right circuit protection device:

1. IP address of the SENTRON Powercenter 1000/1100/2000
2. Device address (or unit ID) of the specific device: 1-4 for the subordinate protection device or 255 for the Powercenter itself.



Registration address	Measured variable	Format	...
0xC00	Temperature	FP32	...
0xC04	Current L1	FP32	...

Detailed overview of the data points and registers for all devices

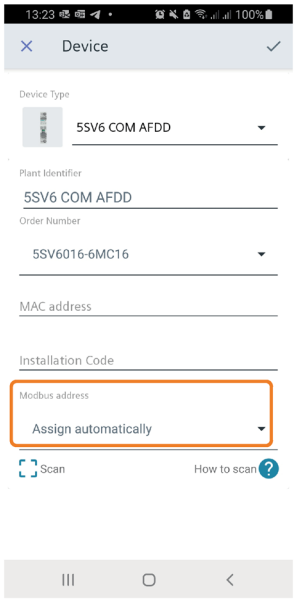
You can find this information online here (https://support.industry.siemens.com/cs/ww/en/view/109973540).

See also

Device addressing via Modbus TCP (Page 85)

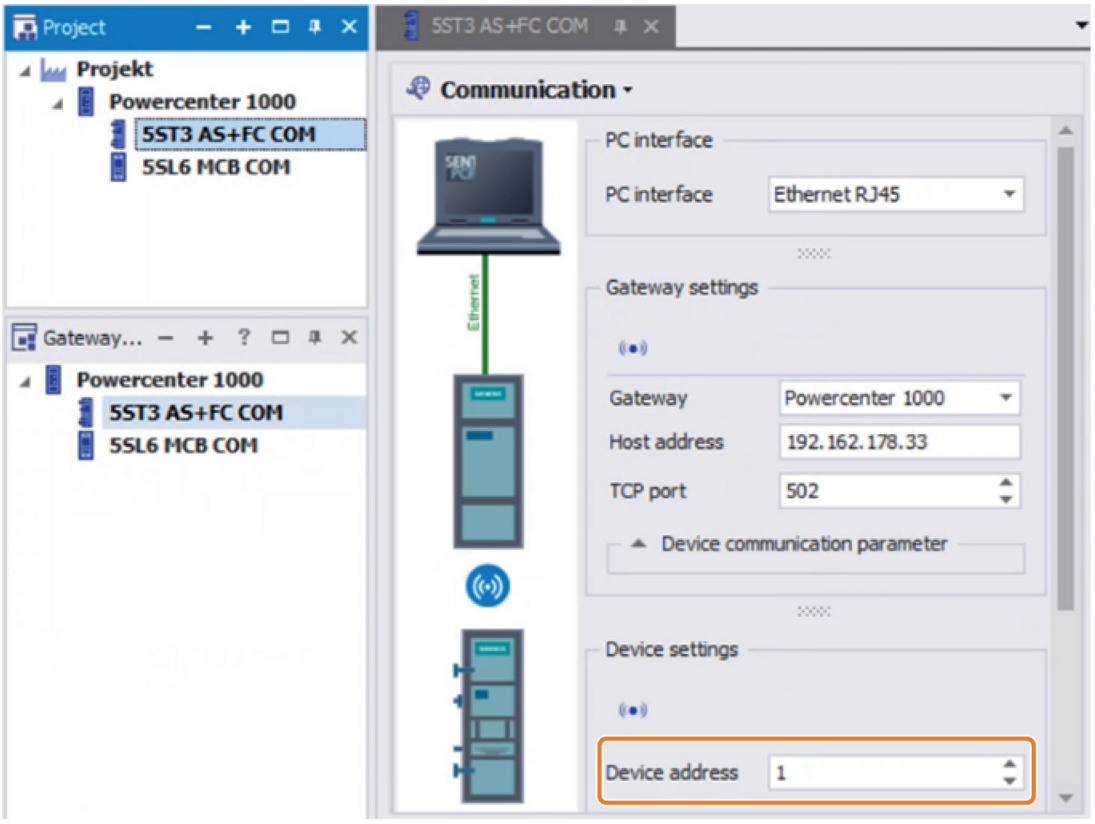
6.10.1 Device addressing via Modbus TCP

In SENTRON Powerconfig mobile, the device addresses are issued consecutively from 1-24 as standard. After a Data Matrix Code of the terminal device has been scanned, the device address can also be selected manually as an alternative.



The device addresses that have been assigned can be displayed in SENTRON Powerconfig mobile in the device list that can be accessed via the gear icon and where new subordinate terminal devices can be added.

In the Powerconfig PC version, the device addresses can be set in the communication view.



The register number for the data point is the same for all devices. The data can be accessed from the different devices via the unit ID or device address.

The device addresses of the communication-capable circuit protection devices including the SENTRON Powercenter 1000/1100/2000 are transferred in the "Unit_ID" (Unit Identifier) field of the Modbus protocol.

Modbus Protocol Header (7 Bytes)				Protocol Data Unit (PDU)	
Transactions Identifier	Protocol Identifier	Lenghtfield	Unit Identifier	Function Code	Data
(2 Bytes)	(2 Bytes)	(2 Bytes)	(1 Byte)	(1 Byte)	(varies)

Modbus TCP/IP Application Data (ADU)
(This information is embedded into the data portion of the TCP frame)

For the information of the SENTRON Powercenter 1000/1100/2000 itself, e.g. its operating hours or the system time, this means that 255 (0xFF) must be entered in the unit ID. The first device is addressed with 0x01. If, for example, a 3NA COM fuse has been added at the first position, a valid voltage measurement value cannot be read out, because this is only supported by 5SL6 COM and 5SV6 COM.

See also

Messaging on TCP / IP Implementation Guide V1.0b
(https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf)

Modbus Application Protocol Specification V1.1b
(https://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf)

6.10.2 Protocol information

Register addressing

According to the Modbus specification the registers are numbered starting from 1 but addressed starting with 0. Subsequently, the start address in the protocol must be decremented by -1 when reading out a register.

Function codes

Read processes (Read = R) are carried out alternatively with the function codes 0x03 or 0x04 according to the Modbus specification.

Write processes (Write = W) take place with function codes 0x06 or 0x10 according to the Modbus specification.

Data formats

The following data formats are possible:

Abbreviation	Description
U8	unsigned 8 Bit
U16	unsigned 16 Bit
U32	unsigned 32 Bit
S16	signed 16 Bit
UCHAR	unsigned Character with x Bytes
FP32	floating point 32 Bit (according to IEEE-754)
FP64	floating point 64 Bit (according to IEEE-754)
TS	time stamp
ST	system time - System time

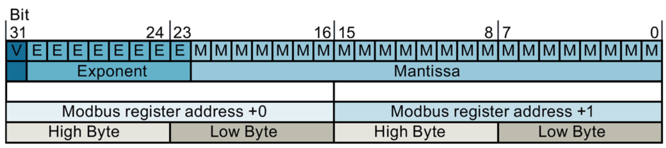
Storage of the time stamp according to the Unix format (UNIX_TS) in seconds since January 1, 1970

Byte arrangement with big-endian data transmission

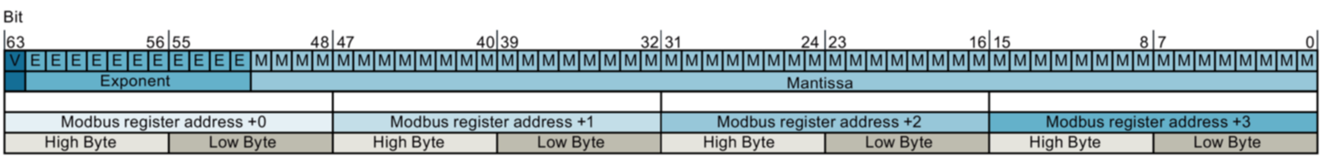
Register		U8	U16	U32	FP32
Register address	High byte	0x00	High data byte	1st data byte	1st data byte (sign bit)
	Low byte	Data byte	Low data byte	2nd data byte	2nd data byte
Register address + 1	High byte	-	-	3rd data byte	3rd data byte
	Low byte	-	-	4th data byte	4th data byte
Number of registers		1	1	2	2

Individual units of information are identified by register addresses. A register is 16 bits in size. If a unit of information is larger than 16 bits, it will require the corresponding number of registers.

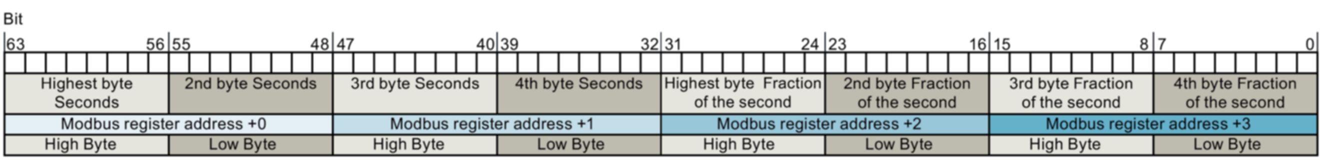
Example of the representation by means of a 32-Bit floating point number FP32 according to IEEE 754



Example of the representation of a 67-Bit floating point number FP67 according to IEEE 754



Example of the representation of a time stamp based on a FP64 number



Invalid values

Due to temporary events, e.g. interruption of supply voltage or communication, it is necessary to check the contents of registers for validity. Invalid measured values are marked as Not a Number (NaN according to IEEE-754). The connection status of a terminal device is stated via the "Device status" data point of the respective device. This is used to conclude whether the communication of the terminal device can be established and thus current values can be read. If validity is important for an application, the measured values must be checked for not equal to "NaN" and the device status equals "3 = connected" before processing. This apples to all 1 - 24 terminal devices.

Intervals

It is recommended to query each device no more than 1x per second. The terminal devices must be addressed individually and should be processed sequentially. The measured values are updated at least every 2 s (see Measured value transmission frequency (Page 67)).

If possible, several registers should always be polled in blocks instead of sending one protocol per register.

6.10.3 Delayed Response and parallel accesses

For many devices there is enough time to acknowledge the Modbus access within the required response time.

The system, comprising at least one SENTRON Powercenter 1000/1100/2000 and the connected circuit protection devices, is a spatially distributed system however. This may lead to a delayed response (Delayed Acknowledge DA) during write accesses via Modbus.

This function is necessary, especially when writing parameters or sending commands. Without the Delayed Acknowledge function, a write command can only be sent to a terminal device around every 10 seconds. The device is busy in the meantime.

In order to send write commands to terminal devices at shorter intervals, register 4096 with the status Delayed Acknowledge must be read out in the Powercenter. If the value is 0x01, no further write command can be issued. If the value is 0x02 (success) or 0x03 (failed), the value 0x00 (idle) can be written to the register (via Modbus TCP write access 0x06 or 0x10). Only in this state can a further write command be sent to the terminal device. Several consecutive commands can therefore be sent to a terminal device at shorter intervals.

In order to avoid overlaps, a terminal device should only ever be parameterized from a physical connection. The write requests should be executed sequentially on the same terminal device.

Note

To support multiple applications at the same time, it is necessary to clarify the Write permissions at application level so that the applications do not influence each other, i.e. changes are not overwritten by each other.

Therefore it is recommended to use only one application and to set parameters only via Powerconfig (mobile or PC) and to clearly define the responsibility.

6.10.4 Data points and Modbus register

Different metering and communication-capable SENTRON circuit protection devices support different measured values and parameters/data points. Some data points are identical across multiple devices and some are device-specific.

A full overview of all device types and all data points can be found using the link below. The Modbus register map is provided as a separate file due to the large volume of information.

Overview of data points (https://support.industry.siemens.com/cs/ww/en/view/109973540)

The information is read off as shown in the following illustration, which uses a sample extract from the Modbus register map:

Register	Length	Designation	Format	Value range	Unit	Access	AS+FC 5ST3	MCB 5SL6	5TY1 ECPD
3072	2	Current temperature	FP32		°C	R	x	x	x
3074	2	Average temperature	FP32		°C	R	x	x	x
3076	2	Actual current L	FP32		A	R	---	x	x
3078	2	Average current L	FP32		A	R	---	x	x
3080	2	Maximum current L	FP32		A	R	---	x	x
3082	2	Voltage L-N	FP32		V	R	---	x	x
3084	2	Line frequency	FP32		Hz	R	---	x	x
3086	2	Active power {L}	FP32		W	R	---	x	x
3088	2	Apparent power {L}	FP32		VA	R	---	x	x
3090	2	Total reactive power Qtot {L}	FP32		V	R	---	x	x
3092	2	Power factor {L}	FP32			R	---	x	x
3094	4	Imported active energy	FP64		Wh	R	---	x	---
3098	4	Exported active energy	FP64		Wh	R	---	x	---
3102	4	Imported reactive energy	FP64		varh	R	---	x	---
3106	4	Exported reactive energy	FP64		varh	R	---	x	---
3110	1	Switching status of the (attached) circuit protection device	U16	0 = Status unknown 1 = Off, without tripping operation 2 = On 3 = Tripped 4 = Tripped, but lever on/blocked 5 = Standby (for ECPD) 6 = Standby tripped (for ECPD)		R	x	x	x

The register number and the data format must be specified to connect the devices via Modbus TCP.

An "x" indicates that the corresponding data point or register is available for a device type. The "Access" column indicates whether a data point is readable, or readable and writable, and represents the Modbus TCP function codes:

- RO (read only): 0x03, 0x04
- RW (read, write): 0x03, 0x04 or 0x10
- WO (write only): 0x10
- CMD (command): 0x06

6.11 Secure protocol – https via REST-API

The https secure protocol is encrypted using TLS. It provides an alternative to Modbus TCP communication and is used as the standard communication path for the SENTRON Powerconfig commissioning software (mobile app or desktop).

The secure protocol is being extended step by step. It is therefore necessary to always use the latest firmware versions of the SENTRON Powercenter 1100/2000. See the section Function overview for each firmware version (Page 92) for a list of functions that are already supported.

6.12 Role-based access control

Role based access control (RBAC) is a cybersecurity function used with https communication. One application example for this is that normal personnel in a company only have read access to all data. No further knowledge is necessary. Persons responsible for the IT infrastructure on the other hand have extended access rights and can also change parameters such as IP addresses.

Up to five different users with the following three user roles can be created in SENTRON Powercenter 1100/2000:

- Observer: Only has read access to all data, cannot change parameters or send commands.
- Engineer: Has read access and can write parameters with the exception of communication parameters (e.g. terminal device pairing, IP parameters). Writing parameters also includes sending commands, e.g. the remote switching command.
- Superuser: Full access, i.e. can read and write all data points including communication parameters and user management. Data points that can be written exclusively by the Superuser are marked in the Modbus register map. All other parameters can also be set by the engineer. For more information on this subject, see the section Data points and Modbus registers (Page 89).

A user with the "Superuser" role must be created during first commissioning so that the Powercenter can be used in the first place. A unique user name and password must be stored.

Only a Superuser can create additional users and delete users. Individual users are able to change their own password. This is enabled via the "Security" view in the SENTRON Powerconfig commissioning software (mobile app and desktop).

If a user forgets their password, a Superuser can delete and recreate that user. Alternatively, all users can be deleted by pressing the button on the front for 20 s until the LEDs are lit yellow. The delete instruction must then be confirmed by a short press of the same button again within 10 s. If a reset is performed using the button, a new Superuser must be created the next time communication is established.

No users are available for communication via Modbus TCP.

6.12.1 Function overview for each firmware version

The RBAC function and REST API are being extended step by step on the SENTRON Powercenter 1100/2000. It is always necessary to update to the latest version for this reason. Functions are supported by the firmware versions as follows:

Version V6.0:

- Create/change/delete local users
- Remote switching function for 5TY1 COM ECPD and 5ST3 COM remote control auxiliary (RCA)

Version V7.1:

- MQTT settings for Powercenter 2000
- Output switching (Force Output) for 5TT4 COM DIDO

6.13 Cloud connection via MQTT

The MQTT interface of the SENTRON Powercenter 2000 enables a native connection to different cloud solutions. This is used to send measured values, parameters and status messages of the SENTRON COM system to an MQTT-Broker (server). The MQTT protocol (Message Queuing Telemetry Transport) makes it possible to transmit data in the Publisher/Subscribe model and is encrypted via TLS.

The MQTT interface of the Powercenter 2000 is intended for operators with prior knowledge of cloud solutions. Terms such as broker, QoS (Quality of Service), topics, etc. are not explained in this manual for that reason.

In the first version of Powercenter 2000, the focus is on a native connection to the AWS service (AWS IoT Core Message Broker) via MQTT protocol. All the specific requirements of further cloud solutions, such as Azure, are not yet fully supported.

SENTRON Powercenter 2000 offers a generic MQTT client which supports the functions of MQTT protocol version V3.1.1.

6.13.1 Configuration

All the settings of the MQTT interface are entered via the secure https protocol via REST API. The following settings are necessary or possible depending on the particular firmware version. The MQTT connection should always be stopped before making changes in the configuration.

Basic settings

- **Client ID**: Unique client ID to identify the client to the broker. This consists of a UTF-8 coded character sequence up to 128 bytes.
- **Server end point**: Host name or IP address of broker
- **Server TCP port:** Default 8883

Certificates

- **TLS client certificate with private client key**: X.509 certificate and private key for authentication. The certificate and the private key must be uploaded to the device by the operator. It is not possible to read them back out of the device. It is only possible to read back the subject of the certificate for checking. The availability status of the private key is also displayed.
- **TLS server certificate**: X.509 certificate authentication of the server. This certificate is uploaded to the device by the operator, provided that it is available. It is not possible to read them back out of the device. It is only possible to read back the subject of the certificate for checking.

Connection

- **Automatic reconnection in the event of an interrupted connection**: Only possible if the client has previously established a successful connection. If the client was stopped manually, this function is not possible.
- **Start or stop client**: In order to start the client, the server end point, the server TCP port, the TLS client certificate and the private key must be configured. If the client has been started, this status remains active. If this is the case, the client is automatically reconnected after a device restart.
  If a terminal device is unpaired, or if a new device is paired, the client connection should be restarted so that all data are transmitted correctly.
- **Test connection**: Before the client server is started, the connection can first be tested with all the necessary entries.
- **MQTT connection status:** Displays the current status of the connection from the client to the broker. Successful connection and the reason for a connection error can be determined here:
  - 0: Connection successful
  - 1: MQTT protocol version not supported by the server
  - 2: Client ID rejected by server
  - 3: Server not available
  - 4: Incorrect user name or password
  - 5: No authorization to connect (e.g. due to system problems, etc.)
  - 256: Disconnected
  - 257: Invalid server end point/host name/port, or IP address of the server is incorrect or cannot be reached. Check that all values have been entered correctly and check the DNS processes or firewall settings.
  - 260: Cipher error. For all errors under MBEDTLS_CIPHER_C
  - 500: Connection failed, e.g. due to network error

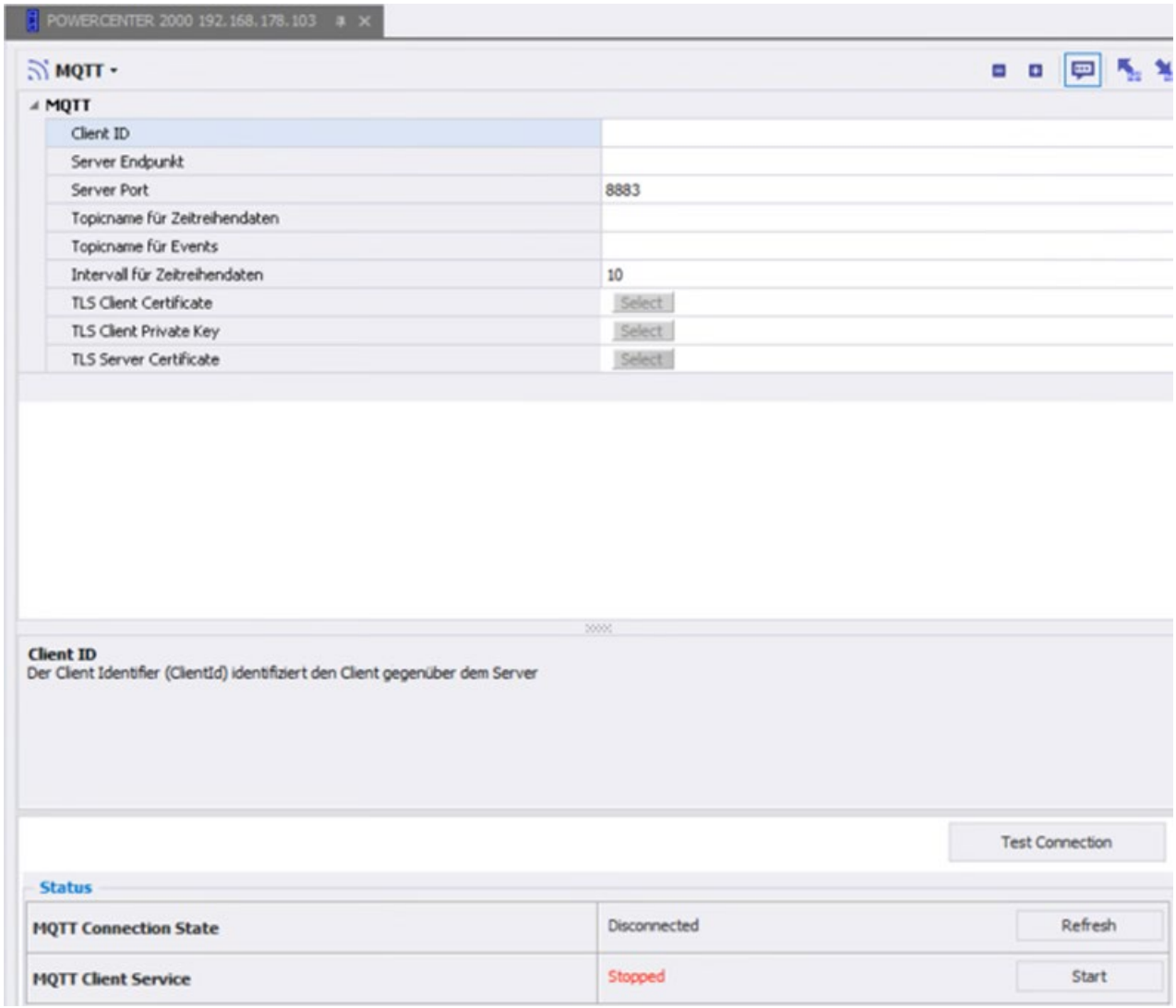
Non-configurable parameters

- TLS is always active
- TLS Version V 1.2
- MQTT Version 3.1.1
- Cipher: TLS_AES_128_GCM_SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256
- Quality of service (QoS)

Configuration using SENTRON Powerconfig

In SENTRON Powerconfig (desktop or app), navigate to the "MQTT" view via SENTRON Powercenter 2000.

All the parameters are entered here and transferred to the device. The connection can also be tested, started and stopped here.



6.13.2 MQTT topics

SENTRON Powercenter 2000 supports the following topics. Each topic has a settable topic name (UTF-8 coded). If the name is empty, the topic is not published. The Payload cannot be adapted. Data are only transmitted from terminal devices if these are paired and online.

The data is not buffered if the connection is lost.

Events/event data

The event topic publishes alarms, events and tripping operations of devices when a value changes. This allows the system to respond to events as quickly as possible. General device information, e.g. name or firmware version, are also transferred here. Device information and events are published when the service is started.

The event topic cannot be deactivated. The QoS (Quality of Service) is 1. All events of all terminal device are always transmitted.

Information that is published once on startup:

- 5TY1 COM ECPD settings: Protected parameters
- Filter settings of all RCM devices
- Alarm settings
- 5ST3 COM RCA settings: Test parameters, ARD settings, remote control via cable or COM interface
- Parameters for device identification (name, rated current, firmware version, etc.)

Events that are published when a value changes:

- Alarm and tripping operations
- Breaker statuses
- Blocking status of protected parameters for 5TY1 COM ECPD

Time-series data

The time-series data topic transmits cyclic measured and status values that are necessary for long-term data storage operations and data analyses. The QoS (Quality of Service) is 0.

The interval for publishing time-series data can be set under MQTT.

The subordinate circuit protection devices whose measured values are to be published can be selected.

Note

If the maximum number of terminal devices is paired and all data point groups are activated, it is recommended to set the interval for publishing time-series data to a value greater than or equal to 60 seconds to ensure optimal performance.

The following groups of measured values can be activated/deactivated. If a group of measured values is active, this applies for all the selected terminal devices. If the group is not

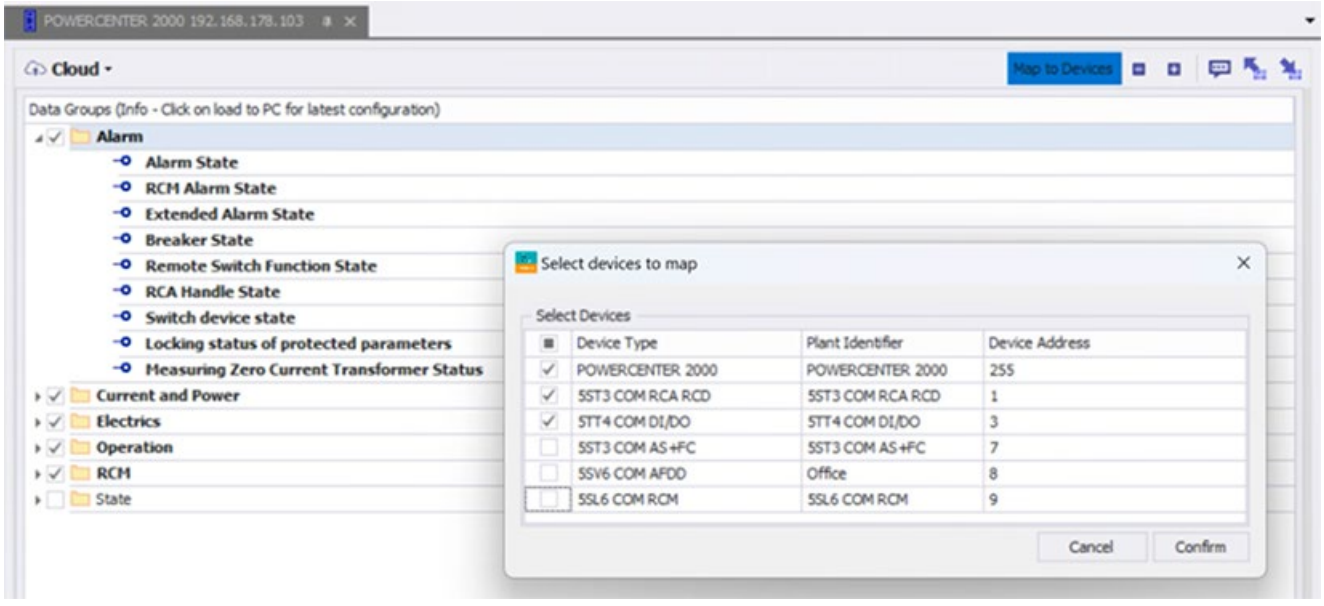
present in a terminal device type, it remains empty. In a second step, the terminal devices from which the selected measured value groups are to be transferred must be selected.

Group name	Values contained in the group
Current/power	All current and power values
Electrical values	All other electrical values, e.g. voltage, power factor, energy, frequency
RCM	All RCM measured values
Status	
Alarm	Alarms, tripping operations, breaker statuses
Operating information	System time, temperature, operating hours, number of operating cycles, number of tripping operations, number of tests

As soon as the SENTRON Powercenter 2000 is successfully connected to the MQTT broker and actively running, newly paired terminal devices are automatically added to the "Assign devices" configuration. The associated time-series and event data are published directly. If a terminal device is unpaired and disconnected from the SENTRON Powercenter 2000 during this time, it is automatically removed from the "Assign devices" configuration and none of the data of this device are published any longer.

Configuration using SENTRON Powerconfig

As usual, a project must first be created in SENTRON Powerconfig with SENTRON Powercenter 2000 and the lower-level terminal devices. The individual data points of the different terminal devices and the SENTRON Powercenter 2000 are assembled in the "Cloud" view. The data points which are to be transferred in the topic for time-series data are selected here.



6.13.3 MQTT payload structure

The time-series data and event data are published with the following structure. The example shows the payload from the time-series data.

```
{
  "id": "9e5b36ee-2104-46d3-a8bc-862c1d8d9347",
  "source": "RBG S10/Geb 3.3/-F10/Kitchen/LQN/240902000025",
  "specversion": "1.0",
  "type": "com.siemens.sentron.poc2000.ts.published.v2",
  "subject": "ts",
  "time": "2023-07-04T09:49:44.020Z",
  "data": [
    {
      "id": "5",
      "type": "item",
      "attributes": {
        "itemType": "AFDD",
        "serialNumber": "ZHG/210924500065",
        "plantIdentifier": "-F2",
        "orderNumber": "5SV6016-6MC16",
        "dataItems": [
          {
            "id": "3072",
            "type": "dataItem",
            "attributes": {
              "legibleValue": "37.4",
              "quality": "valid",
              "name": "TEMP"
            }
          }
        ]
      },
      "relationships": {
        "parent": {
          "data": {
            "id": "0",
            "type": "item"
          }
        }
```

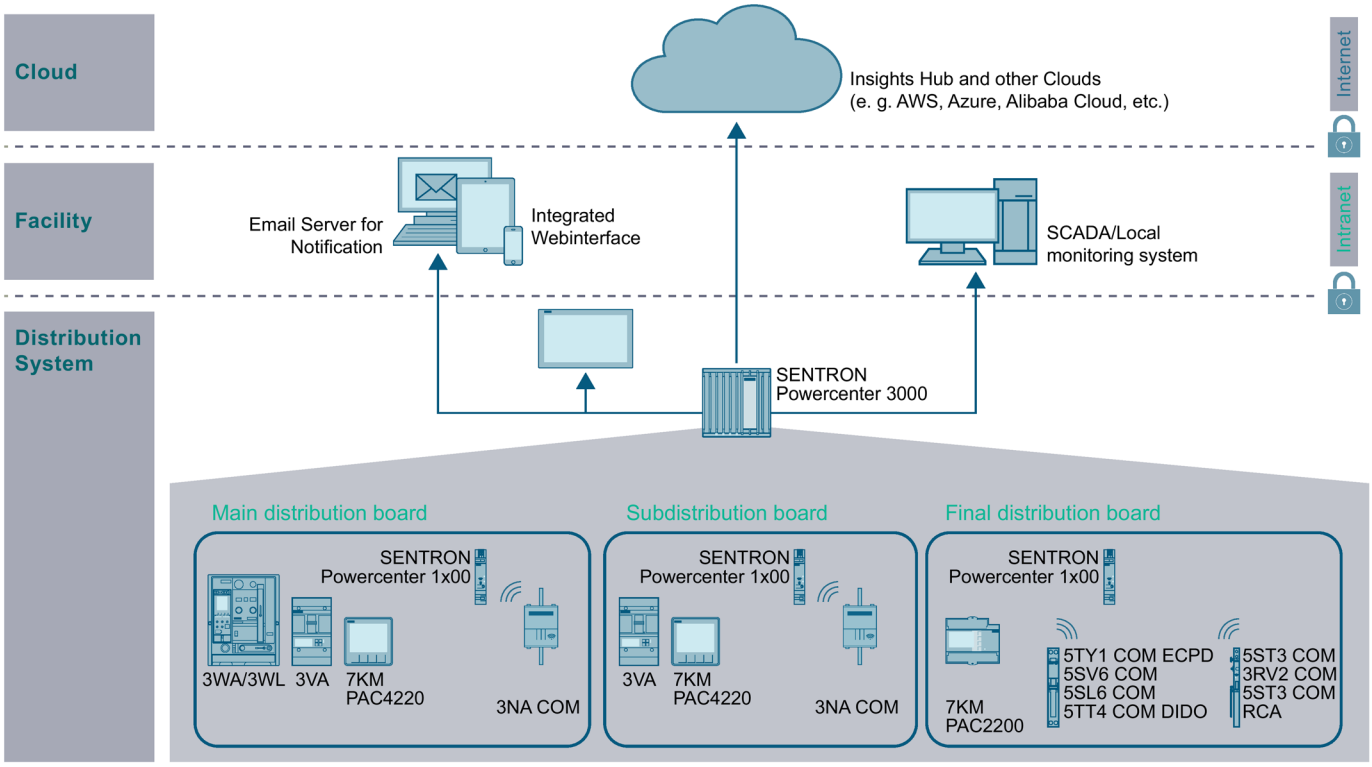
```
            }
          }
        ]
      }
```

Structure	Description
id	Identification of message. The value contains a version 4 UUID with hyphen separation in accordance with RFC 4122. The SENTRON Powercenter 2000 ensures that the combination of source + id is unique for each message.
source	Identifies the SENTRON Powercenter 2000 that is sending the message, comprises {location}/{plant identifier}/{serial number}
specversion	Version of the Cloud Events specification
type	Message type: Time-series (.ts.) or event data (.ev.)
subject	Subject of the message, e.g. 'ts' for time-series data, 'ev.onchange' when a value changes or 'ev.onstartinfo' when the service for event data starts
time	Time stamp of the Powercenter 2000 in ISO 8601 format
data	Payload
id	Address of the device from which the data originate. 1-24 for the terminal devices or 255 for the Powercenter 2000. See the section Device addressing via Modbus TCP (Page 85).
type	'item' data type signifies device
attributes	Details about the device from where the values originate
itemType	Device type
serialNumber	Serial number
plantIdentifier	Plant identifier
orderNumber	Order number
dataItems	Data points that are transferred
id	ID of the datapoint
type	'dataItem' data type signifies data point
attributes	Details about the data point
legibleValue	Display value of the data point
quality	Quality of the data point, e.g. 'valid' (value available) or 'invalid' (not available or device disconnected)
name	Internal name of the datapoint
relationship	Describes the hierarchical relationship of the device to the Powercenter 2000
parent	Information about the higher-level device
data	Information Payload
id	Higher-level device. This remains empty if the data point belongs to the Powercenter itself.
type	'item' data type signifies device

Application examples

7

The SENTRON circuit protection devices with communication and measuring function protect the final circuit and acquire its data to increase system availability. The devices are used in a main or subdistribution board. In doing so, the increased transparency allows predictive fault detection through early warnings or targeted, simplified maintenance through permanent status recording. The acquired data still have to be processed in higher-level applications. The SENTRON or Siemens portfolio offers different digitalization solutions for this purpose.



This can be directly connected to different applications via the Modbus TCP connection of the SENTRON Powercenter 1000/1100/2000, for example to:

- The power monitoring system SENTRON Powermanager
- The IoT (Internet of Things) data concentrator SENTRON Powercenter 3000 with web-based display
- The SENTRON Powermind cloud-based application in the Insights Hub via SENTRON Powercenter 3000
- Control systems, e.g. the TIA-Portal (via S7-1200 and S7-1500) or LOGO! 8.3
- the building services management system, e.g. Building X

The SENTRON Powercenter 3000 can be used to connect the measurement and communication-capable SENTRON circuit protection devices with SCADA, power monitoring and maintenance systems. The SENTRON Powercenter 3000 has an integrated web server to visualize the status and measured value display of all connected devices without requiring other software to be installed.

Furthermore, it also offers the possibility of archiving the data and thus, a more profound data analysis. Similarly, the SENTRON Powercenter 3000 makes it possible to send warnings via email. It also enables connection to other cloud systems via MQTT for fully comprehensive and long-term data availability, even outside the local network. You can find more information on the functions of the SENTRON Powercenter 3000 in the Equipment Manual.

Other types of devices can be connected and visualized via SENTRON Powercenter 3000. For example SENTRON PAC measuring devices, other Modbus TCP devices or air and compact circuit breakers (3WA and 3VA). Up to 32 devices of the low-voltage power distribution board can be connected with a SENTRON Powercenter 3000 device. The SENTRON Powercenter 1000/1100/2000 data transceiver (including its up to 24 terminal devices) counts as one device.

As an alternative to cloud solutions, a secure VPN connection via the router provides access to the data in the local network from any location.

See also

Equipment Manual - SENTRON Powercenter 3000 (https://support.industry.siemens.com/cs/ww/en/view/109763838)

SENTRON Powermanager (https://support.industry.siemens.com/cs/ww/en/view/109771760)

Modbus TCP connection (Page 84)

Cybersecurity

8

This chapter describes how to configure the system such that maximum protection against unauthorized access by third parties is achieved. This is necessary so that data cannot be read out and to prevent unwanted settings or switching operations.

8.1 Requirements with respect to the operating environment and security assumptions

Siemens recommends the following security precautions:

- Performing a threat and risk assessment (as part of security management)
- Concepts for network security
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
- Concepts for access control (use of access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

8.1.1 Threat and risk assessment

Vulnerabilities and risks are identified and countermeasures proposed to ensure the security of the system, the networks, and data.

8.1.2 Concepts for network security

You will find information on network security in the white paper "Industrial Network Security Architecture," available at Download center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrialsecurity/ downloads.html) on the Industrial Cybersecurity website (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

8.1.3 Concepts for network security

Network security should be established for power distribution systems with reference to IEC 62443-3-3.

8.1.4 Concepts for access control

Physical protection

In addition to the closing off and/or monitoring of entire production plants, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security

Physical corporate security can be ensured by the following measures:

- Closed off and monitored company site
- Entry control, keys/card readers and/or security personnel
- Escorting of external personnel by company employees
- Security processes in the company are taught and followed by all employees

Physical production security

The physical security of a production location can also be ensured via the following measures:

- Separate access control for critical areas, such as production areas.
- Installation of critical components in lockable control cabinets/switching rooms including monitoring and alarm signaling options. The control cabinets/electrical rooms must be locked using the appropriate cylinder locks. Do not use simple locks such as universal, triangular/square or double-bit locks.
- Radio link planning to limit wireless coverage so that it is not available outside the zones defined (for example the factory hall).
- Guidelines that prevent the use of third-party data storage media (e.g. USB flash drives) and IT devices (e.g. notebooks) classified as insecure on systems.

8.2 Defense-in-depth strategy

8.2.1 "Defense in Depth" holistic cybersecurity concept

The Defense in Depth multi-layer security concept offered by Siemens provides comprehensive and far-reaching protection for industrial plants in accordance with the recommendations of international standard IEC 62443.
Productivity and know-how are protected on 3 levels:

Plant security

Plant security uses a variety of methods to protect against physical access by persons to critical components. This begins with classical building entrance and extends to the safeguarding of sensitive areas using access control (for example, code card, iris scan, fingerprint, or access code).

Network security

Networks must be protected against unauthorized access. This can be achieved by means of security measures in the product but also in the immediate vicinity of the product.

System integrity

Targeted measures must be implemented to protect existing know-how and to protect against unauthorized access to plants.

You can find more information about Defense in Depth, plant security, network security, and system integrity on the SIEMENS web page
Industrial Cybersecurity (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

And to obtain more information on the subject of industrial cybersecurity, use the download center (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity/downloads.html).

The "Operational Guidelines" provide recommendations for basic cybersecurity measures for secure plant operation, for example.

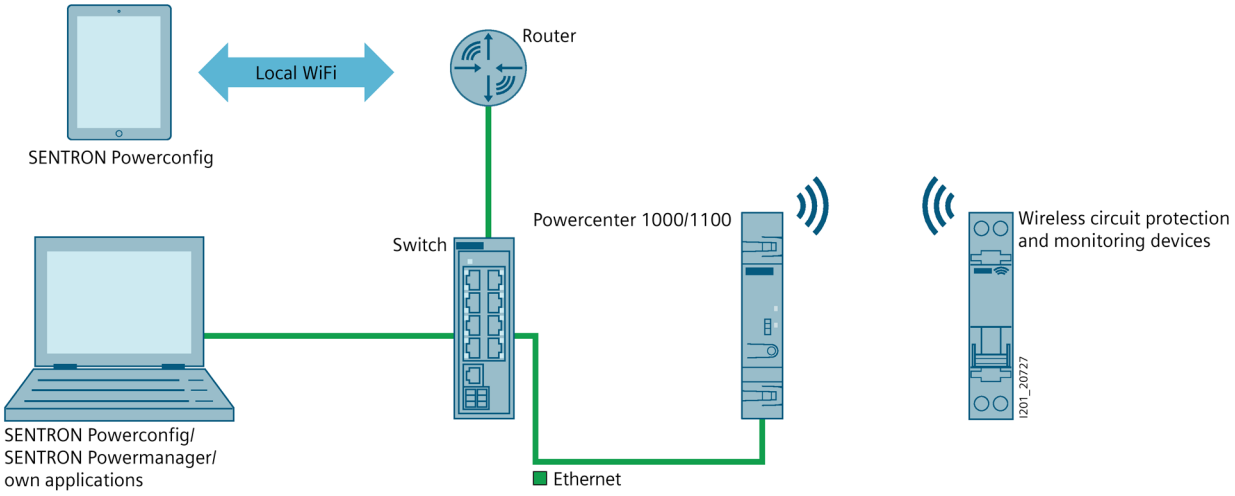
See also

Cybersecurity information (Page 11)

8.3 Intended operating environment

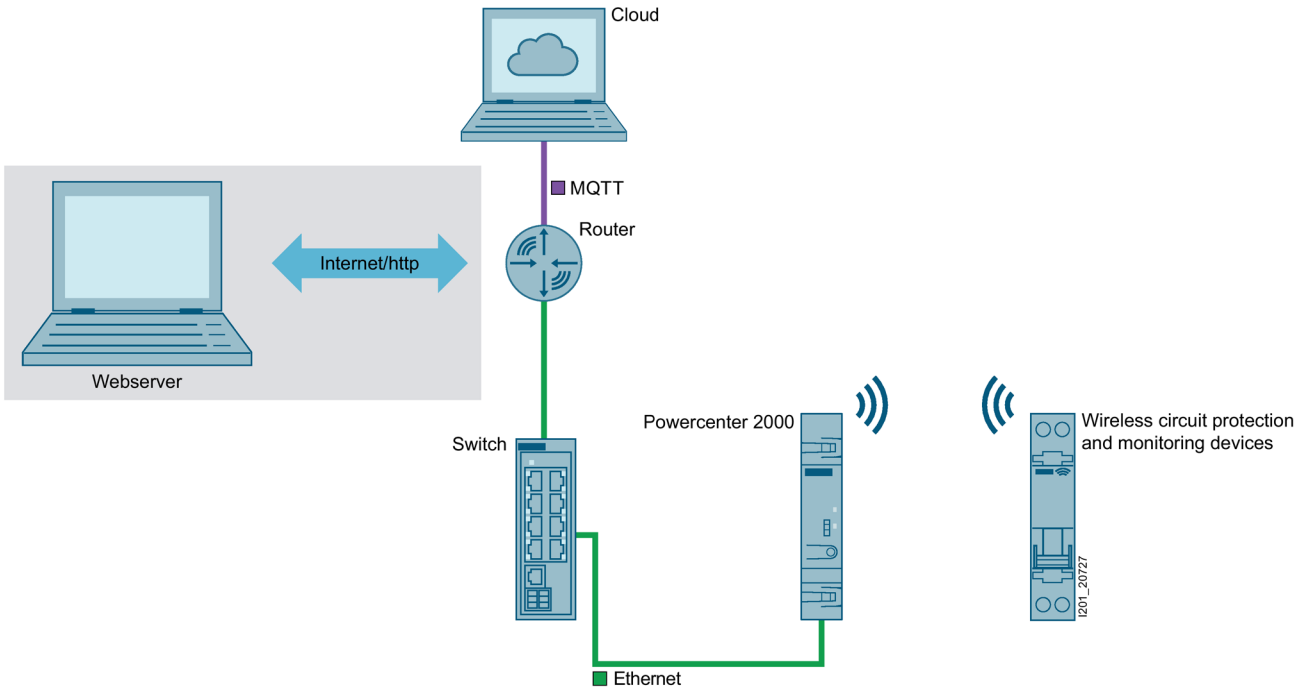
In order to be able to operate devices in a cybersecure manner, it is necessary to combine the devices/applications to form a cybersecure network.

8.3.1 Local network



The system of communication-capable circuit protection devices together with a SENTRON Powercenter 1000/1100 are connected to the local network via Ethernet. The data are read out via this network, e.g. using SENTRON Powerconfig. Further SENTRON devices, such as PAC measuring devices, can also be connected in the same way. Other actors, gateways or proprietary software solutions may also be present in the local network.

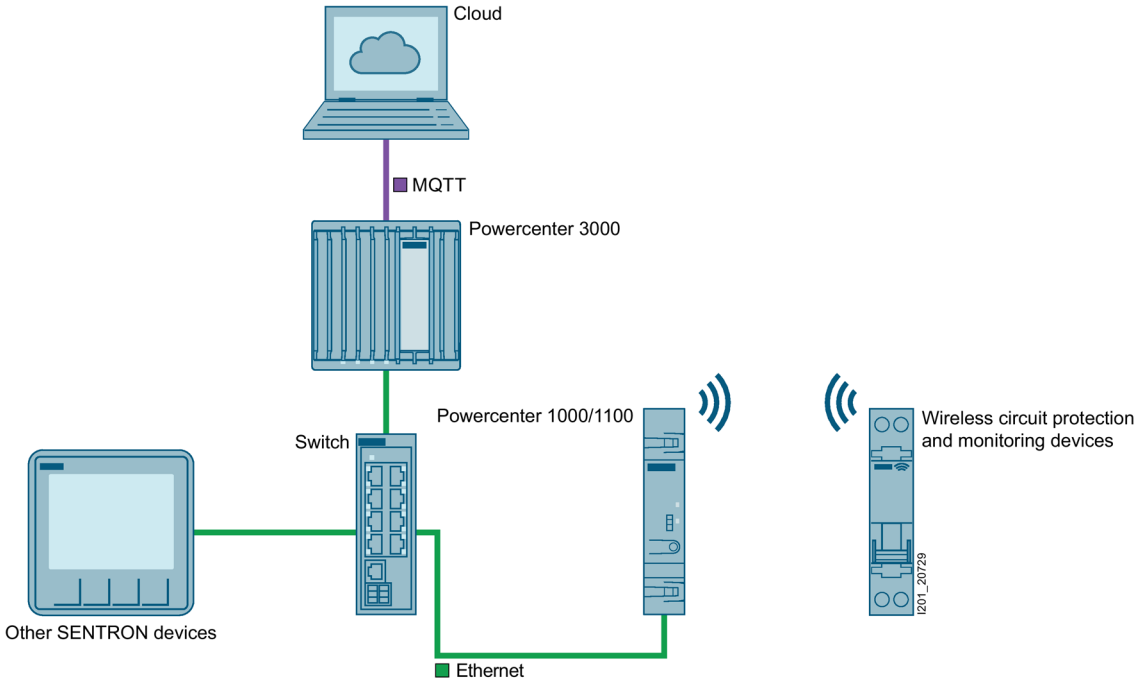
8.3.2 Cloud connection via Powercenter 2000



If an application in the local network is not sufficient, communication in dedicated cloud solutions can take place using a Powercenter 2000. The SENTRON Powercenter 2000 can send measured values directly to a specially configured cloud application via the MQTT interface. All the measures required for network security (e.g. firewall) and for cloud security must be implemented.

The integrated web server of the SENTRON Powercenter 2000 can also be accessed as an alternative to the cloud connection.

8.3.3 Cloud connection via Powercenter 3000



As an alternative to the direct cloud connection of the Powercenter 2000, its SENTRON Powercenter 3000 IoT gateway can also be used in conjunction with a Powercenter 1000/1100 to communicate data to the cloud. This is especially necessary as soon as additional communicative devices from the SENTRON family, e.g. PAC measuring devices, 3VA circuit breakers, etc., are present in an application. In this case, the Powercenter 3000 takes charge of the necessary security measures in this network.

8.4 Communication protocols used

8.4.1 RF communication

Every communication-capable circuit protection device communicates with the associated SENTRON Powercenter 1000/1100/2000 by means of a point-to-point connection. Communication between the terminal devices and the Powercenter is wireless and cannot be deactivated. This radio frequency communication is based on the standard: Zigbee Pro.

- All network nodes authenticate themselves by means of a secure process in which network keys are never transmitted unencrypted over the air.
- The network keys are updated periodically.
- 16 different radio channels can be used in the 2.4 GHz radio frequency band so as to increase protection against unwanted signals and interference.
- The radio transmit power of each device can be set. If the range is limited, only devices in the immediate vicinity can establish a connection. This further increases the security of the system.
- During the pairing process, i.e. as soon as a subordinate circuit protection device starts to enter the wireless network of the Powercenter, the network must be secured to a greater degree, e.g. by reducing the radio transmit power, or the process must be monitored until it is complete. The reason for this is a possible attack vector in this time-limited status.
- Encryption used: AES CCM algorithm with 128 bits.

8.4.2 Bluetooth®

One option for communicating with a Powercenter 1000/1100/2000 is to set up a Bluetooth® connection between the Powercenter and a mobile terminal device and the SENTRON Powerconfig software. Bluetooth® Low Energy (BLE) (version 4.2 or higher) with a Passkey entry authentication method is used for this purpose:

- Encryption used: AES CCM algorithm with 128 bits.
- LE Secure Connections Pairing: The FIPS-certified algorithm Elliptic Curve Diffie- Hellmann (ECDH) is used for creating the cryptographic key. This increases the security of the radio connection during the initial pairing process.
- Passkey Entry: The user enters the identical 6-digit code (Passkey) on the smartphone that is printed on the Powercenter (plain text on the side or in the Data Matrix Code on the front). The Passkey is not used as the input for the encryption algorithm. If an attacker knows the Passkey, it will therefore be of no help in decoding the encrypted data that have been transmitted between the devices.
  The Passkey can be changed by the user after first commissioning for added security. The Passkey is reset to the factory setting with a long button press (≥ 10 s).
- The BLE function is only activated with a short button press when it is needed. When the Bluetooth® connection is no longer needed, it should be deactivated with another short

button press. If a connection is not established within 180 s, the BLE function automatically switches itself off.

- Limited range of BLE connection to approx. 3 m

8.4.3 Ethernet interfaces

Several protocols and services are available over the Ethernet connection. The table below shows the services that are supported by the different Powercenter versions.

Service	Protocol	Encryption	Default port	Properties	POC 1000	POC 1100	POC 2000
MQTT Cloud Service	MQTT	Via TLS 1.2	8883	• Configurable • Activated by default, can be switched off	---	---	x
Web interface	http		80	• Activated by default	---	---	x
REST API	https	Via TLS 1.2	443	• Activated by default	---	x	x
Modbus TCP gateway function	TCP		502	• Configurable • Activated by default	x	x	x
Identification (network discovery service)	UDP		17008	• Activated by default	x	x	x
SNTP time synchronization	UDP		123	• Not active by default, can be activated	x	x	x
DHCP network setting	UDP		68	• Configurable • Activated by default, can be switched off	x	x	x
SNMP	UDP		161	• Activated by default	x	x	x

The Modbus TCP connection has no built-in encryption. Security-critical systems must therefore make use of the https connection.

In Version V7.0, https communication is not yet fully integrated for all data points. It is only used for the MQTT interface settings, the user management and secure remote switching.

The MQTT settings and the user settings incl. passwords can only be configured via the https connection.

8.4.4 Further interfaces

Physical interfaces must only be accessible to authorized personnel. These include buttons, slide switches or levers on devices, as well as external signals that can be wired on a device.

Further internal interfaces and protocols are also present, e.g. UART, JATG, etc. These are internal interfaces that cannot be read out. They are used for communication between microcontrollers, for production purposes or service processes, for example.

8.5 Deviation from supported standards

One deviation from a standard relates to radio communication. Mechanisms such as device pairing, encryption, the ZigBee Cluster Libraries, and the firmware update (OTA) conform to the Zigbee Pro standard. However, identification data points that deviate from the standard are used, as are proprietary commands for starting a firmware update. This is due to increased security requirements and compatibility with other SENTRON devices.

8.6 Security functions

8.6.1 Access control

Up to five local users can be created on a Powercenter 1100 (as of firmware version V6.0) or Powercenter 2000. These users are assigned a level of authorization resulting in role based access control (RBAC).

When the device is commissioned for the first time, no user with a default password is stored. At least one user with the "Superuser" role must therefore be created so that all other settings can be defined.

For more detailed information about authorizations, see the section Role-based access control (Page 91).

Users are always configured via the https connection using SENTRON Powerconfig (app or PC).

Passwords are only transmitted via the encrypted https channel. TLS 1.2 is used for encryption and decryption. Passwords are stored in the device in hashed form.

Other data stored on the Powercenter, e.g. parameters, terminal device configurations, etc., are not encrypted.

8.6.2 Write protection

A slide switch is installed on the front of the SENTRON Powercenter 1100/2000. This switch is in the "locked" state on delivery. This status prevents all write commands from the software to the device. Write commands include all parameter changes, commands e.g. for remote switching, but also commands for pairing/unpairing terminal devices. Before first commissioning, the switch must be set to "unlocked" using a screwdriver so that terminal devices can be paired and parameters can be set.

After first commissioning and configuration of the system, it is recommended to return the write protection switch to the "locked" state so as to prevent unwanted changes.

However, if the system is to be controlled remotely, e.g. for activating/deactivating the remote control auxiliary (RCA) or the ECPD, write protection must remain "unlocked".

The yellow slide switch on the 5ST3 COM remote control auxiliary can be used to block remote access. Remote access is not activated by default on the 5TY1 COM ECPD and must first be activated by pressing a button for confirmation following two-factor authentication.

8.6.3 Protected parameters in 5TY1 COM ECPD

The scope of configuration of the 5TY1 COM ECPD is extensive. Protection parameters such as rated current can also be set for example. These parameters are known as "protected parameters".

A user with the "Superuser" access role is required so as to ensure that these protected parameters are not changed by unauthorized persons. Alternatively, provided Modbus TCP is used for communication, changes of protected parameters must first be confirmed with a button press after the request for a change has been issued by the software. For more information on this subject, see the section Switching operation with the 5TY1 COM ECPD (Page 79).

8.6.4 Firmware updates

In order to ensure that the device complies with cybersecurity requirements, the entire system can only be updated by means of signed firmware files. A signed firmware update can only be performed using SENTRON Powerconfig PC. This makes operation with corrupted or manipulated firmware impossible.

It is recommended to always use the latest firmware version on all devices. You can find the latest firmware and a description of the update procedure here (https://support.industry.siemens.com/cs/ww/en/view/109797242).

Devices must be restarted after a firmware update. When the entire system update is complete, all firmware versions can be checked under "Parameters".
The Bluetooth® interface of the SENTRON Powercenter 1000/1100/2000 cannot be used during the update.

8.7 Decommissioning

Perform the following steps prior to disposal of a device or the entire system to ensure that no sensitive data fall into unauthorized hands.

- Purging of sensitive data
  Perform the following steps prior to disposal of a device or the entire system to ensure that no sensitive data fall into unauthorized hands.
- Reset of the devices
  Reset the communication of all relevant devices with a 10 s button press. Also reset all local users including passwords on the Powercenter 1100/2000 with a 20 s button press. See the section Standard operator controls - levers and buttons (Page 44).
- Removal of the devices from the network
  Inform the network administrator so that all further data tracking operations are deleted.
- Disposal of devices as old electrical equipment
  Some devices, e.g. LV HRC fuses, can be recycled. When disposing of old electrical equipment, the current local national/international regulations must be observed.
- Reuse of devices
  Instead of disposing of products that are no longer required, devices can also be reused by others (resale).
- Documentation with respect to disposal

See also

Disposal of waste electronic equipment (Page 117)

8.8 Cybersecurity guidelines for cybersecurity hardening

Cybersecurity guidelines for secure operation and during commissioning. The following points are designed to help the user to keep the device in operation without disturbances even in the event of cyberattacks.

- **Restrict physical access**
  Ensure that only authorized personnel have physical access to the device/system. This can be implemented by means of access restriction in the form of a lockable environment, for example.
- **Install the latest firmware version**
  Keep your product software up to date. New versions should be installed without delay. You can download patches, updates and hotfixes for Siemens products in the Siemens SiePortal (https://sieportal.siemens.com/en-ww/support).
- **Set up a backup and restore process**
  Set up a backup and restore process so that operation can be resumed as quickly as possible after an incident. This entails the regular creation of backups, testing of the functionality of backups, secure storage of backups and the creation of a recovery plan for use in an emergency. Use the SENTRON Powerconfig functionality to create a backup of the SENTRON Powerconfig project file.
- **Set up access control**
  Activate access control and set it up. Do not create a single account for a user group in which a password is shared by several members of personnel. Work with user accounts or groups with minimal rights.
  For more information, see the section Role-based access control (Page 91).
- **Only use secure passwords**
  Data can easily be misused if insecure passwords are used. Insecure passwords can be guessed or decrypted easily.
  - It is important to always change the standard passwords during commissioning for this reason and to use different passwords for different functions and devices.
  - When changing passwords, avoid using passwords (or elements of passwords) that have been used before.
  - Change the passwords for functions you do not use as well, because unused functions are also susceptible to misuse.
  - Always keep your passwords secret and make sure that passwords are only accessible to authorized individuals.
  - Choose passwords that are longer than the required minimum password length and use a mix of lower-case and upper-case letters, numbers and special characters.
- **Activate the security functions**
  Ensure that all cybersecurity functions of the devices are activated.
- **Reduce the attack surface**
  Deactivate functions that are not necessary for operation before startup. Do not activate remote switching of the 5TY1 COM ECPD if this is not necessary, for example.
- **Sensitization of personnel**
  Regular trainings with respect to cybersecurity and continuous testing of the success of training are essential in order to ensure that cybersecurity measures in processes and

work procedures are fully embraced. Training courses on production equipment and software should also include the topic of cybersecurity wherever applicable.

8.9 Cybersecurity vulnerabilities

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 only the latest product versions are always used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed at: RSS Feed (https://www.siemens.com/cert)

You can read about potential vulnerabilities in Siemens products on the public and freely accessible Siemens CERT/RSS (https://www.siemens.com/cert) web page. Siemens provides information about known vulnerabilities relating to Siemens products on this web page. SSAs (Siemens Security Advisory) are published for this purpose. Each SSA contains a description of the vulnerability and its solution.

You can contact us at any time with security-related queries about the Siemens portfolio or the Siemens infrastructure. This is especially important if you would like to report a security issue. Please note that we can only process emails in English or German.

You can find our contact details on the internet under Siemens CERT/RSS (https://www.siemens.com/cert).

Email: productcert@siemens.com (mailto:productcert@siemens.com)

Service and maintenance

9

9.1 Repair instructions

The standard warranty obligations apply to the SENTRON circuit protection devices. You are exempt from a repair.

⚠ WARNING

Hazardous voltage.
Will cause death or serious injury.

This device/unit can result in hazardous voltages.

Touching live parts will result in death or serious bodily injury.

Installation, commissioning and maintenance only by qualified personnel.

9.2 Firmware update

The firmware updates of all SENTRON circuit protection devices with communication and measuring function are available in the SiePortal. The current firmware update can be found here (https://support.industry.siemens.com/cs/ww/en/view/109797242).

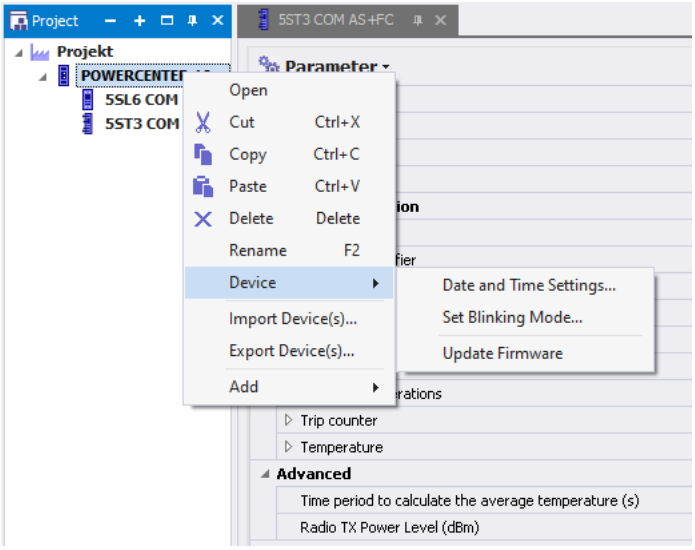
The latest firmware must always be installed on all devices to ensure optimum use of all functions and to avoid potential security vulnerabilities.

The firmware update comprises the entire device network so as to avoid a mixture of different firmware versions within a system.

Note

A secure, signed update can only be carried out with the SENTRON Powerconfig PC version.

A firmware update is possible for every communication-capable circuit protection device. This can be carried out via the device menu of the SENTRON Powercenter 1000/1100/2000.



The updates are transferred to the SENTRON Powercenter 1000/1100/2000 via the Ethernet cable if the Bluetooth® function is switched off. The connected terminal devices receive their update automatically via wireless transmission from the SENTRON Powercenter 1000/1100/2000, even if they are not set up in the Powerconfig project. As a result of wireless communication, it can result in longer wait times. The progress of the system update can be checked in Powerconfig or restarted in the event of an error. Set parameters are maintained in the devices after a firmware update. Devices are restarted after a firmware update. No data are transmitted during this time.

The duration of a firmware update depends on the capacity utilization of the radio channels. An update of a SENTRON Powercenter usually takes approx. 2 minutes. It takes about 5 minutes per terminal device, although it may take 10-15 minutes for the 3NA COM fuse. To save time here, the firmware update is started for several devices simultaneously.

Note

All devices must be permanently supplied with power during the firmware update for it to be successful.

In the case of the 3NA COM fuse, a continuous current flow of at least 10 A through the fuse must also be guaranteed.

It is recommended to perform an update on the SENTRON Powercenter first before pairing new terminal devices with it. This serves to ensure that a new terminal device or its firmware version is supported by the SENTRON Powercenter. It is also recommended to read out the new firmware version after the update and to perform a device test, if available, using the test button or a command.

The SENTRON Powercenter 1000 supports functions of terminal devices only up to version V4.0. More recent terminal devices and functions can only be used in conjunction with Powercenter 1100/2000. See the section Overview of compatibility (Page 28).

Note

During the firmware update of a 5TY1 COM ECPD, the protection function is briefly interrupted. The update must be performed during a quiet operating time for this reason. The device also changes to the Standby (STBY) status briefly when it is restarted. This means that the loads are not supplied with power for a short time.

9.3 Disposal of waste electronic equipment

Disposal of waste electronic equipment

Waste electronic equipment must not be disposed of as unsorted municipal waste, e.g. household waste. When disposing of waste electronic equipment, the current local national/international regulations must be observed.

FAQs

10

You can find more FAQs in the SiePortal

https://sieportal.siemens.com/ → Knowledge base → Type: Other entry types: FAQ

10.1 Error on commissioning

Fault description	Solutions
The LEDs are not lit	Check the power supply units.
No SENTRON Powercenter 1000/1100/2000 found in the list of available Bluetooth® devices	• Check whether the mobile device has activated Bluetooth® and the GPS data • Check whether the SENTRON Powercenter 1000/1100/2000 has been set to Bluetooth® mode with a short button press (LED flashes green at 2 Hz for max. 180 s if a connection cannot be established) • If another device is connected to the SENTRON Powercenter 1000/1100/2000, or tries to connect, the Bluetooth® connection can be disconnected using the button. After this try again • Switch Bluetooth® mode on again and check whether the manual entry of the PIN code is correct
SENTRON Powercenter 1000/1100/2000 can no longer be connected to a mobile device that has already been paired	Perform a new Bluetooth® search. If the device is displayed but cannot be paired, reset everything and perform Bluetooth® commissioning again: • Unpair SENTRON Powercenter 1000/1100/2000 with a long button press (> 10 s) and reset the Bluetooth® keys • Remove SENTRON Powercenter 1000/1100/2000 in the operating system under the connected devices • Delete SENTRON Powercenter 1000/1100/2000 from the app project • Activate Bluetooth® on the mobile device and SENTRON Powercenter 1000 with a button press < 3 s (COM LED flashes green at 2 Hz) • Perform Bluetooth® search and add device incl. scan process and PIN entry

Fault description	Solutions
No SENTRON Powercenter 1000/1100/2000 found in the WLAN search	• Check whether the mobile device is also connected to the same network • Update the list once again • Check the router settings • Unplug and plug in the Ethernet cable on the SENTRON Powercenter 1000/1100/2000 and perform search again
The pairing is running in a timeout	• Check the power supply of the device • Pairing is running in the background, even if the timeout is displayed after 60 seconds • If wait times are too long, unpair the devices, reset the devices with a long button press ≥ 10 s and repeat the pairing process
SENTRON Powercenter 1000/1100/2000 no longer supplies any data after commissioning	• Check whether the mobile device is also connected to the same network as the SENTRON Powercenter 1000/1100/2000 • Check whether the SENTRON Powercenter 1000/1100/2000 has been assigned a different IP address by carrying out the WLAN search again • Check the power supply. Are the LEDs lit? • Check whether the LEDs of the devices are permanently green • Unplug and plug in the Ethernet cable on the SENTRON Powercenter 1000/1100/2000 • Restart the devices (disconnect power supply or switch off devices using the operating lever)
The devices no longer supply any data	• Check that communication with the SENTRON Powercenter 1000/1100/2000 is functioning properly. Is the data transceiver supplying values? • Check the power supply and the LEDs • Restart the devices (disconnect power supply or switch off devices) • Disconnect the terminal device from the SENTRON Powercenter 1000/1100/2000 with a long button press on the terminal device or carry out the Unpair function with the app and then pair the terminal device again
WLAN search is not finding any devices with the existing VPN connection	For security reasons, the IP address of the SENTRON Powercenter 1000/1100/2000 can only be entered manually via a VPN connection
Time line of the trends and time stamp of the messages do not match	Check the system time of the SENTRON Powercenter 1000/1100/2000 and re-synchronize the time with the mobile terminal device or check the SNTP server

Fault description	Solutions
Devices flash yellow permanently (device error)	• Switch power supply or device on and off • Remove possible sources of radio interference to rectify a communication error • Reset with a long button press ≥ 10 s to exclude communication error • Replace devices if device error persists
Device flashes red continuously (tripping operation active)	Confirm the tripping operation with a short button press
Device flashes green/yellow (limit warning) or yellow/red (end of service life warning)	• Check the active alarm messages • Check the alarm parameters that are switched on and their threshold values (increase threshold value if necessary) • Check the status of the final circuit (an overload tripping operation may occur soon)

10.2 Error with Modbus TCP connection

Fault description	Solutions
Devices not reachable	• Check power supply (communication only possible if the device is supplied with power. If necessary, the device has tripped) • Check the correct device address • Check the correct register
Data point provides incorrect value	• Check the correct device address and register of the desired device (each terminal device does not support each data point) • Check whether the start address of the register has been decremented by -1 for readout
Parameters cannot be modified	• Check the correct function code • Check the value range

10.3 Error on MQTT connection

Error description	Possible solutions
Cloud connection is not possible	• If a static IP address is used, cloud functionality is not supported. Check the settings and activate DHCP.
The "Load to device" function cannot be executed.	• Check that all terminal devices are switched on and connected.

10.4 Error with firmware update

Fault description	Solutions
Update not possible	• Check the power supply • Check that communication is error-free • Check that the correct firmware version is correct (this must be higher than the current one) • Check that the device type is correct • Restart firmware update
Update runs into a timeout	• Restart update

Technical specifications

11

You can find detailed data sheets under:

https://sieportal.siemens.com/ → Knowledge base → Type: Technical specifications

11.1 SENTRON Powercenter 1000/1100/2000

Designation	Value	Value	Value
Order number	7KN1110-0MC00	7KN1111-0MC00	7KN1210-0MC00
Product name	SENTRON Powercenter 1000	SENTRON Powercenter 1100	SENTRON Powercenter 2000
Enclosure version	DIN rail instrument		
Suitability for application	5ST3 COM, 5SL6 COM, 5SV6 COM, 3NA COM, 3RV2 COM From firmware V2.0: 5SL6 COM with RCM function From firmware V3.0: 3RV2 COM, 5ST3 COM RCA From firmware V4.0: 5TY1 COM ECPD (basic function only)	5ST3 COM, 5SL6 COM, 5SV6 COM, 3NA COM, 3RV2 COM, 5SL6 COM, 3RV2 COM, 5ST3 COM RCA, 5TY1 COM ECPD, 5SV8 COM RCM, 5TT4 COM DIDO	
Number of supported devices	24		
Supply voltage	24 V DC SELV		
Standard for Bluetooth® wireless communication	V5.1		
EU Radio Equipment Directive (RED)	2014/53/EU		
RF protocol transmission frequency	2400 - 2483.5 MHz		
Radio transmit power	< 4.5 dBm (BLE), < 1.5 dBm (RF)		
Protocol supported: Modbus TCP	Yes		
Protocol supported: https via REST API	No	Yes	
Protocol supported: MQTT	No	No	Yes
Number of Ethernet ports	1	2	
Write protection available	No	Yes	
Frame size (MW)	1		

11.2 5ST3 COM auxiliary switch and fault signal contact

Designation	Value
Order number	5ST30620MC
Product name	5ST3 COM auxiliary switch/fault signal contact
Enclosure version	DIN rail, not attached to main device
Supply voltage	24 V DC (SELV)
Product expansion can be mounted	Universal (CB, RCCB, RCBO, AFDD ON/OFF switch 5TL1 remote control auxiliary)
Typical electrical endurance (operating cycles)	10000
EU Radio Equipment Directive (RED)	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz
Radio transmit power	2.5 dBm
Frame size (MW)	0.5

11.3 5SL6 COM miniature circuit breaker

Designation	**Value**	**Value**
Order number	5SL60xx-yMC (xx = 02, 04, 06, 08, 10, 13, 16, 20, 25, 32; y = 6 or 7)	5SL60xx-yMF (xx = 02, 04, 06, 08, 10, 13, 16, 20, 25, 32; y = 6 or 7)
Product name	5SL6 COM compact miniature circuit breaker with power measurement	5SL6 COM miniature circuit breaker with RCM function and power measurement
According to product standard	EN 60898-1	EN 60898-1 and for RCM: IEC 62020-1
Residual current monitoring type	---	F
Operational current for AC rated value	2 A, 4 A, 6 A, 8 A, 10 A, 13 A, 16 A, 20 A, 25 A, 32 A	
Tripping characteristic class	B and C	
Supply voltage for AC rated value	230 V	
Current breaking capacity acc. to EN 60898 rated value	6 kA	
Number of poles	1 pole + N (N could be omitted on the output side)	1 pole + N
Typical mechanical endurance (operating cycles)	10000	
Measurable load current with AC	0.04 A ... 2 x I_n	
EU Radio Equipment Directive (RED)	2014/53/EU	
RF protocol transmission frequency	2400 - 2483.5 MHz	
Radio transmit power	10 dBm	
Frame size (MW)	1	

11.4 5SV6 COM arc fault detection device

Designation	Value
Order number	5SV6016-xMCyy (x= 6 or 7, yy= 06, 10, 13, 16, 20, 25, 32)
Product name	LS-combo 5SV6 COM arc fault detection device with power measurement
According to product standard	IEC/EN 60898-1
Operational current for AC rated value	6 A, 10 A, 13 A, 16 A, 20 A, 25 A, 32 A
Tripping characteristic class	B and C
Supply voltage for AC rated value	230 V
Supply voltage frequency rated value	50 Hz
Number of poles	1 pole + N
Typical mechanical endurance (operating cycles)	10000
Measurable load current with AC	0.04 A ... 2 x I_n
EU Radio Equipment Directive	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz
Radio transmit power	10 dBm
Frame size (MW)	1

11.5 3NA COM fuse

Designation	Value
Order number	3NA32xx-4KK0y (xx = 24, 30, 32, 36, 40, 42, 44, 52; y = 1, 2, 3, 4)
Product name	3NA COM LV HRC fuse
Versions	With and without electronic module
Tripping characteristic class	gG and gFF
Operational current for AC rated value	80 A, 100 A, 125 A, 160 A, 200 A, 224 A, 250 A, 315 A
Supply voltage for AC rated value	400 V
Design of the indicator	Front indicator
Mounting type	Non-insulated grip lugs
Approvals	VDE, KEMA KEUR
EU Radio Equipment Directive (RED)	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz
Frame size	NH2

11.6 3RV2 COM wireless auxiliary and signaling switch for 3RV2 motor starter protectors

Designation	Value
Order number	3RV2921-5M
Product name	3RV2 COM wireless auxiliary and signaling switch
Supply voltage	24 V DC
Product expansion can be mounted	3RV2 motor starter protector
Typical electrical endurance (operating cycles)	10000
EU Radio Equipment Directive (RED)	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz
Radio transmit power	2.5 dBm
Frame size (MW)	1

11.7 5ST3 COM remote control auxiliary (RCA)

Designation	Value	Value
Order number	5ST3072-0MC	5ST3073-0MC
Product name	5ST3 COM remote control auxiliary with ARD	5ST3 COM remote control auxiliary with ARD and RCD test
Product standard	IEC 63024	
Enclosure version	DIN rail, not attached to main device	
Supply voltage	230 V AC (100 ... 240 V AC)	
Product expansion can be mounted	Universal (CB, RCCB, RCBO, AFDD ON/OFF switch 5TL1 remote control auxiliary) with adapter	
Typical electrical endurance (operating cycles)	10000	
Auxiliary switches and fault signal contacts installed	Mechanically and via communication	Only via communication
Remote switching function	Either mechanical (wired) or via communication	
Minimum interval between two commands	10 s	
Minimum response time 1 s	1 s	
EU Radio Equipment Directive (RED)	2014/53/EU	
RF protocol transmission frequency	2400 - 2483.5 MHz	
Radio transmit power	2.5 dBm	
Frame size (MW)	2	2.5

11.8 5TY1 COM electronic circuit protection device (ECPD)

Designation	Value
Order number	5TY1350-3MF06, 5TY1350-3MF10, 5TY1350-3MF16
Product name	5TY1 COM electronic circuit protection device (ECPD)
Operational current for AC rated value	6 A, 10 A, 16 A
Tripping characteristic class	In line with B (instantaneous tripping in the range 3 ... 5 * In / delayed tripping in the range 1.05 - 1.13 * In)
Supply voltage for AC rated value	230 V
Supply voltage frequency rated value	50 Hz
Number of poles	1 pole + N
Typical mechanical endurance (operating cycles)	10000
Measurable load current with AC	0.04 A ... 2 x I_n
EU Radio Equipment Directive (RED)	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz
Radio transmit power	10 dBm
Frame size (MW)	2

11.9 5SV8 COM RCM and MRCD

Table 11- 1 Type A RCM:

Designation	Value	Value
Order number	5SV8022-6MP	5SV8223-6MP
Product name	5SV8 COM RCM residual current monitor	
According to product standard	IEC 62020-1	
Residual current type	A	F
Rated residual current I_{dn}	10 mA ... 30 A	6 mA ... 30 A
Relay contacts	1x alarm	1x pre-alarm 1x alarm
DI/DO	---	1 DI, 2 DO (alarm, pre-alarm)
Summation current transformer compatible	5SV871.-0KK	
Diameter of summation current transformer	20 ... 210 mm	
Number of channels = number of connectable summation current transformers	1	4
Display available	No	Yes
Rotary selector switch available	Yes	No
EU Radio Equipment Directive (RED)	2014/53/EU	
RF protocol transmission frequency	2400 - 2483.5 MHz	
Frame size (MW)	1	2

Table 11- 2 Type B RCM:

Designation	Value	Value
Order number	5SV8022-4MR	5SV8223-4MR
Product name	5SV8 COM RCM residual current monitor	
According to product standard	IEC 62020-1	
Residual current type	B	
Rated residual current I_{dn}	10 mA ... 8 A	10 mA ... 8 A
Relay contacts	1x pre-alarm 1x alarm	1x pre-alarm 1x alarm
Rated voltage relay contact	230 V AC	
DI/DO	1 DI, 2 DO (alarm, pre-alarm)	1 DI, 2 DO (alarm, pre-alarm)
Summation current transformer compatible	5SV871.-2K.	
Diameter of summation current transformer	35 ... 210 mm	
Number of channels = number of connectable summation current transformers	1	4
Display available	No	Yes
Rotary selector switch available	Yes	No
EU Radio Equipment Directive (RED)	2014/53/EU	
RF protocol transmission frequency	2400 - 2483.5 MHz	
Frame size (MW)	2	2

Table 11- 3 MRCD:

Designation	Value	Value
Order number	5SV8122-6MP	5SV8122-4MR
Product name	5SV8 COM modular residual current device (MRCD)	
According to product standard	IEC 60947-2 Annex M	
Residual current type	A	B
Rated residual current I_{dn}	10 mA ... 30 A	Type B 30 mA ... 3 A
Relay contacts	1x alarm	1x pre-alarm 1x alarm
Rated voltage relay contact	230 V AC	
DI/DO	---	1 DI, 2 DO (alarm, pre-alarm)
Number of channels	1	1
Summation current transformer compatible	5SV871.-0KK	5SV871.-2K.
Rotary selector switch available	Yes	Yes
EU Radio Equipment Directive (RED)	2014/53/EU	
RF protocol transmission frequency	2400 - 2483.5 MHz	
Frame size (MW)	1	2

11.10 5TT4 COM digital input/output module

Designation	Value
Order number	5TT4322-2MC
Product name	5TT4 COM digital input/digital output module with communication function
Supply voltage	24 V DC (SELV)
Operating cycles	100000
Number of digital inputs	2
Rated voltage of digital inputs	24 V AC/DC
Number of digital outputs	2
Switching capacity of digital outputs	230 V AC, max. 5 A 30 V DC, max. 5 A 125 V DC, max. 0.2 A
Frame size (MW)	1
EU Radio Equipment Directive	2014/53/EU
RF protocol transmission frequency	2400 - 2483.5 MHz

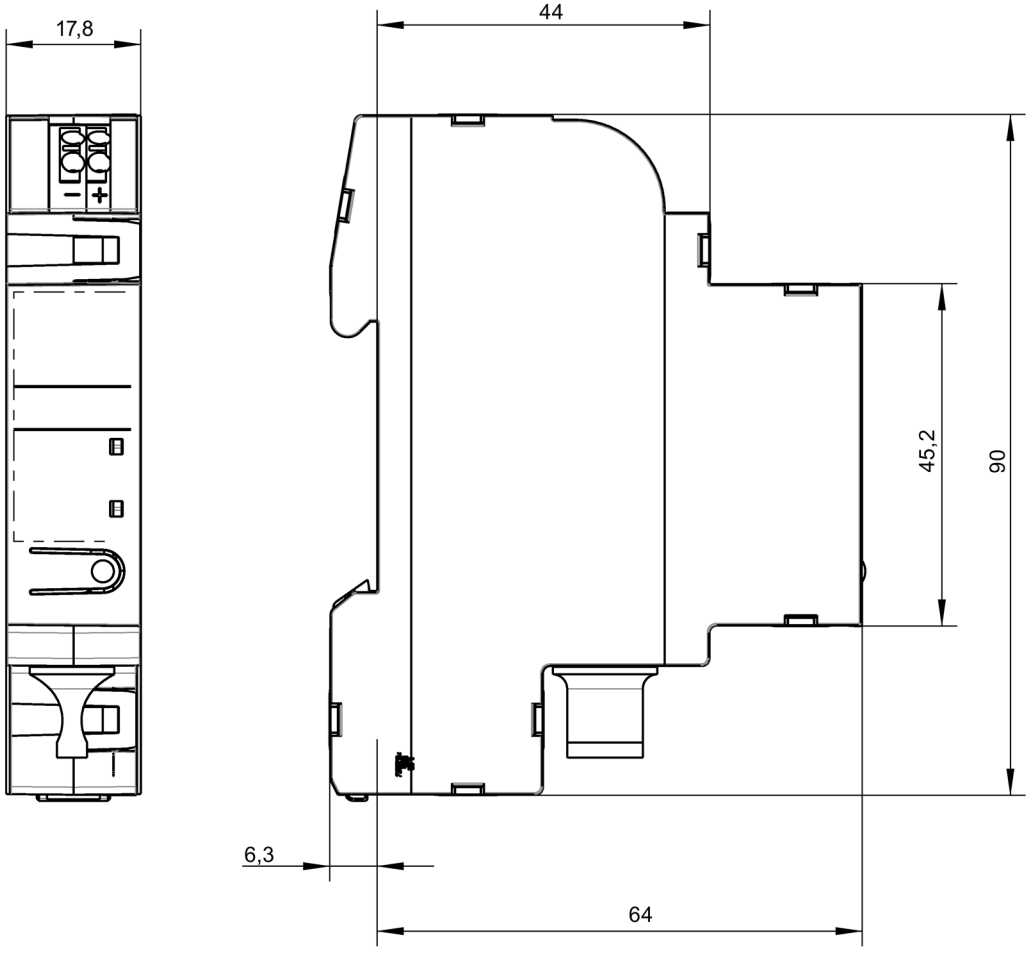
Dimension drawings

12

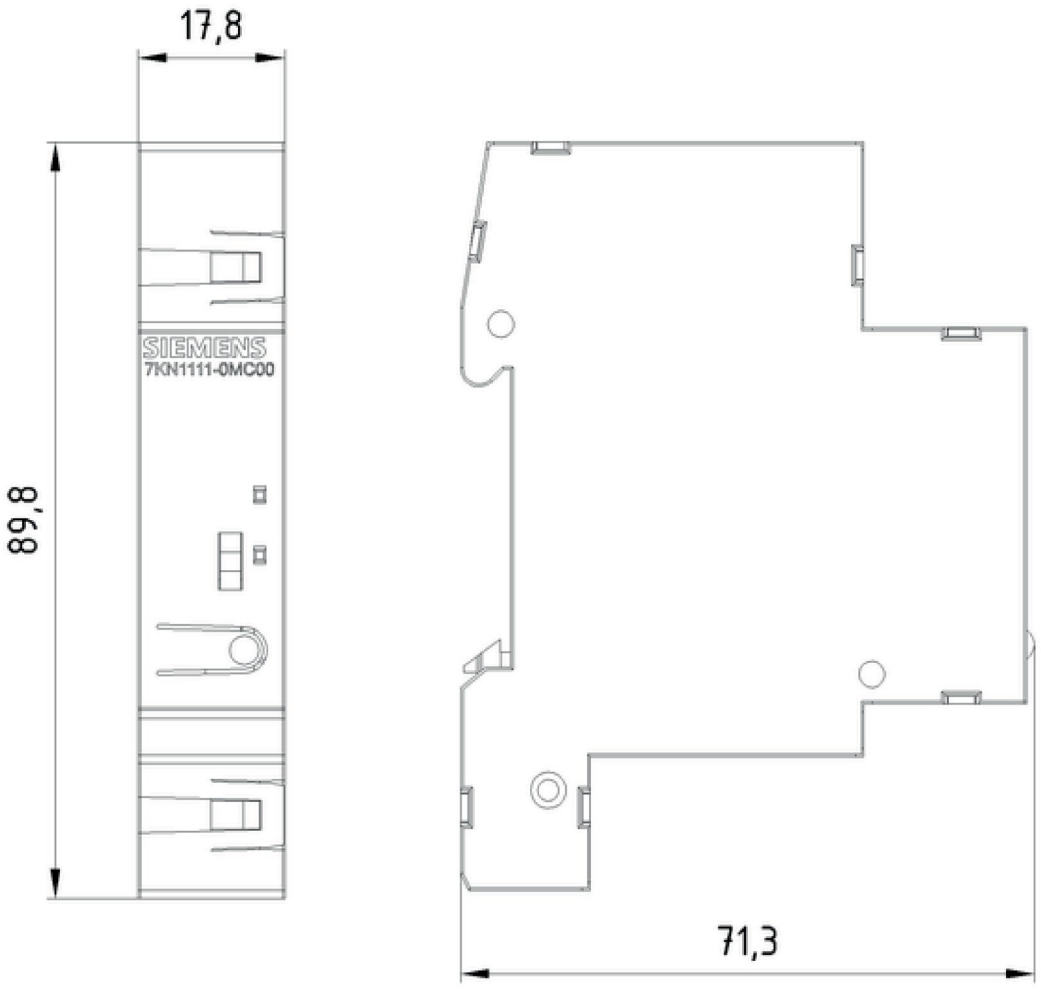
12.1 SENTRON Powercenter 1000/1100/2000

Dimensions in mm

Powercenter 1000

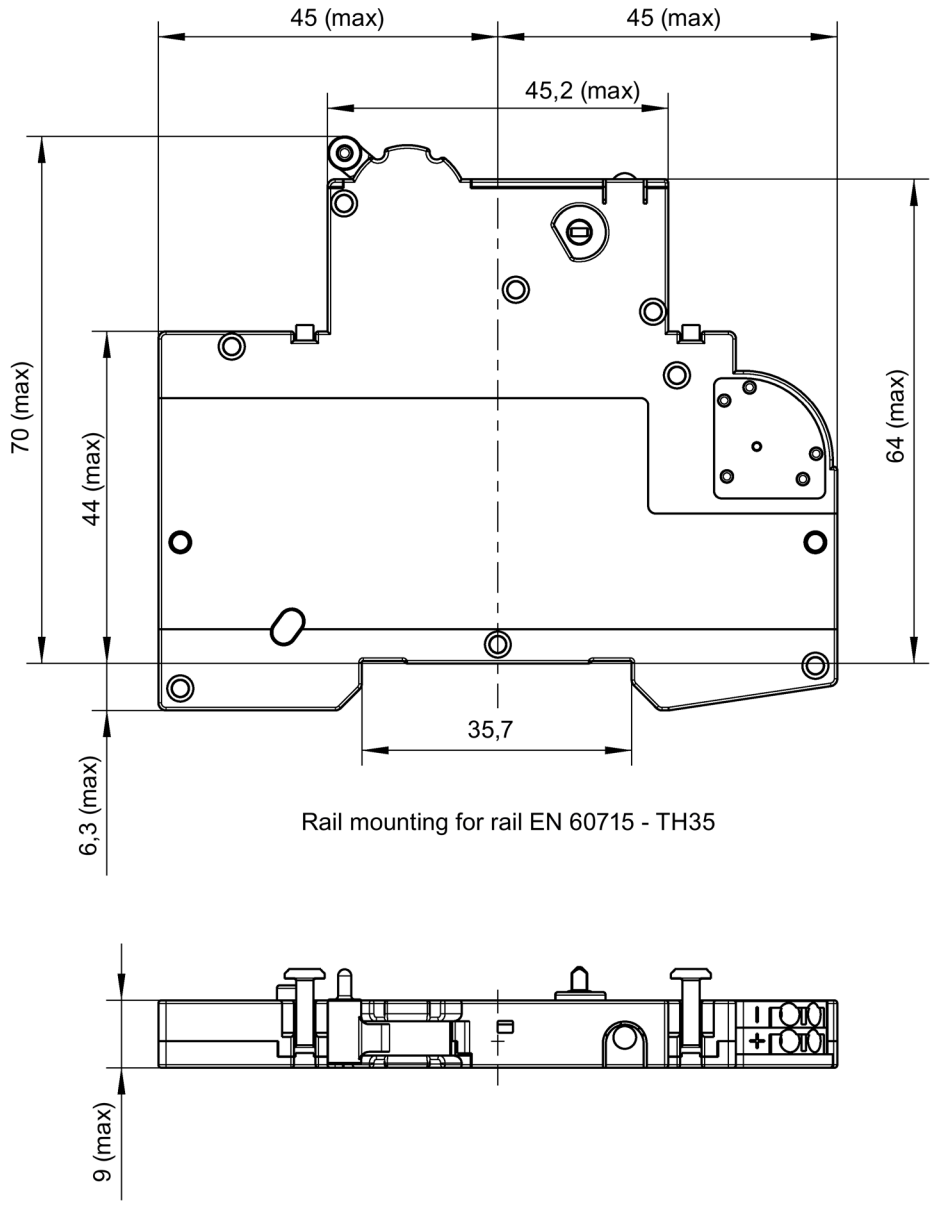


Powercenter 1100/2000



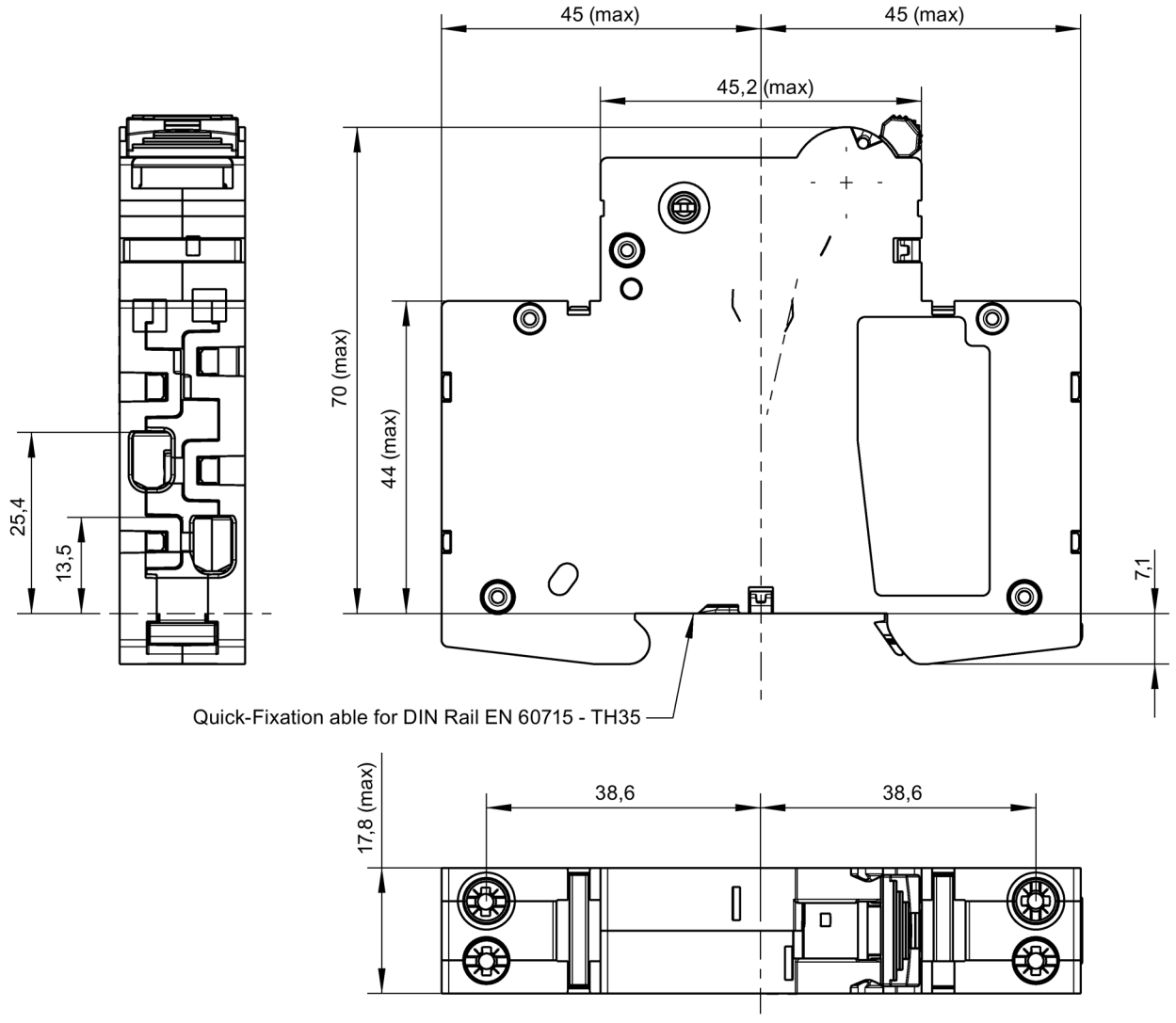
12.2 5ST3 COM auxiliary switch and fault signal contact

Dimensions in mm



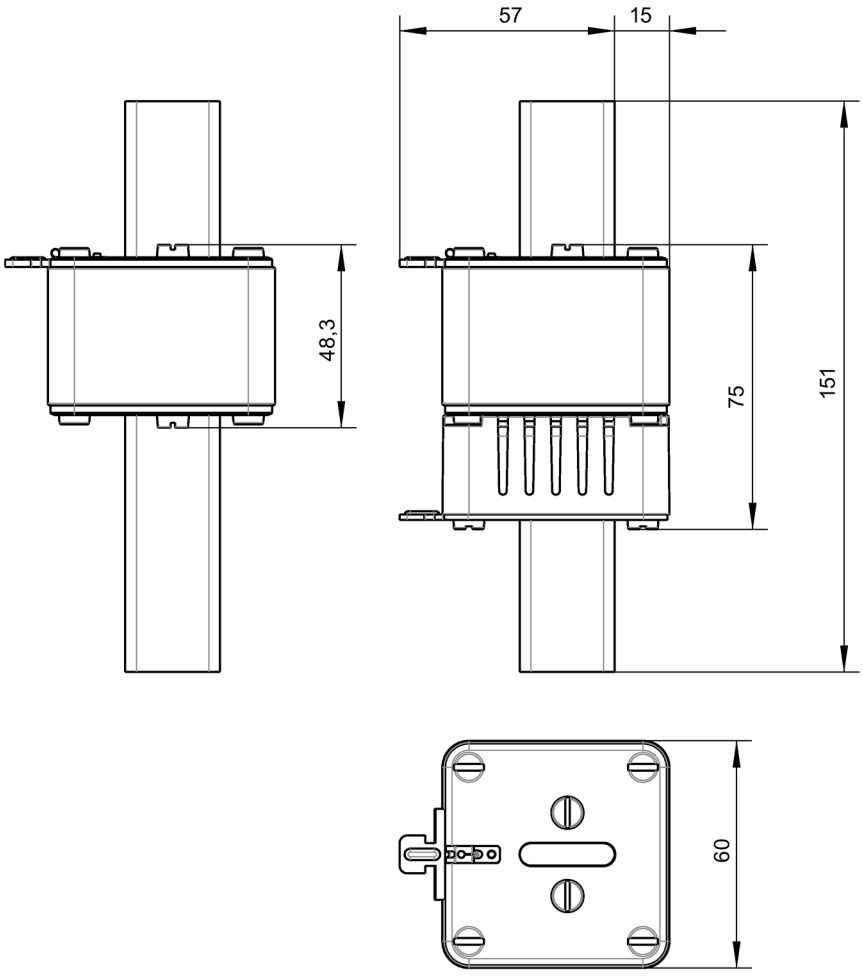
12.3 5SL6 COM / 5SV6 COM miniature circuit breaker and arc fault detection device

Dimensions in mm



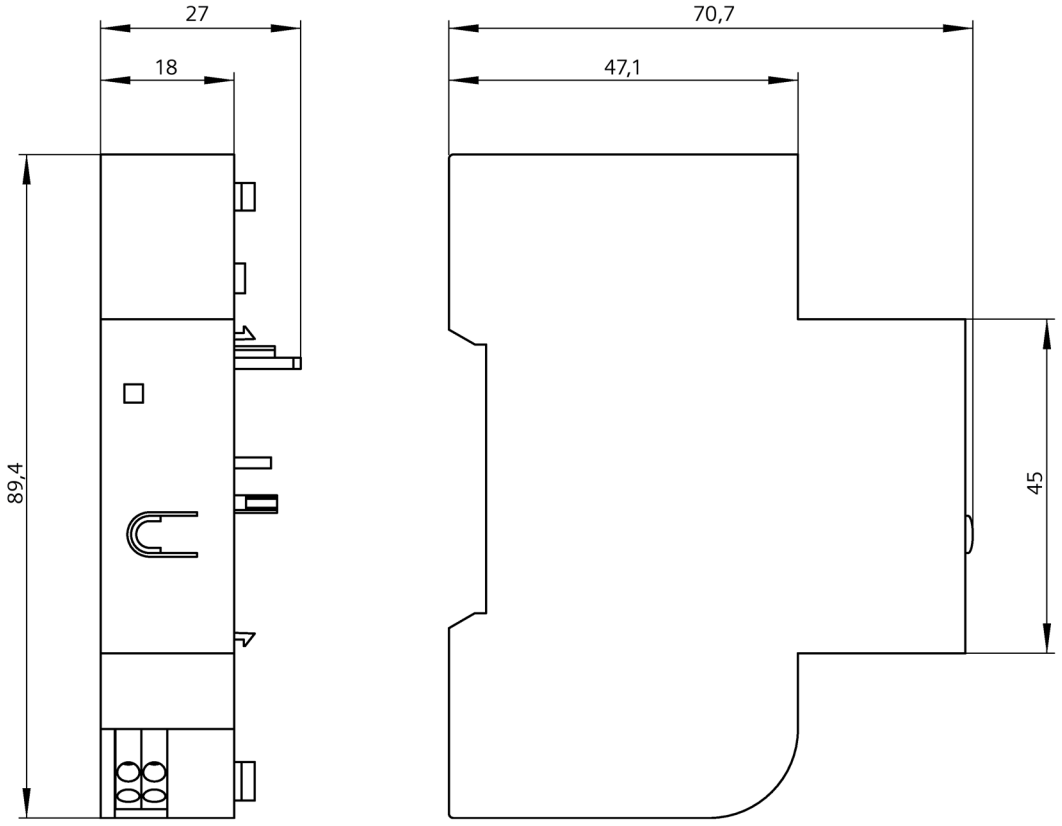
12.4 3NA COM fuse

Dimensions in mm



12.5 3RV2 COM wireless auxiliary and signaling switch for 3RV2 motor starter protectors

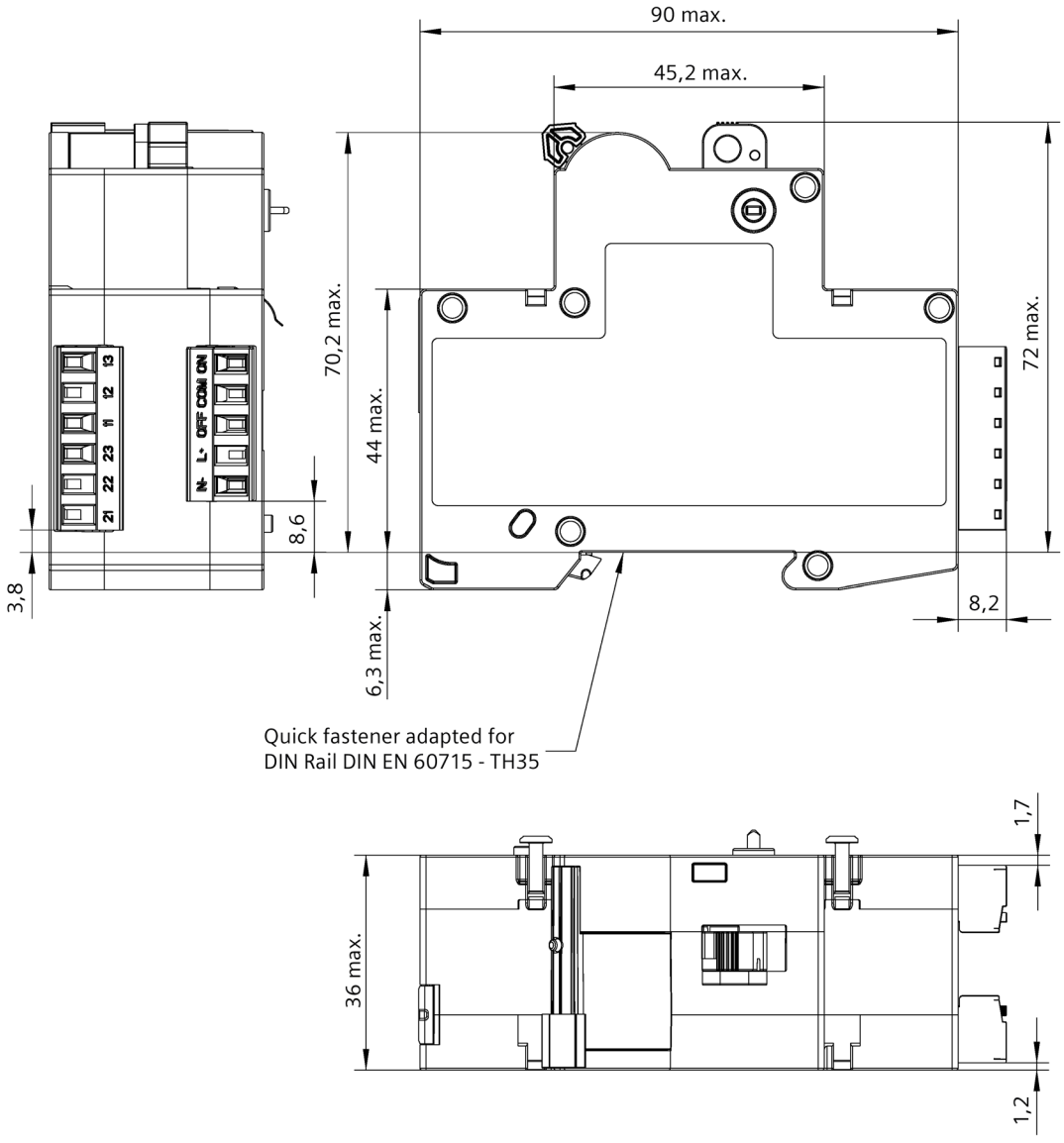
Dimensions in mm



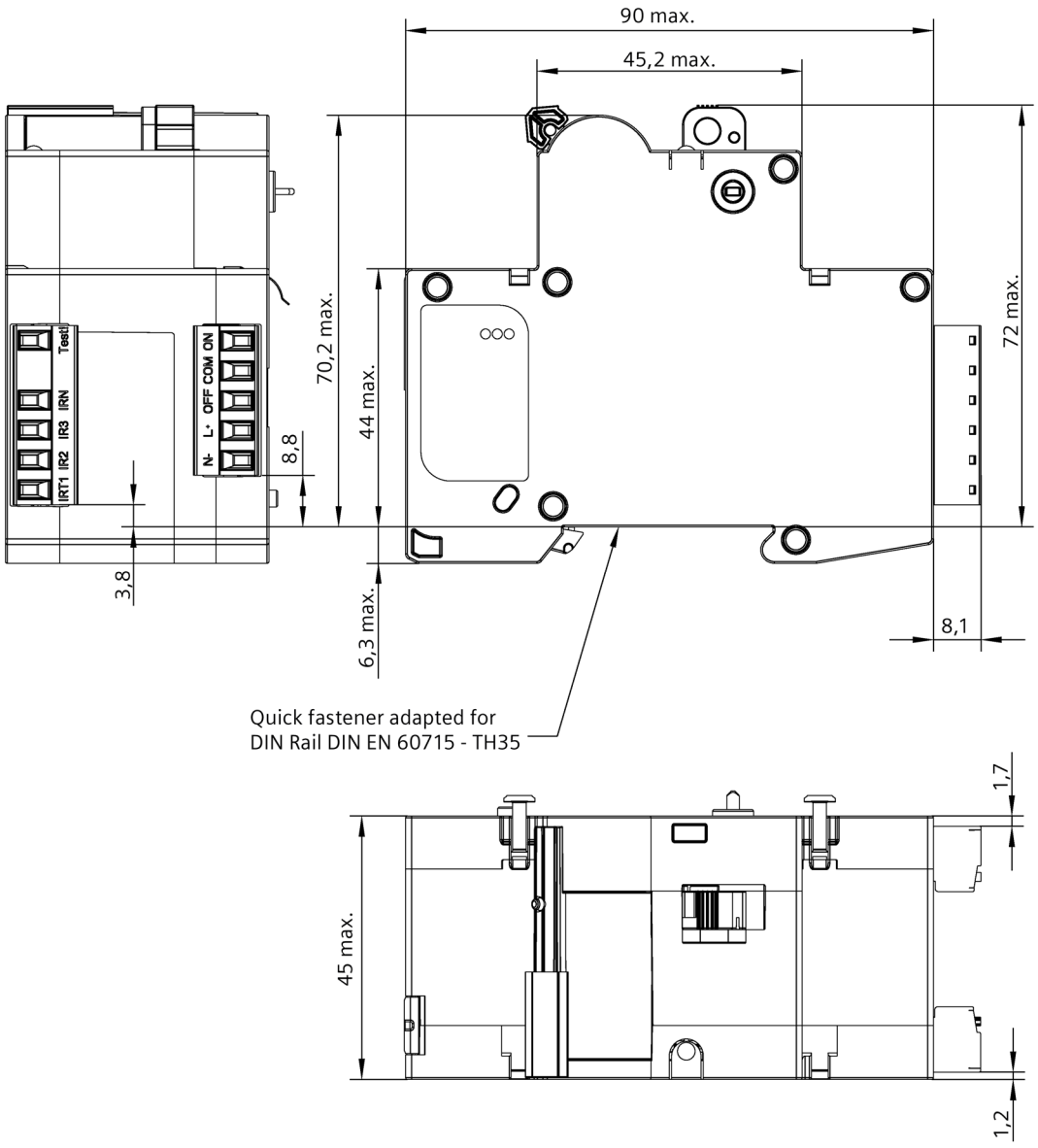
12.6 5ST3 COM remote control auxiliary

Dimensions in mm

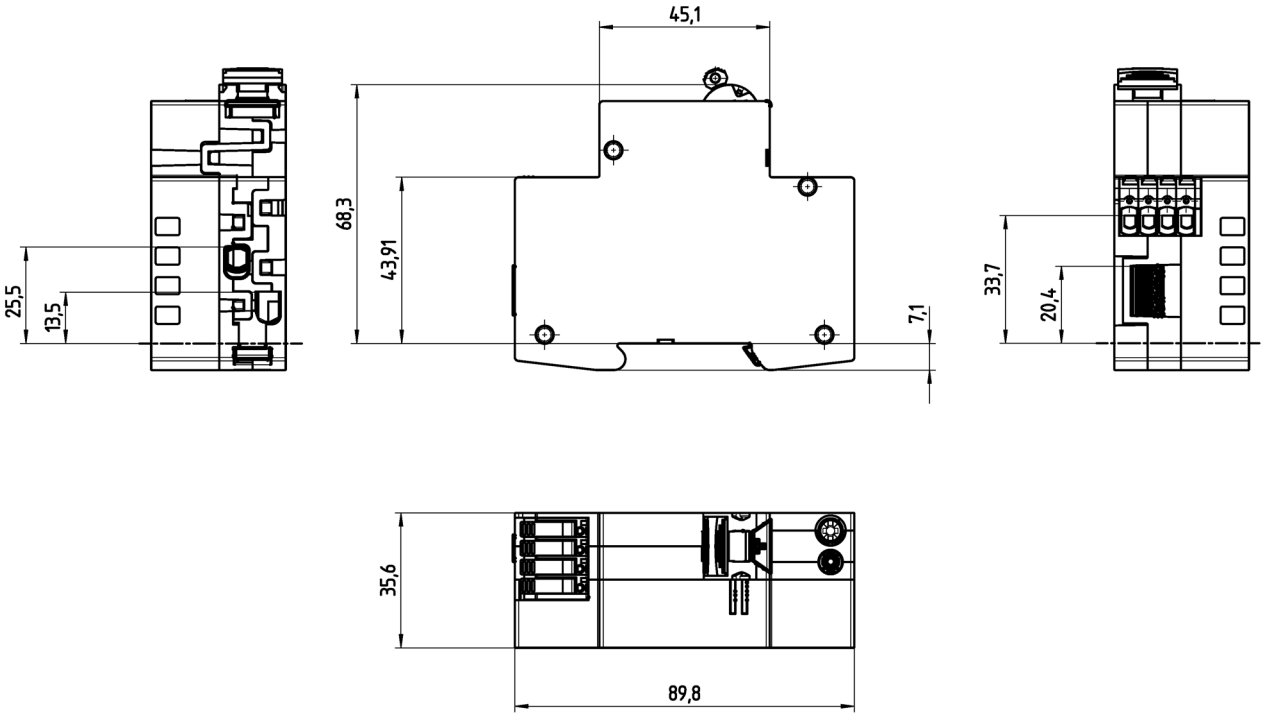
5ST3072-0MC (standard version)



5ST3073-0MC (RCD test version)



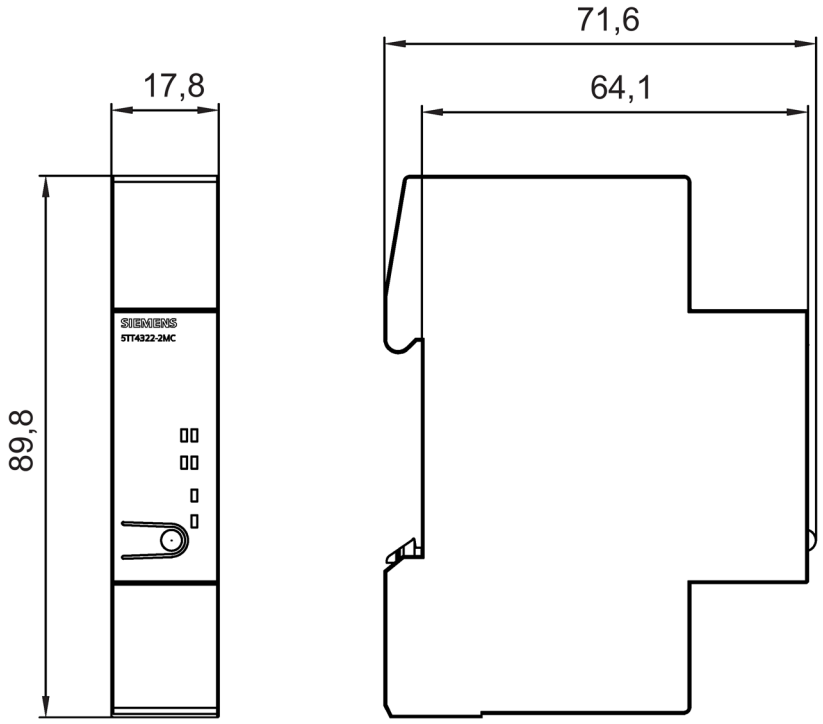
12.7 5TY1 COM electronic circuit protection device (ECPD)



12.8 5SV8 COM RCM

The dimension drawings can be found in the Configuration Manual – 5SV8 residual current measuring devices and modular residual current protective devices (https://support.industry.siemens.com/cs/ww/en/view/109975845)

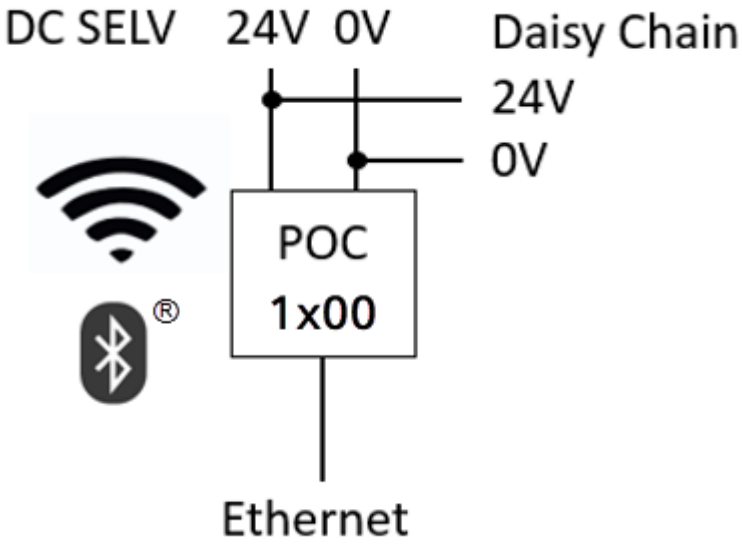
12.9 5TT4 COM digital input/output module



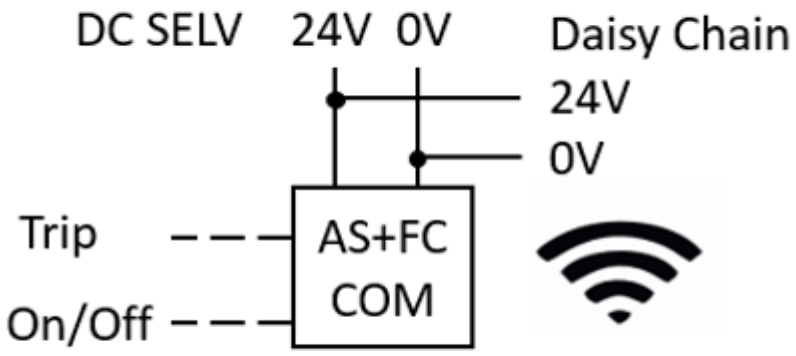
Circuit diagrams

13

13.1 SENTRON Powercenter 1000/1100/2000

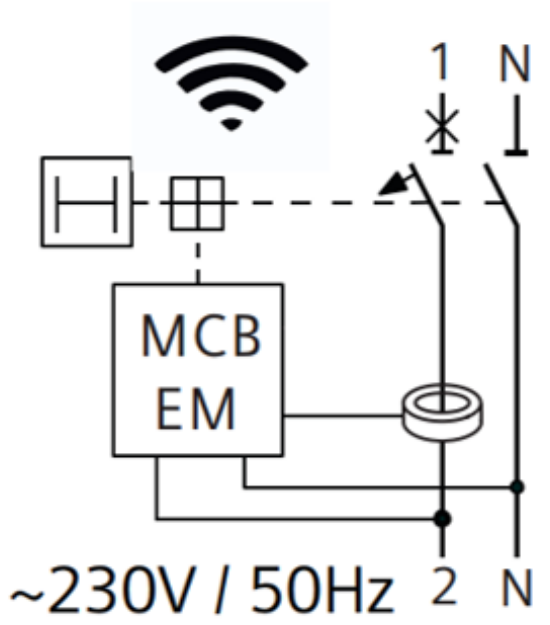


13.2 5ST3 COM auxiliary switch and residual current switch

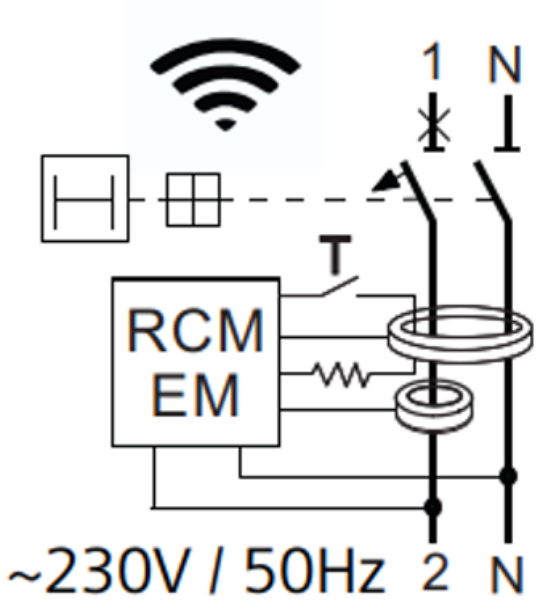


13.3 5SL6 COM miniature circuit breaker

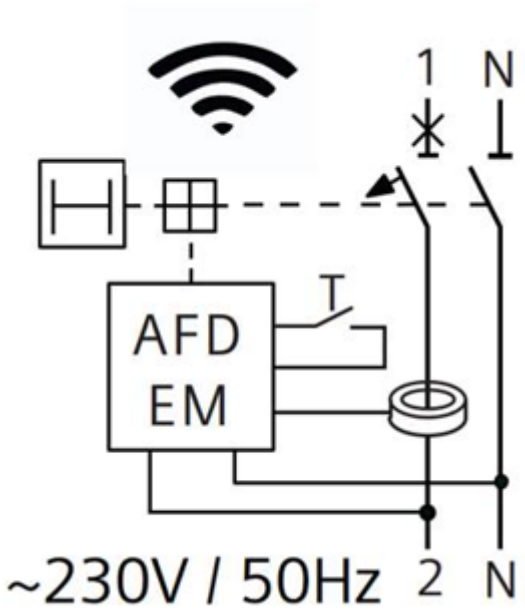
5SL6 COM miniature circuit breaker with power measurement



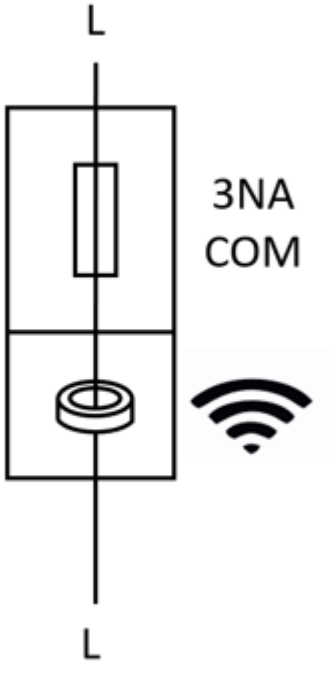
5SL6 COM miniature circuit breaker with power measurement and RCM function



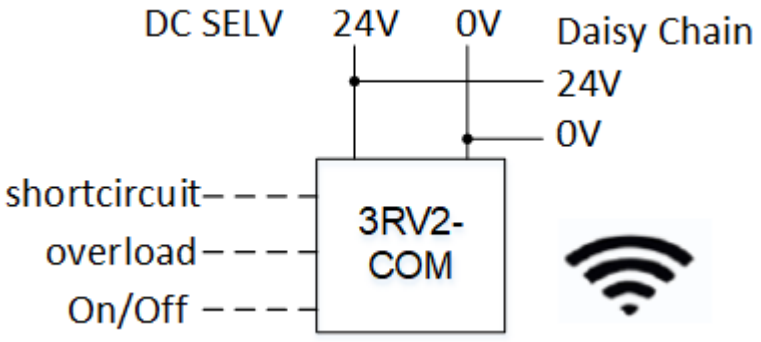
13.4 5SV6 COM arc fault detection device



13.5 3NA COM fuse

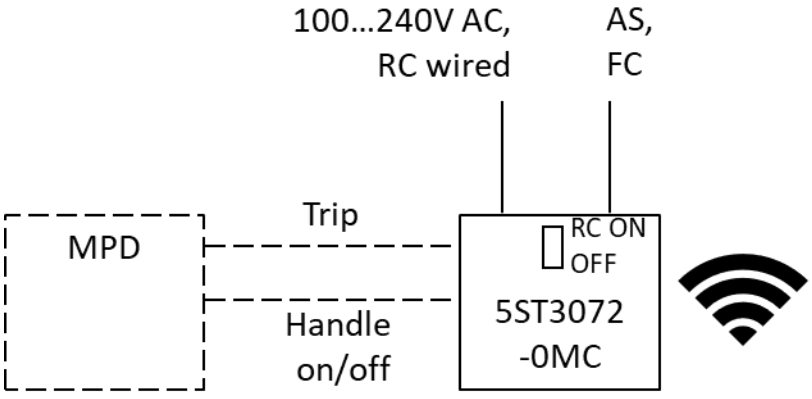


13.6 3RV2 COM wireless auxiliary and signaling switch for 3RV2 motor starter protectors

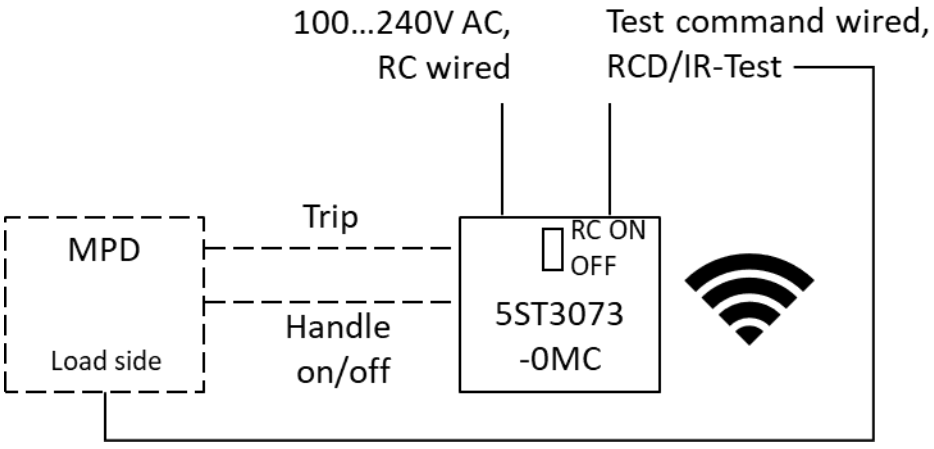


13.7 5ST3 COM remote control auxiliary

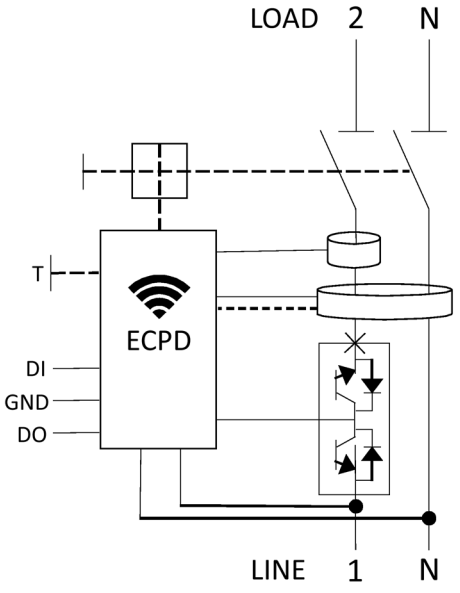
5ST3072-0MC



5ST3073-0MC



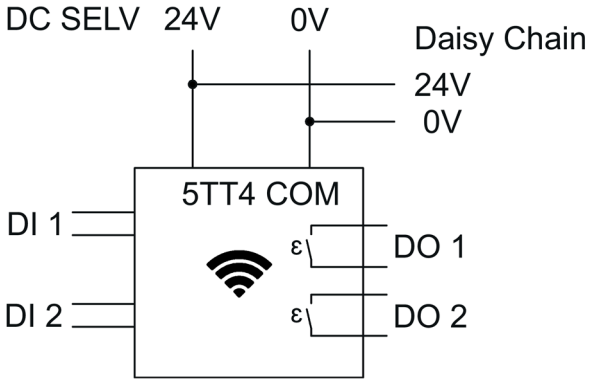
13.8 5TY1 COM electronic circuit protection device



13.9 5SV8 COM RCM

Further information about the circuit diagrams can be found in the Configuration Manual – 5SV8 residual current measuring devices and modular residual current protective devices (https://support.industry.siemens.com/cs/ww/en/view/109975845)

13.10 5TT4 COM digital input/output module



ESD guidelines

A

A.1 Electrostatic sensitive devices (ESD)

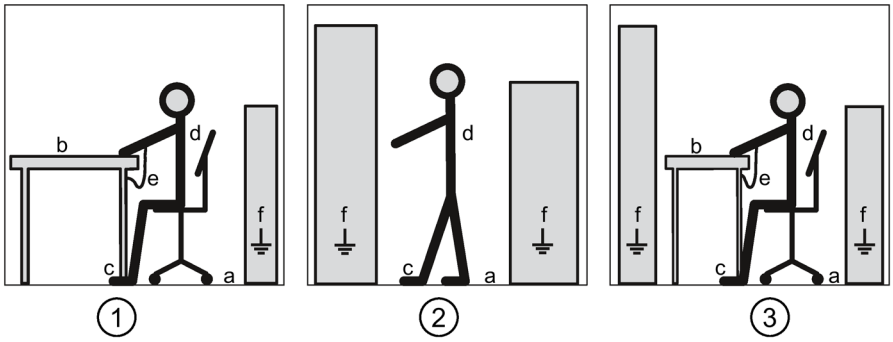
ESD components are destroyed by voltage and energy far below the limits of human perception. Voltages of this kind occur as soon as a device or an assembly is touched by a person who is not electrostatically discharged. ESD components which have been subject to such voltage are usually not recognized immediately as being defective, because the malfunction does not occur until after a longer period of operation.

ESD Guidelines

NOTICE
Electrostatic sensitive devices Electronic modules contain components that can be damaged by electrostatic discharge as a result of improper handling. • You must discharge your body electrostatically immediately before touching an electronic module. To do this, touch a conductive, grounded object, e.g., a bare metal part of a switch cabinet or the water pipe. • Always hold the component by the plastic enclosure. • Electronic modules should not be brought into contact with electrically insulating materials such as plastic film, plastic parts, insulating table supports or clothing made of synthetic fibers. • Always place electrostatic sensitive devices on conductive bases. • Always store and transport electronic modules or components in ESD-safe conductive packaging, e.g. metalized plastic or metal containers. Leave the component in its packaging until installation.

NOTICE
Storage and transport If you have to store or transport the component in non-conductive packaging, you must first pack the component in ESD-safe, conductive material, e.g., conductive foam rubber, ESD bag.

The diagrams below illustrate the required ESD protective measures for electrostatic sensitive devices.



(1) ESD seat

(2) ESD standing position

(3) ESD seat and ESD standing position

Protective measures

a Conductive floor

b ESD table

c ESD footwear

d ESD smock

e ESD bracelet

f Cubicle ground connection

List of abbreviations

B

Abbreviations

AFDD	Arc Fault Detection Device
ARD	Automatic reclosing function (Auto Reclosing Device)
DA	Delayed Acknowledge
DHCP	Dynamic Host Configuration Protocol
DIDO	Digital Input/Digital Output
DMC	Data Matrix Code
ECPD	Electronic Circuit Protection Device
FI or RCD	Residual current device
IR	Insulation Resistance
MCB	Miniature Circuit Breaker
MRCD	Modular Residual Current protective Device
RBAC	Role Based Access Control
RCA	Remote Control Auxiliary
RCM	Residual Current Monitoring
RF	Radio Frequency
RMS	Used here as an abbreviation for the combination of AC & DC measured values for RCM devices (does not indicate mean value)
RSSI	Received Signal Strength Indicator
SSA	Siemens Security Advisory
I_n	Rated current
IoT	Internet of Things
U_n	Rated voltage

Published by
Siemens AG

Smart Infrastructure
Electrical Products
P. O. Box 10 09 53
93055 Regensburg, Germany

For the U.S. published by
Siemens Industry, Inc.
Electrical Products North America
3617 Parkway Lane
Peachtree Corners, GA 30092
United States

Further information

Always at your disposal: our extensive support
www.siemens.com/online-support

SI EP
online