Wireless Controller ARC600

User Manual

Document ID: 1MRS758459
Issued: 2023-03-30
Revision: J
Product version: 3.4

Copyright

Trademarks

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

abb.com/mediumvoltage

Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of anti virus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment. In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2014/30/EU) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2014/35/EU). This conformity is the result of tests conducted by ABB in accordance with the product standard EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

Safety information

Dangerous voltages can occur on the connectors, even though the auxiliary voltage has been disconnected.

Non-observance can result in death, personal injury or substantial property damage.

Only a competent electrician is allowed to carry out the electrical installation.

National and local electrical safety regulations must always be followed.

The frame of the device has to be carefully earthed.

This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment or as part of such equipment in any hazardous environment requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the hardware or software described in this manual could lead directly to death, personal injury, or severe physical or environmental damage.

To prevent damage both the product and any terminal devices must always be switched off before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. The output voltage of the power supply should be checked before connecting any power cables.

The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.

Contents

1 Introduction

1.1 This manual

The user manual provides introductory information as well as detailed instructions on how to set up and manage the device as part of a network environment.

1.2 Intended audience

This manual addresses the personnel involved in installing and managing the devices.

The personnel is expected to be familiar with basic working principles of Internet technology.

1.3 Product documentation

1.3.1 Product documentation set

Product series- and product-specific manuals can be downloaded from the ABB Web site *abb.com/mediumvoltage*.

1.3.2 Document revision history

Document revision/ date	Product version	History
A/2015-12-18	A	First release
B/2017-09-22	3.4	Content updated to correspond to the product version
C/2019-04-24	3.4.7	Content updated to correspond to the product version
D/2021-02-25	3.4.7	Content updated
E/2021-05-31	3.4.7	Content updated
F/2021-06-04	3.4.7	Content updated
G/2021-12-10	3.4.7	Content updated
H/2022-06-20	3.4	Content updated
J/2023-03-30	3.4	Content updated

Download the latest documents from the ABB Web site *abb.com/mediumvoltage*.

1.3.3 Related documentation

Name of the document	Description	Document ID
Arctic Cyber Security Deployment Guideline		1MRS758860
3G/LTE configuration guide Technical Note	Configuring Wireless Gateways, Controllers and M2M Gateway	1MRS758449
3G/LTE Wireless Gateway firmware update Technical Note	Updating firmware of Wireless Gateway devices	1MRS758451
Wireless Controller RTU_interoperability Technical Note	ARC600 RTU application configuration	1MRS758476
Wireless Controller RTU configuration guide Technical Note	IEC 60870-5-104 and IEC 60870-5-101 interoperability	1MRS758477

Product series- and product-specific manuals can be downloaded from the ABB Web site *abb.com/mediumvoltage*.

1.4 Symbols and conventions

1.4.1 Symbols

The electrical warning icon indicates the presence of a hazard which could result in electrical shock.

The warning icon indicates the presence of a hazard which could result in personal injury.

The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.

The information icon alerts the reader of important facts and conditions.

The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged

equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

1.4.2 Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.

  Select **Main menu** > **Settings**.
- Parameter names are shown in italics.

  The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks.

  The corresponding parameter values are "On" and "Off".

2 ARC600 overview

2.1 Overview

Wireless Controller ARC600 is a compact, solution based device for remote controlling and monitoring of secondary substations, such as network disconnectors, load break switches and ring main units (RMU) in distribution networks. It enables the SCADA system to wirelessly monitor and control the field devices over the public communication infrastructure (cellular network). Wireless Controller ARC600 utilizes the built-in wireless communication features for reliable and secure end-to-end communication providing remote monitoring and control of three switching devices and can be expanded as required by using external I/O expansion modules.

The use of Wireless Controller ARC600 in distribution networks improves the quality of power distribution and reduces the outage time in the affected areas. Areas directly adjacent to these affected areas show reduced outages and overall effects. This also reduces the capital expenditures in the distribution network by allowing integration of legacy devices and contributes to more direct cost savings by facilitating preventative maintenance. The operational expenditure can be reduced by lowering the System Average Interruption Duration Index (SAIDI) and System Average Interruption Frequency Index (SAIFI), resulting in lower penalties for undelivered energy. Wireless Controller ARC600 is also ideally suited to be retrofitted to existing applications thus enabling the remote control of these devices and further extending the life cycle of the switching devices itself.

Typically, the IEC-104 protocol is utilized for communication to the SCADA system but for the existing installations with a IEC-101 line or modem, Wireless Controller ARC600 supports also IEC-101 communication (including dial-up) to the SCADA system.

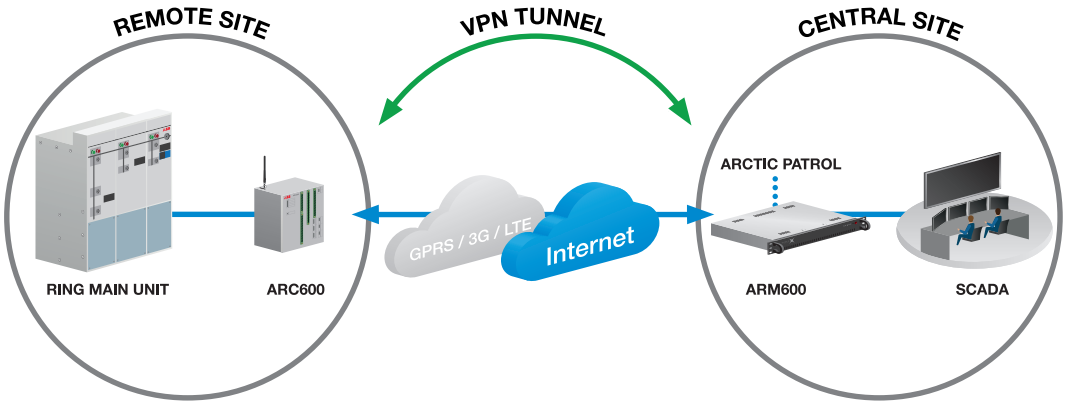

Figure 1: Communication system overview with Wireless Controller ARC600 and ring main unit

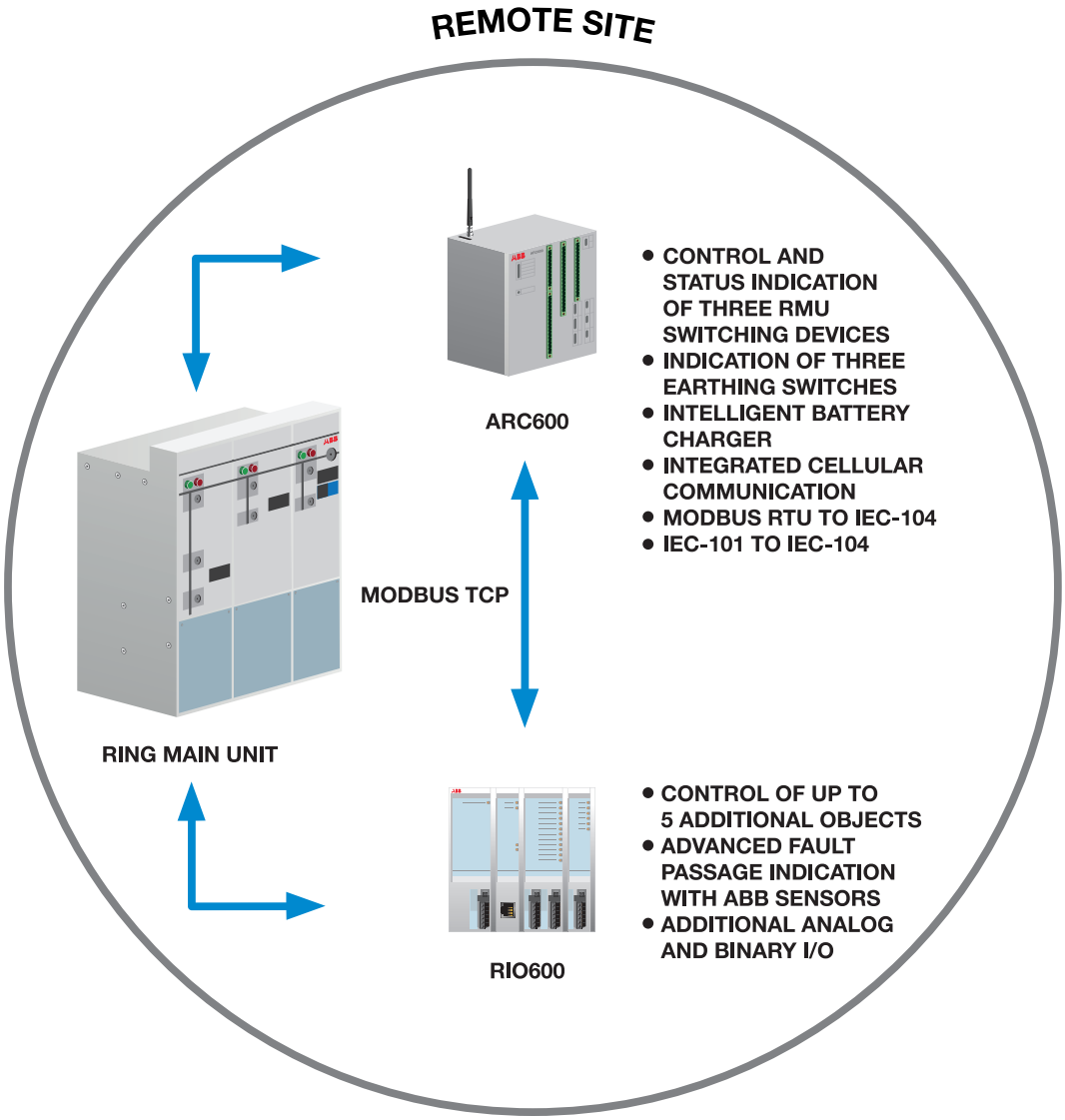

Figure 2: Wireless Controller ARC600 at remote site connected with ring main unit and RIO600. RTU monitoring and control combined with directional fault passage indication example.

2.2 Physical interfaces

2.2.1 Front panel

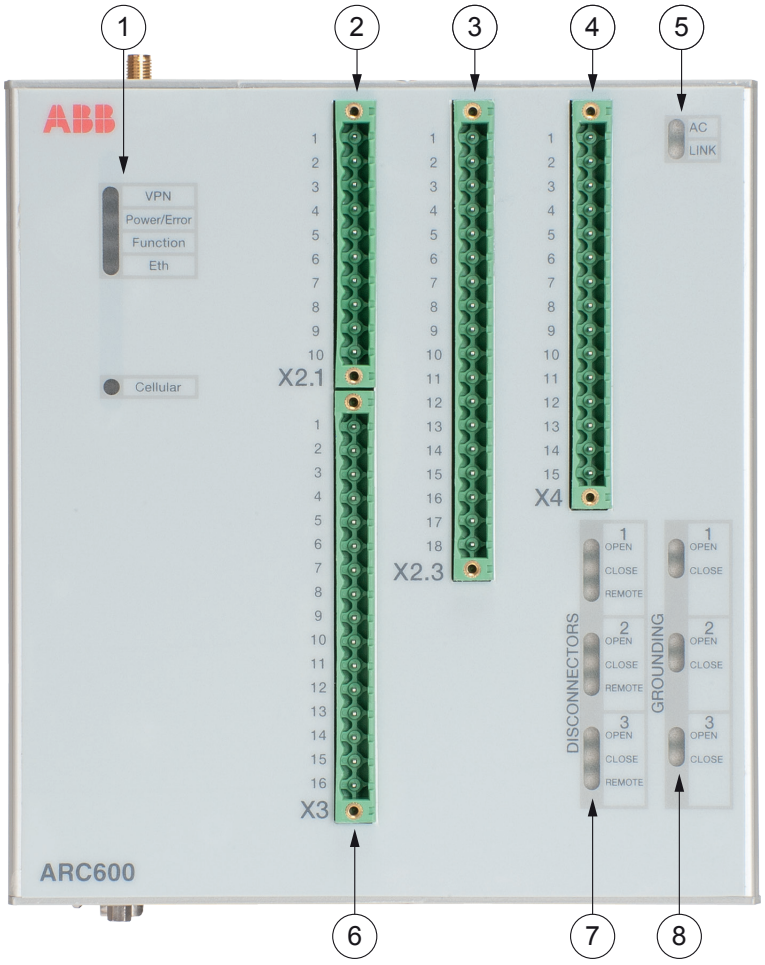

Figure 3: Front panel

1 System status LEDs
2 X2.1 connector
3 X2.3 connector
4 X4 connector
5 AC and LINK LEDs
6 X3 connector
7 Disconnector status LEDs
8 Grounding disconnector status LEDs

2.2.2 Serial panel

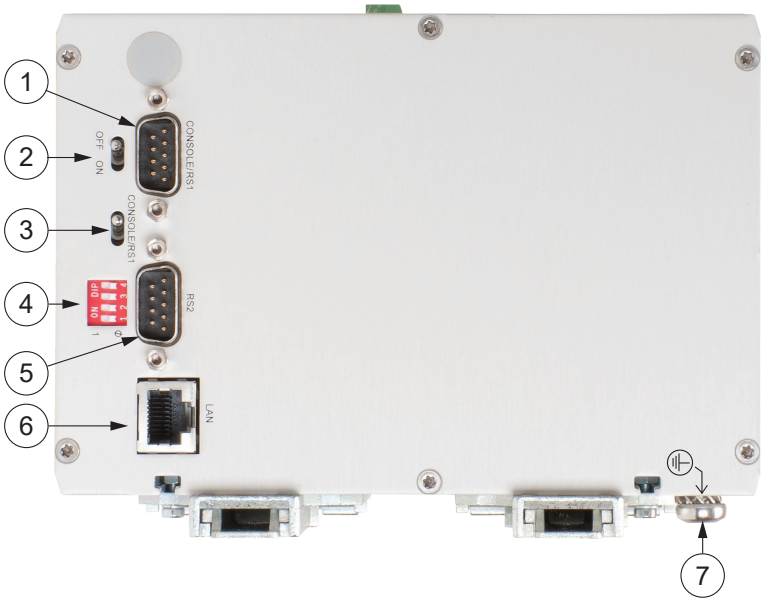

Figure 4: Serial panel

1 Console serial port (DIP switch selectable application or console port RS1)

2 Power switch

3 Serial console switch (RS1)

4 Serial port 2 hardware configuration DIP switches

5 Serial port 2

6 Ethernet connector

7 Protective earth screw

2.2.3 Antenna panel

Figure 5: Antenna panel

1 SIM card tray connector

2 SIM card tray release button

3 Antenna connector SMA (female)

2.2.4 System status LEDs

The device has eight LEDs indicating the system status. They are located on the front panel.

Table 1: Description of available LEDs

Label		State	Description
VPN		On	VPN connection is up
		Flashing	VPN connection is starting
		Off	VPN connection is disabled
Power/Error		On	Operating power is turned on
		Off	Operating power is turned off
Function		On	Device is starting
		Flashing	Device is operating normally
Eth		On	Ethernet link is up
		Flashing	Ethernet link is transferring data
		Off	Ethernet link is down
Cellular		On	This LED is controlled by the internal communication module logic. For more information, see Tools/Modem info on the Web HMI.
		Flashing	This LED is controlled by the internal communication module logic. For more information, see Tools/Modem info on the Web HMI.
		Off	Cellular connection is inactive
AC		On	Connected to AC power
		Off	Not connected to AC power
LINK		On	IEC 60870-5-104 control link to SCADA is active
		Off	IEC 60870-5-104 control link to SCADA is active
DISCONNECTORS 1...3	OPEN	On/Off	Open position indication for disconnector
	CLOSE		Close position indication for disconnector

Table continues on the next page

Label		State	Description
	RE-MOTE	On	Remote control indication
		Off	Local control indication
GROUNDING 1...3	OPEN	On/Off	Open position indication for grounding disconnector
	CLOSE		Close position indication for grounding disconnector

2.3 DIN rail mounting

The device has mounting grooves for DIN rail mounting brackets and it is supplied with pre-installed DIN rail brackets.

2.4 Product information label

The product label contains basic information about the unit such as product name, serial number and Ethernet MAC address.

The product label is found on top of the device.

2.5 Firmware version

The device's firmware version is visible on the welcome page (**System** > **Welcome Page**), which is displayed after logging in to the device.

For firmware updates, contact ABB's technical customer support.

3 Physical connections

3.1 Communication connections

The device uses the serial ports for console or application communication, the Ethernet port for network communication and cellular connectivity for wireless applications.

3.1.1 Serial ports

The device has two application serial ports. Serial port 1 is configurable to either console or data mode and supports RS-232 only. Serial port 2 is configurable to multiple serial modes (RS-232/422/485). Serial port connectors are 9-pin D-sub male connectors. Serial ports function as DTE devices.

3.1.1.1 Console/serial port 1

The console switch enables or disables console access. When the switch is in the right position, serial port 1 is in the serial port mode, and when it is in the left position, serial port 1 is in the console mode.

The console switch is located below the serial port 1 connector. Turn off power from the device before toggling the console switch, as the switch position is read during the boot sequence only. The baud rate is fixed to 115200 bps when the port is configured in the serial console mode.

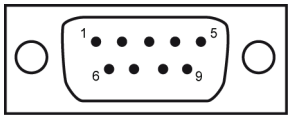

Figure 6: Console/RS1 port connector

Table 2: Console/RS1 port pinout

PIN	Function
1	DCD
2	RXD
3	TXD
4	DTR
5	GND

Table continues on the next page

PIN	Function
6	DSR
7	RTS
8	CTS
9	RI

Table 3: Console/RS1 port configuration

Parameter	Value
Baud rate	300...230400 (console 115200) bps
Data bits	8
Parity	No parity
Stop bits	1
Flow control	No flow control

3.1.1.2 Serial port 2

Serial port 2 can be configured to multiple serial formats (RS-232/422/485). The default is RS-232.

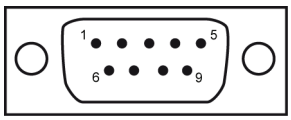

Figure 7: Application serial port

Table 4: Application serial port pinout (RS-232)

PIN	Function
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS

Table continues on the next page

PIN	Function
8	CTS
9	RI

Table 5: Application serial port configuration

Parameter	Value
Baud rate	300...460800 bps
Data bits	8
Parity	No parity
Stop bits	1
Flow control	CTS/RTS

By default, all DIP switches are set to the 0 position (RS-232 mode). DIP switches 2...4 apply only when DIP switch 1 is set to differential mode (RS-485/RS-422).

Table 6: DIP switches

DIP switch	Mode	State	Description
1	RS-232 or differential	0 = RS-232, 1 = RS-485 and RS-422	Selects the serial port operation mode
2	DUPLEX	0 = FULL, 1 = HALF	Selects between RS-422 full-duplex (4- wire) and RS-485 half- duplex (2-wire) differential modes
3	BIASING	0 = OFF, 1 = ON	Enables RS-422 biasing on pins 2 and 8
4	TERMINATION	0 = OFF, 1 = ON	Enables RS-422 termination on pins 2 and 8

If biasing and/or termination is required for the RS-485 half-duplex (2-wire) mode, enable RS-422 biasing/termination with DIP switches and manually connect pins 2-7 and 3-8 together at the application port (RS-2).

Do not connect RS-422 or RS-485 cables to a serial port configured to the RS-232 mode. This could damage the port and the connected equipment.

Table 7: Application serial port pinouts in RS-422/485 modes

PIN	RS-422 full-duplex (4-wire)	RS-485 half-duplex (2-wire)
1	-	-
2	RXD positive (in)	-

Table continues on the next page

PIN	RS-422 full-duplex (4-wire)	RS-485 half-duplex (2-wire)
3	TXD negative (out)	TXD/RXD negative (out/in)
4	-	-
5	GND	GND
6	-	-
7	TXD positive (out)	TXD/RXD positive (out/in)
8	RXD negative (in)	-
9	-	-

3.1.2 Ethernet

The device has an RJ-45 connector for 10/100 Mbps Ethernet connection. The maximum length of the Ethernet cable is 100 m.

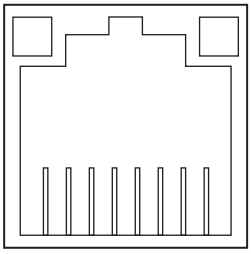

Figure 8: Ethernet connector

Table 8: Ethernet port configuration

Description	Value
Number of ports	1
Speed	10Base-T, 100Base-TX
Duplex	Half and full duplex
Auto-negotiation	Yes
Recommended cabling	Cat5e or better

3.1.3 Wireless network

The device supports cellular connectivity (2G, 3G, LTE) allowing the use of wireless applications. The practical data transfer rates depend on the subscription details and wireless network capacity.

The device with wireless interface includes an SMA female type connector for an external antenna. Any kind of external 50 Ω wide band antenna can be used intended

for GPRS, 3G or LTE frequency bands. The antenna is connected directly to the connector located on the device's back panel.

Commercially available antennas are usually provided with a flexible 50 Ω cable with a length of 2...3 meters and a male type SMA connector.

If the PIN code query is enabled, check that the ARC600 configurator has the correct PIN code entered in the wireless WAN submenu.

3.2 I/O connections

The device has four connectors in the front panel for power input and for switching devices' status monitoring and control, battery condition monitoring, battery charging and measurement functions.

3.2.1 Power connector

Operating power for the device is supplied from connector X2.1. The device can use either an unregulated AC line input or a regulated DC input.

The power switch is located on the serial panel. It turns the unit on and off.

Table 9: Operating voltages of X2.1 connector pins

Input pins	Operating voltage range
1 and 2 (AC)	Nominal auxiliary voltage U_n: 100...165 V DC or 100...240 V AC 50/60 Hz Auxiliary voltage variation: 85...200 V DC or 90...264 V AC
6 and 7 (DC)	20...30 V DC

3.2.2 X2.1 connector

Table 10: X2.1 connector pinout

Pin	Symbol	Description
1	L	230 V AC
2	N	230 V AC
3	NTC_A	NTC resistor (battery temperature comp.)
4	PE	Protective earth
5	NTC_B	NTC resistor (battery temperature comp.)

Table continues on the next page

Pin	Symbol	Description
6	24VDC	24 V DC output/input
7	GND	DC ground
8	GND	DC ground
9	GND	DC ground
10	BAT	Battery charging

Table 11: X2.1 connector types

Connector	Manufacturer	Connector type (part number)
Panel header	Phoenix Contact	MSTBV 2,5 HC/10–GF-5,08 (1924606)
Matching plug	Phoenix Contact	MSTB 2,5 HC/10–STF-5,08 (1912265)

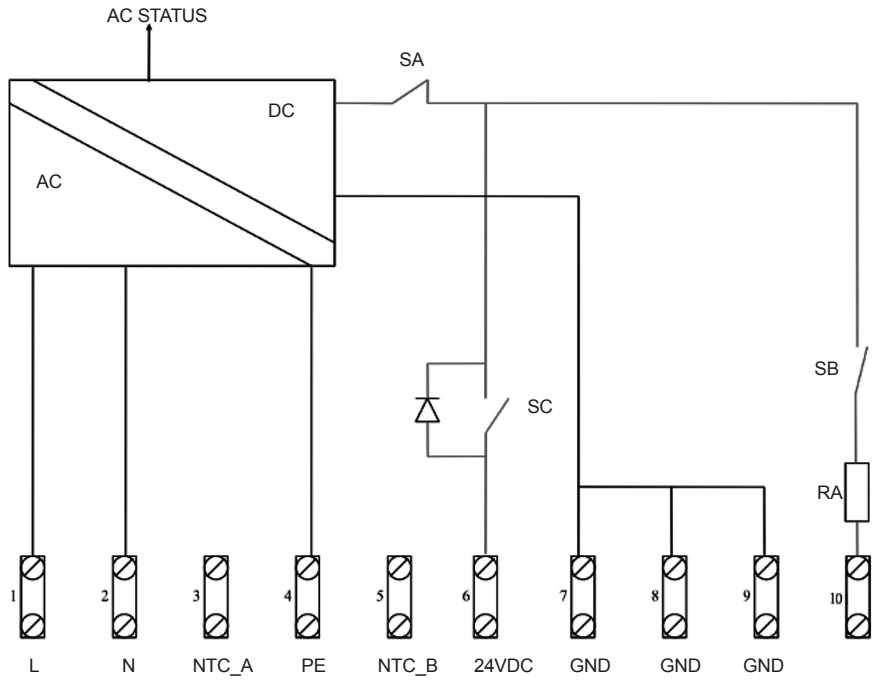

Figure 9: X2.1 connector schematics

With DC (85...200 V DC), connect the negative wire to L and the positive to N.

3.2.3 X2.3 connector

Table 12: X2.3 connector pinout

PIN	Symbol	Description	Disconnector function
1	DI1	Digital input 1	Disconnector 1 opened
2	DI_C1	Common supply voltage for DI1 and DI2	
3	DI2	Digital input 2	Disconnector 1 closed
4	DI3	Digital input 3	Disconnector 2 opened
5	DI_C2	Common supply voltage for DI3 and DI4	
6	DI4	Digital input 4	Disconnector 2 closed
7	DI5_A	Digital input 5	Local/Remote switch for disconnector 1
8	DI5_B	Digital input 5	
9	DI6_A	Digital input 6	Local/Remote switch for disconnector 2
10	DI6_B	Digital input 6	
11	DO1_A	Relay output 1	Close disconnector 1
12	DO1_B	Relay output 1	
13	DO2_A	Relay output 2	Open disconnector 1
14	DO2_B	Relay output 2	
15	DO3_A	Relay output 3	Close disconnector 2
16	DO3_B	Relay output 3	
17	DO4_A	Relay output 4	Open disconnector 2
18	DO4_B	Relay output 4	

Table 13: X2.3 connector types

Connector	Manufacturer	Connector type (part number)
Panel header	Phoenix Contact	MSTBV 2,5/18–GF-5,08 (1777235)
Matching plug	Phoenix Contact	MSTB 2,5/18–STF-5,08 (1778140)

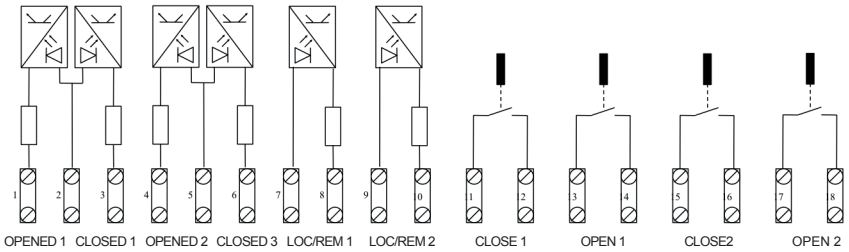

Figure 10: X2.3 connector schematics

3.2.4 X3 connector

3.2.4.1 Disconnector 3 and grounding disconnectors

Table 14: IO3 connector pinout

PIN	Symbol	Description	Disconnector function
1	DI7	Digital input 7	Disconnector 3 opened
2	DI_C3	Common supply voltage for DI7 and DI8	
3	DI8	Digital input 8	Disconnector 3 closed
4	DI9_A	Digital input 9	Local/Remote switch for disconnector 3
5	DI9_B	Digital input 9	
6	DO5_A	Relay output 5	Close disconnector 3
7	DO5_B	Relay output 5	
8	DO6_A	Relay output 6	
9	DO6_B	Relay output 6	Open disconnector 3

Table continues on the next page

PIN	Symbol	Description	Disconnector function
10	DI_C4	Common supply voltage for DI10, DI11, DI12, DI13, DI14 and DI15	
11	DI10	Digital input 10	Grounding disconnector 1 open
12	DI11	Digital input 11	Grounding disconnector 1 closed
13	DI12	Digital input 12	Grounding disconnector 2 open
14	DI13	Digital input 13	Grounding disconnector 2 closed
15	DI14	Digital input 14	Grounding disconnector 3 open
16	DI15	Digital input 15	Grounding disconnector 3 closed

Table 15: X3 connector types

Connector	Manufacturer	Connector type (part number)
Panel header	Phoenix Contact	MSTBV 2,5/16–GF-5,08 (1777219)
Matching plug	Phoenix Contact	MSTB 2,5/16–STF-5,08 (1778124)

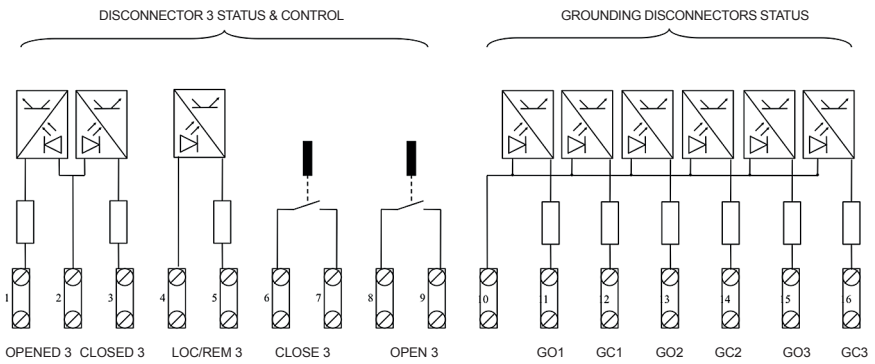

Figure 11: X3 connector schematics

3.2.5 X4 connector

Table 16: X4 connector pinout

PIN	Symbol	Description
1	LOADCUT_A	Load control relay out, normal closed (NC)
2	LOADCUT_B	Load control relay out, normal closed (NC)
3	AI1_A	Analog In 1, -5 V...+5 V measurement, ±300 mV (-10...+55°C, 0 V...+5 V), Hall-sensor [1]
4	AI1_B	Analog In 1, -5 V...+5 V measurement, ±300 mV (-10...+55°C, 0 V...+5 V), Hall-sensor [1]
5	TESTLOAD_A	Relay out, test load for battery test case
6	TESTLOAD_B	Relay out, test load for battery test case
7	HTR_A	Heater/Extra relay
8	HTR_B	Heater/Extra relay
9	AI2_A	Analog In 2, -5 V...+5 V measurement, ±300 mV (-10...+55°C, 0 V...+5 V), Hall-sensor [1]
10	AI2_B	Analog In 2, -5 V...+5 V measurement, ±300 mV (-10...+55°C, 0 V...+5 V), Hall-sensor [1]
11	DIC_5	Common supply voltage for DI16, DI17
12	DI16	Digital input 16
13	DI17	Digital input 17
14	DO7_A	Relay output 7
15	DO7_B	Relay output 7

[1] Can be used as a 4...20 mA input using external resistor

Table 17: X4 connector types

Connector	Manufacturer	Connector type (part number)
Panel header	Phoenix Contact	MSTBV 2.5/15-GF-5.08 (1777206)
Matching plug	Phoenix Contact	MSTB 2.5/15-STF-5.08 (1778111)

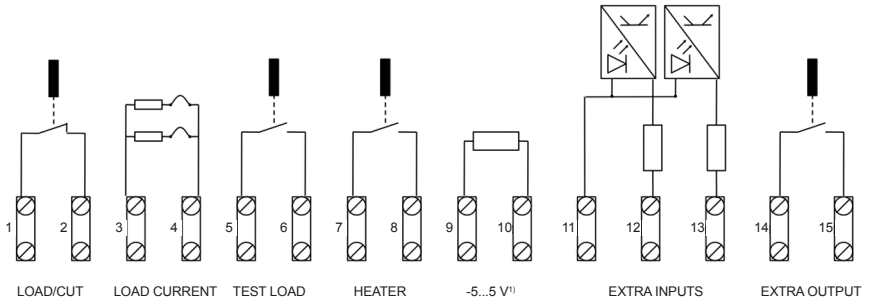

Figure 12: X4 connector schematics

1) Can be used as a 4...20 mA input using external resistor

3.2.6 I/O LEDs

The device has two LEDs indicating the AC and LINK status. Nine LEDs are available to indicate the disconnector status. For indicating the grounding disconnector status, the device has six LEDs.

3.2.6.1 AC and LINK LEDs

The device has two LEDs indicating the AC and LINK status.

Table 18: AC and LINK LEDs

LED	Description
AC	AC power is connected to connector X2.1 pins 1 and 2
LINK	The IEC control link to SCADA is active

3.2.6.2 Disconnector LEDs

The device has nine LEDs to indicate the disconnector status. They are located on the device front panel. Each disconnector has three LEDs, which indicate the status of the disconnector.

Table 19: Disconnector LEDs

Disconnector LED	Description
Disconnector 1 open	Disconnector 1 is opened
Disconnector 1 close	Disconnector 1 is closed
Disconnector 1 remote	Disconnector 1 is on remote control
Disconnector 2 open	Disconnector 2 is opened
Disconnector 2 close	Disconnector 2 is closed
Disconnector 2 remote	Disconnector 2 is on remote control
Disconnector 3 open	Disconnector 3 is opened
Disconnector 3 close	Disconnector 3 is closed
Disconnector 3 remote	Disconnector 3 is on remote control

Disconnector LEDs can indicate two special cases.

Table 20: Disconnector LED special cases

Disconnector LED state	Description
Open and close LEDs are both OFF	Disconnector is changing state
Open and close LEDs are both ON	Disconnector error

3.2.6.3 Grounding LEDs

The device has six LEDs indicating the grounding status. They are located on the device front panel. Each grounding disconnector has two LEDs, which indicate the status of the grounding disconnector.

Table 21: Grounding LEDs

Grounding LED	Description
Disconnector 1 open	Connector X3 digital input on pin 11 is active high
Disconnector 1 close	Connector X3 digital input on pin 12 is active high
Disconnector 2 open	Connector X3 digital input on pin 13 is active high
Disconnector 2 close	Connector X3 digital input on pin 14 is active high

Table continues on the next page

Grounding LED	Description
Disconnector 3 open	Connector X3 digital input on pin 15 is active high
Disconnector 3 close	Connector X3 digital input on pin 16 is active high

All grounding disconnector digital input pins have connector X3 pin 10 as the common ground pin.

4 Functional description

4.1 Control functions

The device is capable of controlling and monitoring an object, for example, a disconnector, and handling the object status information. The device can control and monitor up to three objects. The device can monitor the earthing switch position indications, with one function per disconnector object. Local/Remote indications are also a standard; each disconnector has its own Local/Remote position monitoring. In the Local position, control operations (open or close) can be performed at the site only. In the Remote position, control operations can be performed from the SCADA system in the network control center.

4.2 Condition monitoring functions

4.2.1 Communication diagnostics and watchdog

The device is provided with a self-supervision system, that is, a watchdog function. The self-supervision system handles run-time fault situations and informs the user of faults through the user HMI (function LED) on the front panel.

In addition to hardware supervision, the self-supervision system is able to reestablish the cellular connection and VPN connection (if applicable). Furthermore, it is able to restart the device as a last resort.

4.3 Disconnector control condition monitoring functions

4.3.1 Disconnector travel time monitoring

The OPEN and CLOSE indications are monitored. When a change occurs due to an activated control operation, the opening or closing travel time is measured. If the measured travel time is greater than or equal to the set limit values, an alarm is given. The settings define how the disconnector travel time duration (state change from open to close or vice versa) is reported.

Travel time is reported in seconds. The alarm signals remain active until the fault condition is acknowledged.

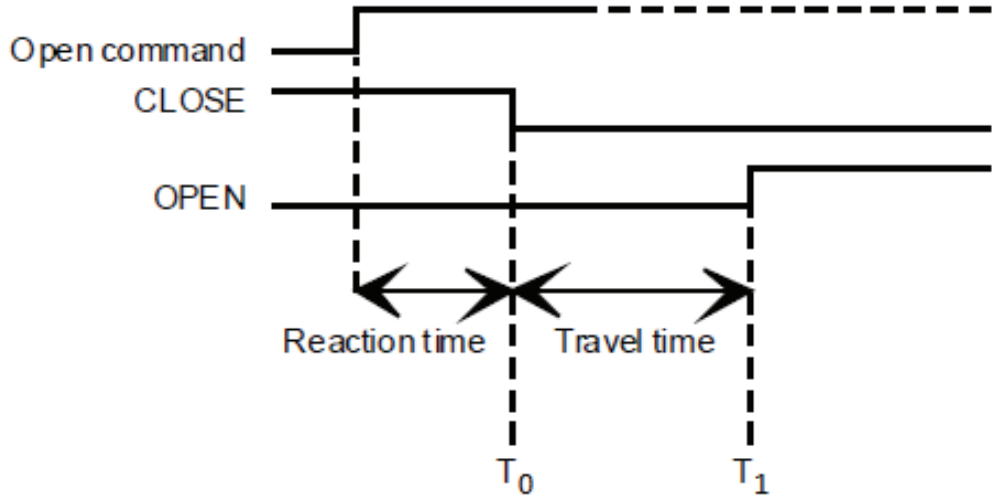

Figure 13: Travel time measurement for open operation

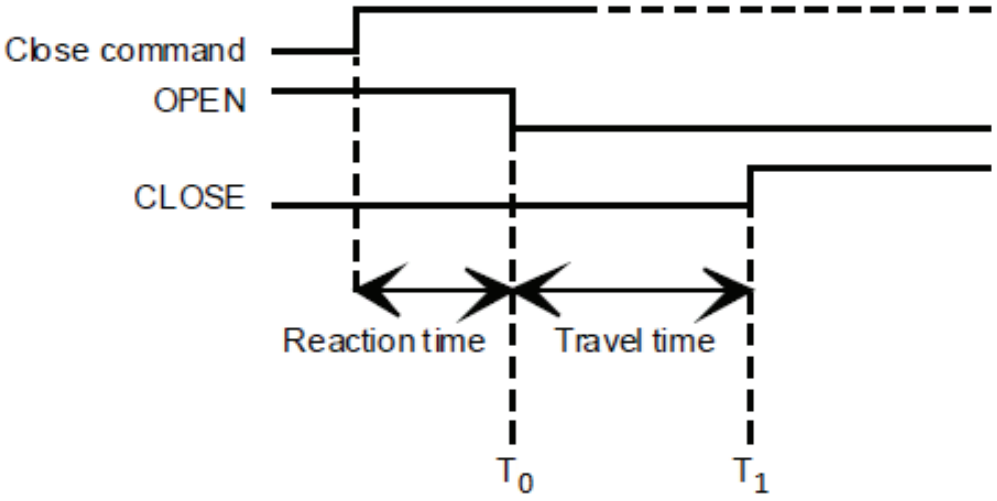

Figure 14: Travel time measurement for close operation

4.3.2 Disconnector actuator motor overload protection

With an optional Hall effect sensor, the device is able to measure the load current that flows through the actuator during the control operation of the disconnector. This current measurement is effectively used to detect an abnormality in the mechanical motion, when the lever that operates the disconnector moves from one end position to the other (for example, from Open to Close). A slip in the mechanical gear unit or a mechanically stiff operation, due to insufficient lubrication or deviation in operation tube positioning, can cause an overload situation which may be harmful to the actuator motor if no action is taken to prevent overloading.

Even if MCB’s are used as an overload protection, they are not optimal from the maintenance point of view, as they require a site visit because the resetting is typically managed manually. The device's intelligent overload protection function, for example, the resetting and adjustment of the current pick-up level, is managed remotely from a utility dispatch center, using a system such as SCADA. The overload

protection is coordinated with the possible MCB in the same circuit so that the current pick-up setting is lower than the MCB operational level to avoid unnecessary site visits.

4.3.3 Monitoring of the pressure of SF6 gas

The SF6 insulated primary equipment is arranged by wiring the pressure sensor contact to one input of the device, used for monitoring the SF6 gas pressure. When the gas pressure drops below the acceptable limit, the falling edge of the digital signal triggers and activates an alarm signal. This information can be obtained as an alarm event from the network control system.

4.4 Battery charging and monitoring functions

Power backup for the station can be arranged by connecting 24 V (2 × 12 V) sealed lead acid batteries to the device. The batteries supply power to both the device and the communication device during a mains failure. As the batteries are charged by the device, the communication between the unit and the network control center is always operating irrespective of distribution network faults or planned outages.

The battery condition is secured by a battery load and condition monitoring test, activated remotely via a command from the SCADA system. In the test, a discharge resistor is connected in parallel to the batteries. During the test, the battery capacity is measured and reported as an Ah value to indicate the remaining capacity, so that maintenance can be optimized. The battery test can be started directly from the control room or run automatically according to the agreed timetable. During the battery load test, which takes 2...5 h, the voltage of the battery charger is shut off and the control functionality is blocked.

If the battery voltage drops to less than the set value, for example, 22 V, during the battery load test, the device generates an alarm event. This indicates that the lifetime of the batteries is ending or that an internal fault has occurred in the battery or its circuitry. In both cases, the battery must be replaced.

During normal control operations, the device makes condition measurements, such as the battery voltage minimum value and the maximum current. The battery condition and lifetime can be estimated based on these recorded values.

4.4.1 Power backup

Power backup for the station can be arranged by connecting 24 V (2 × 12 V) sealed lead acid batteries to the device. The batteries supply the device and keep the communication alive during a mains failure. Thus the communication between the device and a network control centre operates in any situation.

Depending on the application and the required maximum operation time, batteries of different capacity are used; the typical capacity is 17 Ah. With the 17 Ah battery, the maximum operation time is 48 hours (including safety coefficient) at ambient temperature of +20°C.

A low temperature reduces battery capacity and lifetime.

4.4.2 Heater control

The heater control is based on the environmental temperature. Heating is needed if the device is installed in a separate enclosure outdoors where the ambient temperature may be below 0°C. Heating is specifically required in very damp conditions when dehumidifying is needed. The heating control consists of switching on and off an output pin connected to an external control relay of the heating element (resistor), which is located in the enclosure, preferably next to the batteries and the electronics components.

The device contains an internal thermostat for controlling the external heater. The heater element can be set to be constantly on, for example, if the element contains an internal thermostat, constantly off or to be controlled by the environmental temperature.

The heater output pins are X4 7 and 8. This is defined by giving the parameter *heater_output* value “9”.

The settings are defined in the section [HEATER].

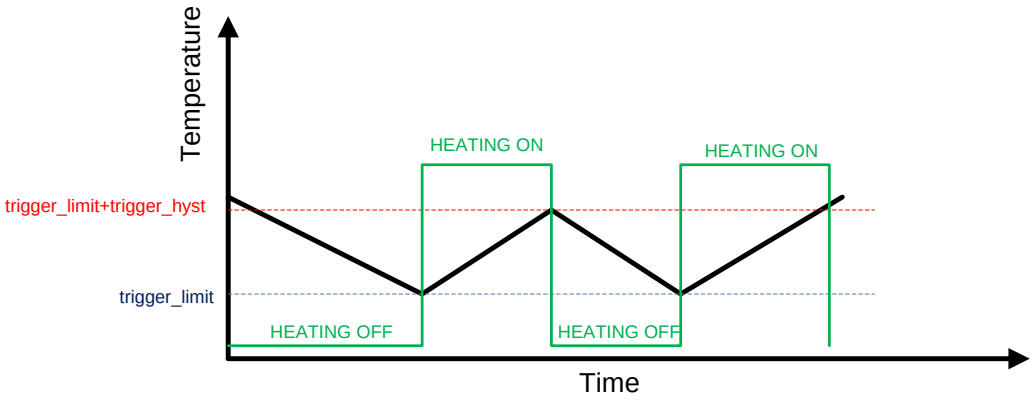

Figure 15: Heater control on auto-mode

4.4.3 Low auxiliary voltage indication

The power supply module gives an internal alarm signal when a drop in the power supply voltage is detected (AC Fail). The indication of a low auxiliary voltage can be reported to any available communication protocol supported by the device.

4.4.4 Over/undertemperature indication

The power supply module gives an internal alarm signal when over- or undertemperature is detected inside the enclosure. The alarm is activated when the temperature inside the enclosure surpasses a set limit or decreases below a set limit. Hysteresis can be set for both indication functions. The indication can be reported through any available communication protocol supported by the device.

4.4.5 Temperature compensation of battery charging voltage

The charging voltage of the internal battery charger of the device is temperature-compensated. The compensation factor is approximately -40 mV/°C. The data about the temperature is acquired with the help of a 2.2 kΩ NTC thermistor that is connected to pins 3 and 5 of the connector X2.1. If the battery charger is not used to charge the battery, the thermistor or the 2.2 kΩ resistor must still be installed between the pins 3 and 5 of the connector X2.1. Otherwise, the overvoltage protection of the charger may activate and prevent the device from starting.

It is recommended to install NTC thermistor between the batteries.

4.4.6 Battery deep discharge protection

When the battery voltage falls below a certain value, the battery is almost empty. To prevent battery damage, the battery should not be further discharged. The battery deep-discharge protection function disconnects the battery from the device in two cases.

- AC supply is not available to charge the battery.
- Battery voltage stays long enough below the defined limit.

Usually the deep-discharge protection causes the device to shut down due to lack of power. The device recovers once the AC supply becomes available again or it is powered up with DC on the modem-supply pin (X2.1 pin 6). External loads such as a Hall sensor, additional DC-powered ARC600 devices or the supply for input circuits should not be connected directly to the battery but to the “master” ARC600 24 VDC In/Out pin (X2.1 pin 6). This way, the whole load can be removed at once when the deep-discharge protection is required. The settings are defined in the section [BATTERY_DISCHARGE_PROTECTION].

4.4.7 Battery capacity test

The device can test the capacity of the battery by disconnecting the charger and draining the battery to almost empty using an external loading resistor. The test is completed when the battery voltage reaches the defined voltage limit. The battery capacity can be returned by protocol communication in ampere-hours. The battery draining current is measured by external Hall sensor connected to analog input 1 (X4 3-4). The loading-resistor current should be routed through the relay contacts of X4 pins 5 and 6.

The test is started by protocol communication command. The information object is defined in the section [BATTERY_TEST_CONTROL_SC].

Certain conditions can be defined to abort the test.

- AC voltage is missing.
- Temperature is too high.
- Temperature is too low.
- Battery voltage does not reach the defined completion limit during timeout.
- Battery draining current too low.
- Battery draining current too high.
- Abortion command is issued by protocol communication.

The test is completed when the measured battery voltage stays below the defined voltage limit. This means the battery is almost empty and the available capacity can be estimated by multiplying the consumed charge by compensation factor. For example, if the defined target voltage means the battery to be 90% discharged, a multiplication factor 1.11 can be used to estimate the available total capacity. The device can compensate the cabling-loss voltage and include its internal charge consumption to the total capacity.

Usually, the disconnectors are internally blocked during the battery test and the test should be remotely stopped (information object [BATTERY_TEST_CONTROL_SC]) before the disconnectors can be operated. The blocked state can be indicated by configuring the local/remote status to double-point indication [DISCONNECTOR_LOCREM_xx].

The load limiter functionality and the heater are disabled during the test.

4.4.7.1 Settings

The battery capacity test settings are defined in the section [BATTERY_TEST].

4.4.7.2 Remote control of the battery test function

Once the battery test functionality is enabled on the configuration file, it can be remotely controlled by protocol communication. The information object is defined in the section [BATTERY_TEST_CONTROL_SC].

- 0 = Abort the battery test
- 1 = Start the battery test

4.4.7.3 Battery test status

The status of the battery testing is available for the protocol communication. The information object is defined in the configuration file section [BATTERY_TEST_STATUS_DPI].

- 0 = Idle (not testing the battery)
- 1 = Testing (discharging the battery by using external load)
- 2 = Test complete
- 3 = Test aborted

4.4.7.4 Battery capacity

The measured battery capacity can be reported as a short floating-point value. The reporting unit is ampere-hours Ah. For settings, see the general floating-point input settings. The measured capacity is always reported after the test is completed. The information object is defined in the configuration file section [BATTERY_TEST_CHARGE_FPI].

4.4.7.5 Measurement file

The device can generate the internal measurement file from the battery capacity testing. The measurement file is written every *averaging_interval_sec* and each line contains a time stamp, status, battery voltage, discharge current and the charge

consumed so far. The file header contains the unloaded battery voltage before the load is applied. The last line of the file contains information whether the test was completed successfully or aborted for a specific reason.

4.5 Measurement functions

The device measures the battery voltage and the ambient temperature. The temperature measurement is calibrated to measure the ambient temperature of the device mounted in an enclosure. The temperature measurement is used to compensate for the charging voltage of the batteries and for activating or deactivating heating in cold environments. The battery voltage is measured as two values: the minimum battery voltage and the maximum current during control operation. The minimum battery voltage indicates the lowest voltage measured during a battery test or during an object's operation. The battery-charging voltage indicates the present voltage on the battery poles. The values can be read from the network control center via the supported communication protocols. The minimum battery voltage and the maximum current can be reset via the serial bus.

The device supports a general-purpose analog input that can be used as a transducer input. It supports voltage mode -5…5 V, ±300 mV (-10...+55°C, 0...+5 V).

The input can be used as current mode 4...20 mA using an external resistor.

4.5.1 Temperature measurement

The device has four temperature sensors.

4.5.1.1 Processor temperature

The ambient temperature of the process is measured by a sensor whose measurement result is available on the System tab of the Web user interface and with the command line command temperature. The measurement data of the sensor is not available with protocol communication.

4.5.1.2 Communication module temperature

The internal temperature of the wireless communication module is available on the Web user interface under **Tools** > **Modem** Info and with the command line command modeminfo. The measurement data of the sensor is not available with protocol communication.

4.5.1.3 Sensor for the temperature compensation of the charging voltage

The internal sensor of the device adjusts the battery charging voltage based on the battery temperature. The data about the temperature is gained with the help of a 2.2 kΩ NTC thermistor that is connected to pins 3 and 5 of the connector X2.1. The thermistor is located between the batteries. The measurement data of the sensor is not available with protocol communication but it is only used for adjusting the charging voltage.

4.5.1.4 Ambient temperature

The temperature of the device casing is used for estimating the ambient temperature. Because the power consumption of the device affects the casing temperature, its effect is compensated based on calculations. The compensation parameters are defined in the setting file section [PHYSICAL_TEMP].

The ambient temperature calculated from the casing temperature is available with protocol communication. The temperature object is defined in the setting file section [TEMPERATURE_FPI]. This temperature is also used for temperature alarm ([TEMPERATURE_LOW_SPI], [TEMPERATURE_HI_SPI]), battery testing temperature guard ([BATTERY_TEST]) and heater control ([HEATER]).

Example

- Casing temperature 47 °C
- Fixed temperature difference -10 °C
- Charging current 2 A
- Charging current effect 3.5 °C/A
- Ambient temperature (47-10) °C - 2 A * 3.5 °C/A = 30 °C

4.6 Load limiter

The device can detect excessive loading of battery due to jammed disconnector switchgear and disconnect the load before the actual physical overcurrent fuse trips. The overload decision is based on both the consumed charge and duration of the loading. The current is measured usually by an external Hall sensor connected to analog input 1 (X4 3-4). The device uses a normally closed relay (X4 1-2, Load Cut) to break down the loading circuit by opening the relay contacts for a moment. Usually this is used to cut the holding circuit of motor contactors, not directly the motor current.

4.6.1 Overload detection settings

The overload detection settings are defined on section [LOAD_LIMITER]. The detection is based on the load current measurement by the external Hall sensor connected to X4 pins 3 and 4.

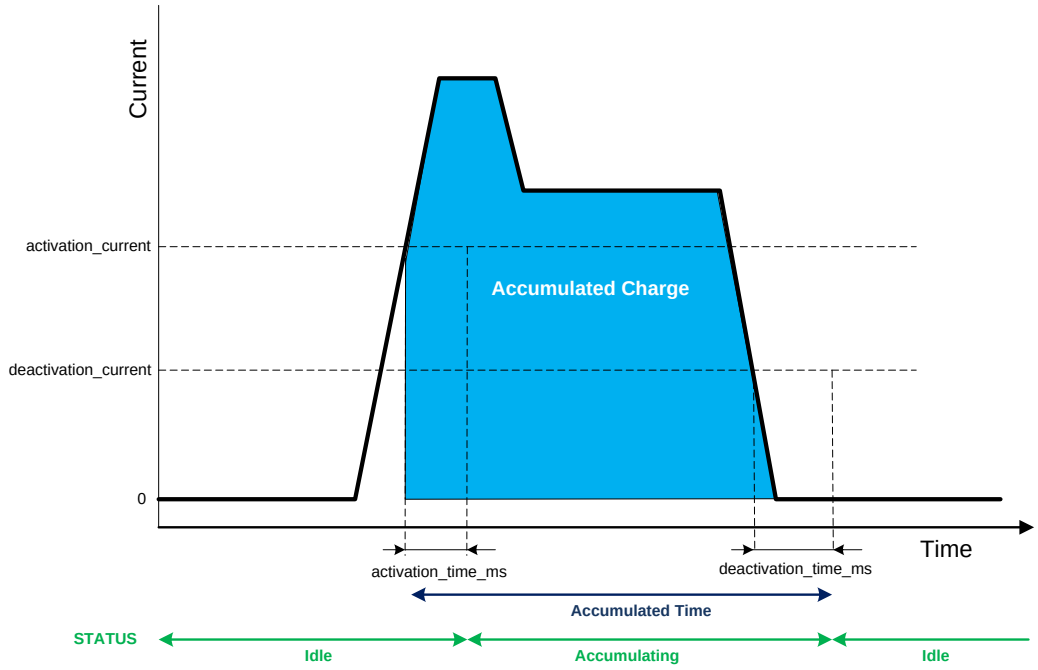

Figure 16: Load limiter measurements

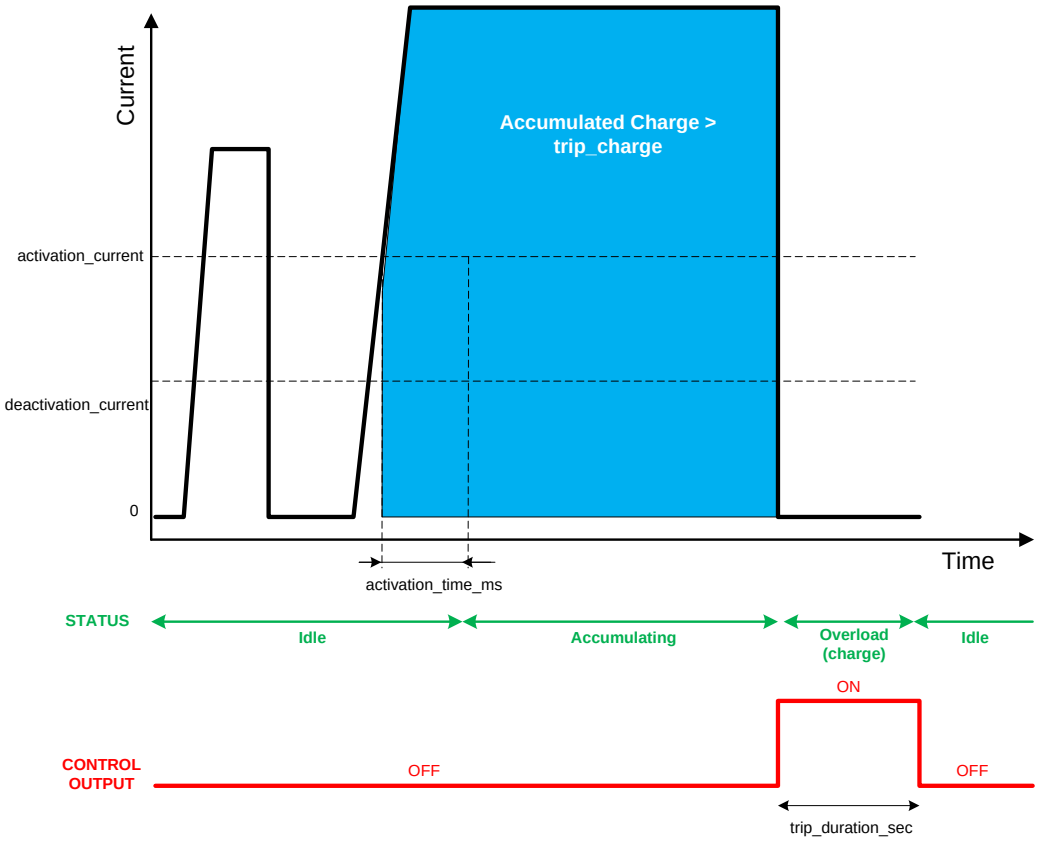

Figure 17: Overload caused by charge

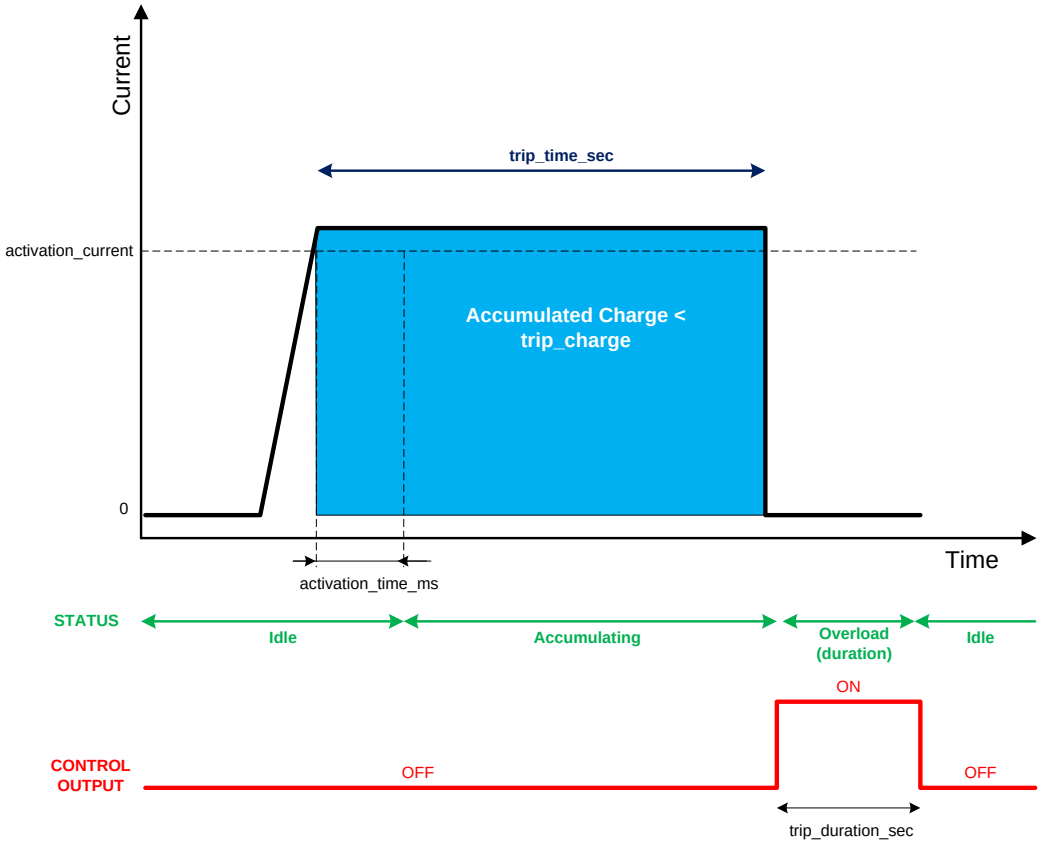

Figure 18: Overload caused by duration

4.6.2 Remote enabling and disabling of the load limiter

Once the load limiter functionality is enabled on the configuration file, it can be remotely controlled by the protocol communication. The information object is defined in the section [LOAD_LIMITER_CONTROL_SC].

- 0 = Disable load limiter
- 1 = Enable load limiter (if enabled on configuration file)

The issued value is not permanently stored and effects only until reboot or application restart.

4.6.3 Load limiter status

The current status of the load limiter function is available for protocol communication. The information object is defined in the section [LOAD_LIMITER_STATUS_DPI].

- 0 = Load limiter idle (waiting for the current to exceed the threshold)
- 1 = Load limiter disabled (does not monitor load)
- 2 = Loading detected, accumulating
- 3 = Overload, load disconnected

4.6.4 Reason for load limiter activity

The overload decision is based on both consumed charge and duration of the loading. Once the overload situation is detected, the reason can be reported as double-point input. The information object is defined in the section [LOAD_LIMITER_REASON_DPI].

- 0 = None, overload situation not detected
- 1 = Overload caused by consumed charge
- 2 = Overload caused by duration of loading
- 3 = Overload detected by manual command

4.6.5 Measured charge during overload

The overload decision is based on both consumed charge and duration of the loading. Once the overload situation is detected, the accumulated charge can be reported as a short floating-point value. The reporting unit is ampere-seconds. If no overload situation has been detected, the reported value is zero and has a non-topical NT flag set. The information object is defined in the section [LOAD_LIMITER_CHARGE_FPI]. This charge is reported only when the overload situation is detected. The consumed charge for normal operation is reported by [DISCONNECTOR_TRAVELCHARGE_N].

4.6.6 Measured time during overload

The overload decision is based on both consumed charge and duration of the loading. Once the overload situation is detected, the loading duration can be reported as a short floating-point value. The reporting unit is seconds. If no overload situation has been detected, the reported value is zero and has a non-topical NT flag set. The information object is defined in the section [LOAD_LIMITER_TIME_FPI]. This duration is reported only when the overload situation is detected. The travel time for normal operation is reported by [DISCONNECTOR_TRAVELTIME_N].

4.7 Support for fault indicators

The device contains a driver for the ABB RIO600, Horstmann ComPass-B and Kries IKI-50 fault indicators. The driver polls the fault indicator devices using Modbus and converts the values to IEC 60870-5-104. Up to four fault indicators can be connected.

5 Cyber security

5.1 Cybersecurity definition

Cybersecurity aims to secure the properties of the organization against security risks. To strengthen the system and increase the security level towards any cybersecurity attacks from the Internet, certain actions are recommended while configuring the device.

- The device should be installed physically secure, for example, in a locked cabinet.
- The latest security updates need to be installed for all network devices.
- The network inventory needs to be documented and kept up to date.
- Unused services and interfaces should always be disabled.
- Only VPN connections should be used to access remote networks.

5.2 Enhancing operator and subscription security

Network subscription and SIM card must be stored safely and configured to prevent misuse of services.

- Disable unused services from SIM cards.
  - Voice calls
  - SMS
  - Paid services
  - Roaming
- Use pin code in SIM cards.
- Prefer a private APN service from the operator.
- Prefer M2M subscription SIM cards from the operator.
- Use private IP addressing from the operator for cellular network based communications.
- If connected to a public IP network, do not use plain text protocols such as http, SNMP and telnet. Always use VPN to connect to the device.

5.3 Configuring firewall and services

Enable the firewall and disable the unused services and interfaces in the device. To start, disallow traffic and allow only the needed traffic. Use the default policy to drop connections.

- Check that the firewall is enabled.
- For incoming connections, always filter (drop) all unused ports which may include DNS, L2TP-VPN, SNMP and so on.

- Check that the default action is “drop” in firewalls and allow only the needed ports.
- Set unique passwords for each device.
- Keep passwords stored in a safe place, for example, Encrypted password management tool.
- Check that all unused services are disabled.
- If possible, allow IP connections only via VPN.
- Back up the configuration.

6 Getting started

6.1 Connecting cables

1. Check that the power switch is in the OFF position.
2. Connect the Ethernet cable between the device’s Ethernet LAN connector and the computer used for the configuration.
3. Connect the power supply to the device.
4. Toggle the power switch to ON position.

   The power/error LED and function LED should turn on immediately after the power switch is turned on.

After the system has initialized, the function LED starts to flash.

6.1.1 Connection principle

The device has configurable network interfaces.

- Ethernet LAN port
- Mobile WAN cellular interface

The device supports cellular connectivity (2G, 3G, LTE) allowing the use of wireless applications. The WAN interface is used for connecting the device to public Internet or private APN. The Ethernet LAN is used for connecting other Ethernet devices to the device's local network.

The WAN interfaces can be configured to create a redundant system where one WAN automatically receives traffic if the other one goes down. For example, if the primary Ethernet connection goes down, the traffic is automatically switched to mobile WAN (secondary connection) and back when the Ethernet interface comes up again.

6.2 Logging in

1. Configure the computer to use the same IP address space as the device. Example: Laptop IP is 10.10.10.11 with netmask 255.255.255.0.
2. Check the IP configuration with the ping command in the command line.
3. In a Web browser, connect to the device over the HTTPS protocol using the device’s IP address.

   Example: The default IP address of the device is 10.10.10.10. The corresponding address to enter in the browser is https://10.10.10.10/.

Ignore the browser's warning about a self-signed certificate.

4. Enter the username and password.

   The default username is “arctic-adm“ and the default password is “arcticm2m”. Change the password before connecting the product to a public network.

5. Click **Login**.

   The **Home Page** opens.

6.2.1 User interface

ARC600 configurator is a tool which is used to manage the device properties via a user-friendly, Web-based interface.

To use the Web configurator, only a computer with an HTML browser and a connection to the device are needed. With the configurator, it is possible to receive status information and set parameters and variables that control which applications and processes are used with the device.

After a successful login, the main window is displayed. It consists of the main navigation menu on the top, the navigation bar on the left, and the content area that displays the currently active content and controls.

When the program starts for the first time, the System/Information window is displayed in the content area. The main navigation menu on the top of the window is used to navigate between the different subsets of the available settings. Selecting an item from the main menu displays the available items related to this subset in the navigation bar. The first of these is displayed in the content area by default.

The navigation bar on the left contains the parameter groups in the subset. Selecting an item from this menu displays the content related to the selected group in the content area.

6.3 Setting Ethernet port function to LAN

Changing Port function to “LAN” disables automatic IP address detection. If Port function is set to the default value “auto”, the Ethernet LAN port tries to automatically obtain the IP address using DHCP when the device boots. If the DHCP discovery fails, the device automatically uses IP address 10.10.10.10.

Change the following setting before changing any other Ethernet settings.

1. In the left pane, under **Network**, click **Ethernet Port**.
2. Set **Port function** to **LAN**.

   If VLAN connection using an external switch is needed, select **VLAN**.
3. Click **Submit** to save the settings.

If the functional mode of the Ethernet port is set to "WAN" or "VLAN", the following details must be noted. Before changing the Ethernet port mode to "WAN", the firewall configuration needs to allow Web UI and SSH access from WAN (**General** > **Firewall** and enable both *Allow WebUI access from WAN* and *Allow SSH access from*

WAN). The VLAN functional mode of the Ethernet port requires an external VLAN switch.

6.4 Configuring mobile WAN

Install the SIM card before configuring the mobile WAN.

1. In the left pane, under **Network**, click **Mobile WAN**.
2. Enter the preferred configuration in the configuration fields.
3. Click **Submit** to save the settings.

6.5 Configuring the default route

1. In the left pane, under **Network**, click **WAN Failover**.
2. Set **WAN Default Route** to **Yes**.

   This setting enables the use of the Ethernet WAN or the Mobile WAN as the default route interface.
3. If configuring Ethernet WAN as the default gateway, in the left pane under **Network**, click **Ethernet Port** and set **Port function** to **WAN**.

   If configuring Mobile WAN as the default gateway, skip this step.
4. Set the default route.
   - To select Ethernet WAN as the default gateway, under **Primary WAN**, set **Interface** to **Ethernet WAN**.
   - To select Mobile WAN as the default gateway, under **Primary WAN**, set **Interface** to **Mobile WAN**.
5. If both Ethernet WAN and Mobile WAN are configured, under **Backup WAN**, set **Interface** to **Mobile WAN** or **Ethernet WAN**, whichever is not selected as the default gateway.

   If the primary WAN interface comes down, the device automatically switches the default route to the backup WAN interface.
6. Click **Submit** to save the settings.
7. Restart the device.

7 Network configuration

7.1 Defining host and domain names

1. In the left pane, under **Systems**, select **General Settings**.
2. In the **Hostname** field, enter the name of the device without the domain part.
3. In the **Domain** field, enter the domain name.

7.2 Configuring communication interfaces

7.2.1 Configuring Ethernet LAN

1. In the left pane, under **Network**, click **Ethernet LAN**.
2. Set **Enabled** to **Yes**.
3. Set **Interface**, **IP Address** and **Subnet mask**.
4. Click **Submit** to save the settings.

7.2.2 Configuring Ethernet WAN

1. In the left pane, under **Network**, click **Ethernet WAN**.
2. Set **Enable** to **Yes**.
3. Select a **WAN interface**.
4. Select a **Configuration Mode**.

   The “Manual (Static IP Address)” mode requires entering the values in the **Manual Settings** fields.
5. Click **Submit** to save the settings.

Use the Connectivity Monitor settings when WAN redundancy functionality is required. The Connectivity Monitor keeps checking the connection to the given remote host to determine the network status. If the ping does not get an answer within a given time window, it informs the WAN switch logic to try the secondary interface.

7.2.3 Configuring the mobile WAN interface

1. Set **Enable** to **Yes**.

2. If the SIM card is protected by a PIN code, enter the code in the **PIN Code** field.
   If necessary, change the SIM card's PIN code by using a mobile phone.
3. If automatic APN discovery does not work, define the APN settings.
   a) Set **APN Type** to **Manual**.
   b) Type the cellular access point name in the **APN** field according to the network operator's instructions.

   By default, the device uses automatic APN discovery with default APN values based on the network ID received from the cellular network. When *APN Type* is set to "Manual", the access point works as a gateway from the cellular network to the Internet. There are public and private access points. A public access point is usually defined. A private access point requires contract with a cellular operator. The device is compatible with both public and private access points.
4. If the cellular network's access point requires authentication, define the authentication settings according to the network operator's instructions.
   a) Set **Authentication** to **PAP** or **CHAP**.
   b) Type the access point's username in the **Username** field.
   c) Type the access point's password in the **Password** field.
5. If the device acts as a wireless router to Ethernet devices, and DNS is needed, enter the DNS settings.
   - Set **DNS Selection** to **From Network** to set up the device to receive DNS server IP addresses automatically from the cellular network.
   - Set **DNS Selection** to **Manual** to set up the device to use DNS servers manually defined in the **DNS Servers** field.
6. Click **Submit** to save the settings.
7. Restart the device to activate the configuration.

7.2.4 Setting WAN failover and backup routing

1. In the left pane, click **Network WAN Failover**.
2. Set **WAN Default Route** to **Yes**.
   This setting enables the use of the Ethernet WAN or the Mobile WAN as the default route interface.
3. Set the value of **Mobile WAN On Demand**.
   - If the backup WAN interface needs to come up only when the primary interface goes down, select **Yes**.
   - If both the wireless and Ethernet WAN interfaces have to be up all the time, select **No**.
4. Click **Submit** to save the settings.
5. Restart the device.

7.3 Routing parameters

The device has multiple configuration options that define routing.

Table 22: Routing parameters

Screen	Parameter	Value	Description
Ethernet WAN	Gateway (IP address)	(IP address)	IP address of router used to reach the internet. If not used, the field should be empty.
WAN Failover	WAN Default Route	Yes No	Usually "Yes" if the default route is defined by "static routes". “No” is required if the selection logic is done on VPN level.
	On Demand	Yes No	"Yes" activates the backup interfaces only when required. "No" makes all the WAN interfaces available simultaneously, for example, for VPNs.
	Primary WAN Interface	None Mobile WAN Ethernet WAN Ethernet WAN Secondary	These three settings configure the high-level default gateways. They must be configured to enable default route.
	Backup WAN Interface	None Mobile WAN Ethernet WAN	
	Secondary Backup WAN Interface	None Mobile WAN Ethernet WAN Ethernet WAN Secondary	
OpenVPN Client Settings	Interface	Any WAN Ethernet WAN Wireless WAN Ethernet LAN	This setting defines which interface to use for connection.
	Routing mode	None Host Net Default route	This setting defines how the routing is configured with OpenVPN. See OpenVPN application note.

7.4 Configuring the network monitor

The network monitor detects Internet connectivity drops by sending ping packets to designated targets. Its use is recommended.

1. In the left pane, under **Network**, click **Monitor**.
2. Set Enable to Yes.
3. Enter IP addresses for ping targets in **Target** and **Secondary target**.
4. Set the other values in the view.
   The user interface contains information on the default values.
5. Click **Submit** to save the settings.

7.5 Configuring DNS proxy

The solution does not require name resolution because IP addresses are used directly in configuration. If name resolution is needed (for example, for browsing the Web), the device act as a DNS server for the devices connected to local LAN. When the DNS proxy is enabled, the device is defined as the DNS server for LAN devices (either manually or through DHCP) and the device forwards the name queries to the actual DNS server and back to the LAN devices.

1. In the left pane, under **Services**, click **Common**.
2. Set **Use DNS Proxy** to **Yes**.
3. Click **Submit** to save the settings.

7.6 Checking network status

The device has user interface views and LEDs that show network status and are useful in troubleshooting situations.

1. In the left pane, under **System**, click **Status** to view network status information.
2. In the left pane, under **Tools**, click **Modem Info** to view the status of the wireless modem.
3. Check if the cellular LED is flashing, indicating network traffic.

8 Serial port configuration

8.1 Configuring serial ports

1. In the left pane, under **Serial Port and I/O**, click **General Configuration**.
2. Select an **Application Mode** for each serial port.
   - Serial Gateway: Transparent connection to any serial device
   - IEC-104: IEC-101 to IEC-104 conversion with IEC-101 serial device protocol
   - Modbus: Modbus conversion with Modbus/RTU or Modbus/ASCII serial device protocol

8.2 Serial gateway

The serial gateway feature enables data from the serial port attached device to be routed to Ethernet/mobile network (serial over IP) and vice versa. Serial gateway processes the transmitted data transparently and does not alter it any way except for buffering it for transmission. Because of the transparent communication, any protocols can be used in actual communication between nodes.Serial gateway configuration depends on used protocols.

9 Additional system configuration

9.1 Changing passwords

1. In the left pane, under **Tools**, select **User Config**.
2. Type the old password in the **Old password** field.
3. Type the new password in the **New password** field and the **New password (confirm)** field.
4. Click **Submit** to save the settings.

See the cyber security deployment guideline for more information on password configuration.

9.2 Setting date and time

1. In the left pane, under **System**, click **Time**.
2. Set **Mode** to **Automatic (NTP)** or **Manual**.

   The “Automatic (NTP)” setting synchronizes the date and time with an remote NTP (or SNTP) server. The NTP server always defines the time in UTC time. The time zone can be set so that the device shows the time in a local format. There is also an NTP server in the device (NTP client and server), this enables the device to work as NTP server for the LAN devices.

3. Click **Submit** under the **Mode** setting.

   The lower part of the view is updated if the setting changed.

4. Check the time and date settings.

   - In the “Automatic (NTP)” mode, check the settings under **Current Time and Date (NTP mode)**, including **Time zone**, and click **Test NTP servers**.
   - In the “Manual” mode, enter the time and date in the **Time** and **Date** fields, respectively.

   Clicking **Copy PC** changes the device’s time and date settings to match the connected PC. This requires JavaScript support from the browser.

5. Click **Submit** to save the settings.

9.3 Restoring factory default settings

1. In the left pane, under **Tools**, click **Default settings**.
2. Select a configuration profile to overwrite with the factory default settings.
3. Click **Submit**.
4. In the confirmation dialog, click **OK**.
5. Restart the device.

9.4 Updating the firmware

Save a configuration profile as a backup of the current configuration before starting the firmware update.

Check that a valid firmware package is stored on the PC before attempting to update the firmware.

1. In the left pane, under Tools, select **Firmware Update**.
   The current firmware version is shown in the **Firmware Update** view.
2. Click **Browse** to open the file selection dialog.
3. Select the new firmware file.
4. Click **Update**.
   A confirmation dialog opens.
5. Click **OK** to confirm firmware.
   The update takes a few minutes.
6. Once the update is finished, restart the device.

9.5 Saving configuration profiles

It is possible to save the device's configuration in a profile for use in other devices or as a backup when updating the firmware. The configuration can be exported as an XML file.

1. In the left pane, under **Tools**, select **Configuration profiles**.
2. Click **Create a new profile**.
3. Select a profile to clone.
   Selecting **Last Boot** allows saving the configuration in use when the device was booted the previous time.
4. Type a name for the profile.
5. Click **Submit** to save the profile.

It is possible to clone, export, and import profiles in the same view.

10 Service configuration

10.1 Configuring services

1. In the left pane, click **Services**.
   The service categories are listed under **Services**.
2. Click a service category.
3. Configure the service with the service parameters listed in the view.
4. Click **Submit** to save the settings.

10.2 Service parameters

Table 23: Common

Name	Description	Value range
Common Services		
Use DNS Proxy	Determines if the device acts as a DNS server for LAN devices	No, Yes
LLMNR responder	The link-local multicast name resolution is a protocol that enables machines on LAN to find the device using its hostname. By default, the device uses its hostname (for example, arctic-02xxyy).	No, Yes
mDNS responder	The multicast domain name system is a protocol that enables Mac® OS X® machines on LAN to find the device using its hostname (for example, arctic-02xxyy).	No, Yes
SSH Server	The SSH (secure shell) is an encrypted network protocol for safe remote command line connections. It is replacing the Telnet protocol.	
SSH Server	Determines if logging into the device using SSH is allowed. The device has internal SSH server, which allows incoming SSH connections when enabled. By default, the SSH service is enabled for LAN connections.	No, Yes

Table continues on the next page

Name	Description	Value range
SSH protocol version	Selects which SSH protocol versions are enabled in SSH Server. It is recommended to allow only SSH protocol version 2 (SSH2) to be used.	SSH1, SSH2
SSH public keys	SSH Public keys can be added for remote logins with SSHkeys.	

Table 24: DHCP server

Name	Description	Value range
DHCP Server Settings		
Enabled	Determines if the device acts as a DHCP server in LAN	No, Yes
Required Settings		
Subnet	Defines the address of the subnet to listen to	
Subnet mask	Defines the subnet mask of the subnet to listen to	
Range low IP address	Defines the lowest IP address to share	
Range high IP address	Defines the highest IP address to share	
Optional Settings		
Domain name	DNS domain name given to clients	
DNS Servers	List of DNS servers (comma separated)	
Gateway IP address	IP address of the default gateway. This must usually be defined as Arctic's own IP address.	
Broadcast IP address	Usually the last IP address of the subnet	
Default lease time	Given to clients that don't request a specific lease length (empty:10800)	
Maximum lease time	The maximum lease time given to clients (empty:10800)	
NTP Servers	List of NTP servers (comma separated)	
LPR Servers	List of line printer (LPR) servers (comma separated)	
WINS Servers	List of WINS servers (comma separated)	

Table 25: DynDNS client

Name	Description	Value range
DynDNS client settings		
DynDNS service client enabled		No, Yes
DynDNS service provider	Selects the supported dyndns service provider	
DynDNS client update interval	Defines how often (in seconds) the device's IP is checked	
DynDNS hostname	Arctic name reported to service, for example, host name	
DynDNS username	User name for dyndns service	
DynDNS password	Service password	
DynDNS logging enabled	Logs dyndns update to system log	No, Yes

Table 26: SNMP agent

Name	Description	Value range
SNMP Agent		
Enable SNMP	Enables SNMP	No, Yes
Read only SNMP community	Defines read only SNMP community	
Read and write SNMP community	Defines read and write SNMP community	
Server port	The default server port is 161.	

Table 27: Arctic Patrol

Name	Description	Value range
Basic Information		
Enabled	Enables Viola Patrol	No, Yes
Name	Free-text field for the unique name of the Patrol connection	
Registration password	Password needed to register to server with HTTPS protocol. This password should not be entered after registration unless re- registering is necessary.	

Table continues on the next page

Name	Description	Value range
Protocol	Patrol communication protocol	HTTPS, SSH
Connection interval	Defines how often to report to server	Seconds
Server Information		
Server address, server port	Server IP address and the port the server listens. If no value is given, the value is 10000.	
SSH Settings (Only needed for SSH protocol)		
SSH local identity	SSH private key to be used if the SSH connection protocol is selected.	
SSH public key	SSH public key to be used if the SSH connection protocol is selected. This key can be copied to Patrol server.	
Remote identity	SSH public key of the Patrol server	
Connection mode	The connection mode defines how the Patrol server polls the clients in the SSH protocol mode. In case of a large number of Patrol connections in the server, the polling mode is recommended.	Polling, continuous
Options		
Backup active configuration to server	When set to “Yes”, copies encrypted version of the XML configuration file to the server.	No, Yes
Allow remote management	Enables remote management by Patrol server	No, Yes
Allow LAN device scan	Allows periodical local network scan for ABB devices. Currently, the supported device is RIO600.	No, Yes

11 IEC-104 application settings

11.1 The use of the IEC-104 protocol

The IEC-104 and IEC-101 protocols share the same ASDU level messaging but differ on the link level. IEC-104 is intended for packet-switched TCP/ IP communication whereas IEC-101 is intended for serial communication. By using the device, the IEC-101 slaves (for example RTUs) can be connected to a IEC-104 master (for example SCADA). The device requests an event from the IEC-101 slave locally and sends them to the IEC-104 master. This eliminates the need to continuously poll the data remotely and therefore reduces the communication costs on pay-per-use wireless network.

See the technical note about Wireless Controller RTU_interoperability for more information on IEC 60870-5-104 and IEC 60870-5-101 interoperability.

11.2 Configuring IEC-104 application settings

1. In the left pane, select **Serial Port and I/O/IEC-104 Gateway (RSx)**.
2. View and change settings in the view that opens.
3. Click **Submit** to save the settings.

11.3 IEC-104 application settings

Table 28: IEC-104 application settings

Name	Description	Value range
Basic settings		
Enable IEC-104 gateway	Enables or disables IEC-104 to IEC-101 gateway functionality.	No, Yes
Serial settings	The serial settings define the properties of physical serial communication between the device and an IEC-101 slave. The selection between RS-232/422/485 is made with physical DIP switches located below the RS2 serial port.	
Serial port	Indicates the serial port to which the settings apply.	RS1, RS2

Table continues on the next page

Name	Description	Value range
Speed	IEC-101 serial communication speed (bits per second)	1200, 2400, 4800, 9600, 19200, 38400, 57600
Data bits	Number of data bits used on IEC-101 serial communication	5, 6, 7, 8
Parity	Parity method used on IEC-101 serial communication	None, Even, Odd
Stop bits	Number of stop bits used on IEC-101 serial communication	1, 2
Use HW flow control	HW flow control mechanism (RTS/CTS) on IEC-101 serial communication. Note: The HW handshaking is available only on RS-232 mode.	No, Yes
Network settings	The Network settings define the general TCP/IP networking properties between the device and the IEC-104 master.	
Network protocol	Network protocol defines the network transmission layer protocol (either TCP or UDP) used on IEC-104 network communication. The IEC-104 standard protocol uses TCP, but for reliable slow speed packet switched networks (for example Mobitex), the UDP protocol can be used to minimize the packets transmitted over network. Note: The IEC-104 standard specifies only TCP protocol.	UDP, TCP
Network protocol to listen	TCP or UDP port number to listen for incoming IEC-104 connections	0...65000
Network idle timeout	Network idle timeout defines the idle timeout of the network connection in seconds. If there is no network data received during the specified interval, the connection is closed by the device. This parameter is required in order to detect partially closed connections and release the resources for new connections especially if the New connection priority parameter is disabled. Value “0” disables the network idle timeout detection. The network idle timeout must be longer than IEC-104 link test interval (t3).	0...65000
New connection priority	It defines the action when a new connection request arrives while a connection is already active. If the set value is ”No”, the new connection is rejected. If the set value is ”Yes”, the present connection is terminated and the new connection is accepted. It is recommendable to set this value to “Yes” in normal configurations having only one IEC-104 master.	No, Yes

Table continues on the next page

Name	Description	Value range
Max clients	Max clients defines the maximun number of connections (redundancy group).	1...3
IEC-104 settings	The IEC-104 settings define the properties of IEC-104 link layer and application layer parameters as described in the IEC 60870-5-104 standard. The IEC-104 communication is carried out between the device and the IEC-104 master over the TCP/IP network.	
TX window size (k)	TX window size defines the maximum number of I format APDU packets the device may send before requiring the IEC-104 master to acknowledge them. If there are k unacknowledged frames sent the device stops polling IEC-101 slave for events until acknowledgement is received. The k must be always less than the maximum sequence number defined below. The IEC-104 standard suggests k to be 12.	1...20
RX window size (w)	RX window size defines the maximum number of I format APDU packets the device may receive before sending acknowledgement to the IEC-104 master. The w should not exceed two-thirds of TX window size k. The IEC-104 standard suggests w to be 8.	1...20
I frames TX timeout (t1)	It defines the timeout in seconds the device waits for acknowledgement from IEC-104 master after sending last I format APDU or control frame (e.g. link test). If no acknowledgement is received during the defined time the device will close the network connection and the IEC-101 link. The t1 must be longer than the network round-trip-time. The IEC-104 standard suggests 15 seconds.	1...255
I frames RX timeout (t2)	This defines the timeout in seconds from the last received I format APDU before sending acknowledgement. The t2 must be smaller than t1. The IEC-104 standard suggests 10.	1...255
Link test interval (t3)	This defines the interval in seconds how often the IEC-104 link is tested if there is no other activity. The recommended value depends on the criticality of the link. The IEC-104 standard suggests 20 seconds but for pay-per-use GPRS connections the practical value may be substantially longer.	1...65000
Test link on suspended state	Answer to test frame activation if the 101 link is in the suspended state.	No, Yes
Suspended timeout	This defines the time in seconds how long a connected IEC-104 link can be in suspended state (STOPD) before the device closes the connection. Using this parameter increases the proba-	1...65000

Table continues on the next page

Name	Description	Value range
	bility of detecting partially closed network connections especially in UDP mode.	
Max sequence number	These are the maximum sequence number used in IEC-104 communication. The default value “0” equals to 32767 as suggested by the IEC-104 standard.	0...32767
Flush buffered events on connection	Defines if buffered events are flushed on new a IEC-104 connection.	No, Yes
Cause of transmission length	It defines the length of IEC-104 Cause of transmission ASDU header field in bytes. The IEC-104 standard defines value “2”.	1, 2, 3
Common address length	This defines the length of IEC-104 Common address ASDU header field in bytes. The IEC-104 standard defines value “2”.	1, 2, 3
Info object address length	This defines the length of IEC-104 Information object address ASDU header field in bytes.	1, 2, 3
IEC-101 settings	The IEC-101 settings define the properties of IEC-101 link layer and application layer parameters as described in the IEC 60870-5-101 standard. The IEC-101 communication is carried out between the device and a IEC-101.	
Slave link address	The link-level address of IEC-101 slave.	1...65000
Link address field length	Defines the length of the IEC-101 link-level address field in bytes. The link-level address of IEC-101 slave.	1, 2
Event poll interval	Event poll interval defines the IEC-101 event polling interval in 0.1 second increments (class 1 or 2 poll). The events are polled only when the IEC-104 connection is active.	1...65000
Link test interval	Link test interval defines the IEC-101 link test interval in 0.1 second increments. Link test is performed if there is no other activity. The link test is performed if there is no other activity during defined interval.	1...65000
Keep link open	Defines that the IEC-101 link is kept always open even when there is no active IEC-104 connection. If the functionality is enabled the device sends link test frames and restarts the IEC-101 link if the test fails. The events are still not polled before the IEC-104 connection is active. Some IEC-101 slaves require the link to be continuously open in order to operate.	No, Yes

Table continues on the next page

Name	Description	Value range
Reply header timeout	Defines the timeout in milliseconds that the device waits the reply to start from IEC-101 slave after command or request.	1...65000
Reply end timeout	Defines the maximum duration of IEC-101 slave response in seconds.	1...65000
Retry limit	Defines the number of retries sent to a IEC-101 slave in case of no reply. If no reply is still received the device closes the IEC-101 and IEC-104 connections.	0...65000
Cause of transmission length	Defines the length of IEC-101 cause of transmission ASDU header field in bytes. The IEC-101 standard defines value 1.	1, 2, 3
Common address length	Defines the length of the IEC-101 common address ASDU header field in bytes. The IEC-101 standard defines value 2.	1, 2, 3
Info object address length	Defines the length of IEC-101 information object address ASDU header field in bytes. The IEC-101 standard defines value 2.	1, 2, 3
ASDU Converter	The ASDU converter can be used to convert ASDU header field lengths between IEC-101 and IEC-104 protocols.	
Use ASDU converter	This defines if the ASDU header level conversion between IEC-101 and IEC-104 is performed. If enabled the ASDU header field lengths are converted between IEC-104 and IEC-101. This parameter must be enabled if the ASDU header lengths differ between the IEC-104 and the IEC-101. The information on the field must fit in the shorter one of the two. It's not possible to convert e.g. value 12000 to a one byte field.	No, Yes
Use ASDU type replacer	The ASDU type replace function can be used to convert an ASDU type (Original type) to another (Applied type) type e.g. in cases when the IEC implementation differs between master and slaves.	No, Yes
IEC-101 ASDU type	The original ASDU type searched by ASDU type replacer.	0...255
IEC-104 ASDU type	The new ASDU type is replaced by the original type.	0...255
Convert short IEC-101 time stamps	Defines if 56-bit timestamps are converted to 24-bit.	No, Yes
Packet collector	The packet collector can be used to collect many IEC-101 messages and events to a single network packet instead of sending every message sepa-	

Table continues on the next page

Name	Description	Value range
	rately. This function is useful for slow packet switched communication network (for example Mobitex) for speeding up especially the general interrogation response.	
Use packet collector	Determines if the packet collector is in use.	No, Yes
Max bytes	Max bytes defines the maximum bytes trigger for packet collector. Before a new packet is inserted into the packet collector buffer the amount of bytes is checked. If the insertion of the new packet would cause the number of bytes in the packet collector to exceed MAX BYTES, the old content is sent to the network before inserting the new one. The value should be smaller than the MTU/MRU of network used.	1...1500
Max time	Max time defines the maximum collect time trigger for packet collector in 0.1 second increments for packet collector. If there has been data on packet collector over MAX TIME, the data is sent to network. The value must be smaller than t1.	1...255
Max packets	Max packets defines the maximum amount of IEC-101 packets stored into the packet collector before sending the data to the network.	1...255
Other settings		
Write syslog	Write syslog defines if the error messages are stored to system log file or not. The system log is available by using Web user interface.	No, Yes

12 Modbus application settings

12.1 Modbus Gateway properties

The Modbus Gateway is an adapter application enabling conversions between serial and network Modbus protocols. The gateway can operate in one mode: connecting the network master to serial slaves.

The gateway offers a number of core properties.

- Supports Modbus RTU and Modbus ASCII serial protocols
- Supports Modbus TCP, Modbus RTU over TCP, Modbus RTU over UDP, Modbus ASCII over TCP and Modbus ASCII over UDP network protocols
- Generates and filters out gateway exceptions
- Makes automatic connection management
- Enables multiple server sessions over the network
- Offers unlimited amount of masters on the network side

12.2 Modbus mode

Network master to serial slaves

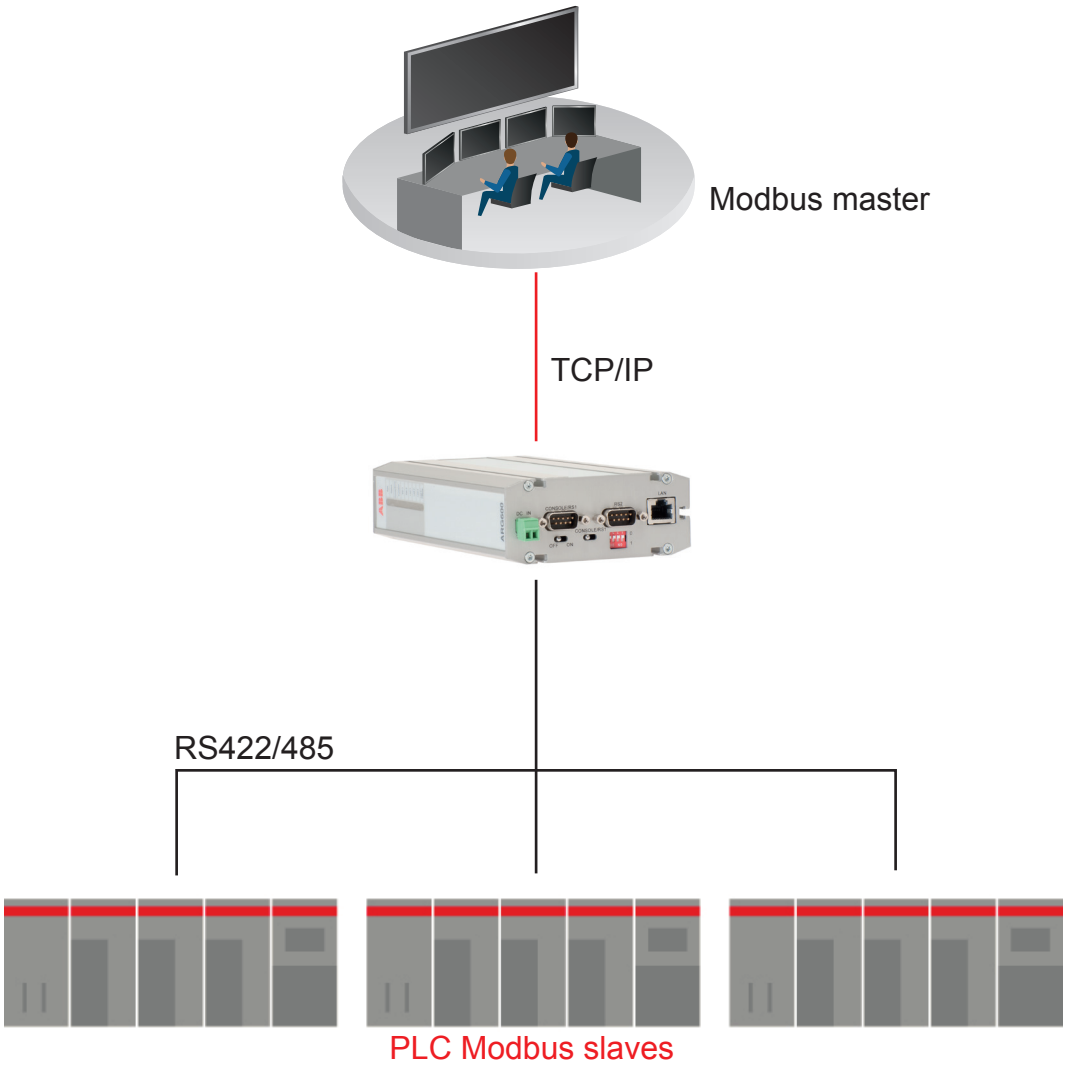

Figure 19: Network master to serial slaves mode

In the “Network master to serial slaves” mode, the device acts like network server where masters (clients) can connect (the default port being 502) and transmit Modbus requests. The device makes conversions between network and serial protocols. If the slave does not reply during defined timeout or if the reply is corrupted, the device sends “gateway exception message” back to the master if the exception generation is enabled. Otherwise, the reply is returned. Multiple masters can connect simultaneously to the Gateway, which handles the multiplexing between masters.

12.3 Configuring the network master to serial slaves mode

1. In the left pane, under **Serial Port and I/O**, click **Modbus Gateway (RSx)**.
2. Set **Enable Modbus gateway** to **Yes**.
3. Set **Gateway mode** to **Network master to serial slaves**.
4. Set the parameters under **Serial settings, Protocols, Framing, Exceptions** and **Network server settings** as the network and the Modbus master and slaves require.
5. Click **Submit** to save the settings.
6. Restart the device.

12.4 Parameter settings

Table 29: Parameters

Name	Description	Value range
Basic settings		
Enable Modbus gateway	If set to “Yes”, the Modbus gateway functionality is enabled for the serial port. Each serial port of the device has its own Modbus gateway definitions.	No, Yes
Serial settings		
Serial port	Defines the serial port that the device uses for Modbus serial communication. The possible settings are “RS1”, which selects serial port 1 (RS-232 console/application port) and “RS2”, which selects serial port 2 (RS-232/422/485 application port). If a single serial port or RS-422/485 is required, port 2 is recommended. If Port 1 is used, the console switch of the device must be in the Application position. DIP switches below the DB-9 serial connector specify the RS-232/422/485 settings of Port 2.	RS1, RS2
Serial settings		
Speed	Defines the serial port speed for Modbus communication in bps. The optimal speed depends on the connected Modbus equipment.	300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Data bits	Defines the number of data bits used in Modbus serial communication. The required number depends on how many data bits the connected Modbus equipment supports. Generally Modbus	5, 6, 7, 8, Auto

Table continues on the next page

Name	Description	Value range
	RTU communication uses 8 data bits and Modbus ASCII communication uses 7 data bits.	
Parity	Defines the parity method used in Modbus serial communication. If set to “None”, no parity method is used. If set to “Even”, an even parity bit is generated and inspected. If set to “Odd”, odd parity bits are generated and inspected.	None, Even, Odd
Stop bits	Defines the number of stop bits used in Modbus serial communication.	1, 2
Use HW handshaking (CTS/RTS)	Enables CTS/RTS handshaking if set to “Yes”.	No, Yes
Gateway mode		
Gateway mode	If set to “Network master to serial slaves”, the slaves are on the serial side.	Network master to serial slaves
Protocols		
Serial protocol	Defines the Modbus protocol that serial devices use in serial communication. The possible settings are Modbus RTU protocol and Modbus ASCII protocol. ModbusRTU is recommended because it is more efficient.	ModbusRTU, ModbusASCII
Network protocol	Defines the TCP/IP and Modbus protocol used on network communication. Possible protocols are Modbus TCP protocol over TCP, Modbus RTU protocol over TCP, Modbus RTU protocol over UDP, and Modbus ASCII protocol over UDP.	ModbusTCP, ModbusRTU over TCP, ModbusRTU over UDP, ModbusASCII over TCP, ModbusASCII over UDP
Framing		
Slave response timeout	Defines the time in microseconds (millionths of a second) how long the device waits for the response from a Modbus slave. If the response is not received, the device can generate and return a Modbus gateway exception. The reply timeout of the Modbus master must be greater than the gateway device timeout. Otherwise, the flow of request-reply communication is violated. The device does not accept a new request before the reply from the slave is received or the reply timeout is elapsed. The delays in network communication can vary especially in wireless networks. When the slaves are located on the network side, ping or another method should be used to estimate the delay packets spend on network.	0...90 000 000 (0...90 seconds)

Table continues on the next page

Name	Description	Value range
Inter-frame timeout	Defines the idle time in microseconds (millionths of a second) that marks the end of Modbus frame in serial communication. If the value is zero, the device uses the standard 4 character time. The recommendation is to use a value as small as possible to speed up communication and increase the value if problems arise. Some PC programs can insert unexpected delays between serial characters.	0...2 000 000 (0...2 seconds)
Exceptions		
Generate gateway exceptions	Defines if the device generates and returns a Modbus gateway exception message to the master if no valid reply is not received from the slave. If set to “Yes”, the generation of exceptions is enabled. This functionality is useful for debugging.	No, Yes
Pass gateway exceptions	If set to “Yes”, gateway exception replies from the slave side are passed to the master. If set to “No”, the replies are filtered away.	No, Yes
Network server settings		
Server TCP/UDP - port	Defines the TCP or UDP port that masters can form connections to. Default Modbus TCP/IP communication port is 502. If multiple Modbus gateways are running on same device (for both serial ports) the TCP/UDP communication ports must not be same. For example, ports 502 and 504 can be used. The network and the device's firewalls must enable TCP or UDP communication for that port.	1...32500
Max. number of clients	Defines how many network masters can be connected to the device simultaneously. The recommended value is at least 2 when using TCP communication. Otherwise if the device does not recognize a partially closed connection, forming new connections is not accepted by the device the time set in parameter “Connection idle timeout” is elapsed.	0...20
Connection idle timeout	If there has not been communication on this route during given amount of seconds, the device automatically closes the TCP connection to slave and therefore frees the slave’s communication resources. This is especially useful when multiple masters access the same slave. The recommended setting is about two times the polling interval of the master.	0...32500
Enable keepalive	Defines if connection testing is performed by sending TCP keepalive packets at certain intervals. enabled for TCP network communication. If set to “Yes”, testing the TCP connection with slave is enabled.	No, Yes

13 Technical data

Technical specifications can be changed without notification. For information on the supported mobile data speed, see the mobile data reference guide.

Table 30: Dimensions

Description	Value
Height × Width × Depth	175 × 160 × 108 mm
Weight	2.4 kg
Protection class	IPX0 IP20 (device mounted and all connectors connected)

Table 31: Hardware

Description		Value
Processor environment	Processor	32 bit RISC
	Memory	128 MB Flash
		128 MB RAM
Other	Sensor	Temperature
	Internal clock	Real time
Power	Power supply	Nominal auxiliary voltage U_n: 100...165 V DC or 100...240 V AC 50/60 Hz Auxiliary voltage variation: 85...200 V DC or 90...264 V AC
		20...30 V DC (external battery)
	Frequency range	45...65 Hz
	Input current, 100% load, 230 V AC	0.8 A
	Efficiency, typical (230 V AC, 100% load)	>83%
	Isolation	Input/ground 1500 V AC RMS 50 Hz 1 min Input

Table continues on the next page

Description		Value
		Output 3000 V AC RMS 50 Hz 1 min
		Output/ground 500 V DC
	Inrush current 25°C, 230 V AC	<25 A <5 ms
	Input fuse	T3.15 A high breaking
	Power consumption	10 W typical (when not charging battery), 60 W (full charging)
	Overvoltage transient protection	VDR 275 V AC 72 J
	Holdup time (230 V, 100% load)	>50 ms
Casing		Aluminium shell
Approvals		CE
Environmental conditions	Temperature range [1]	-30...+55°C (non condensing)
		-40...+70°C (storage)
	Relative humidity	5...85% RH

Table 32: Battery recommendations

Description	Yasa NP 17-12	Yasa NPL 24-12
Rated voltage	12 V	12 V
Capacity	17 Ah	24 Ah
Weight	6.1 kg	9 kg
Size (L × W × H)	181 × 76 × 167 mm	166 × 175 × 125 mm

Table 33: Supply for external devices and input circuits (X2.1 pin 6)

Description	Value
Output voltage	21...29 V
Output current	1 A continuous, 2.2 A peak
Output overvoltage protection level	30.5 V

[1] The maximum operating temperature is +40°C at 1 A load on X2.1 pin 6.

Table 34: Temperature-compensated charger for batteries

Description	Value
Rated charging voltage	27.4 V at 20°C
Output power	60 W
Fuse	4 A
Temperature compensation	-40 mV/°C
Output overvoltage protection level	30.5 V

Table 35: Supported protocols

Master protocol	Slave protocol
IEC 60870-5-104	IEC 60870-5-101
IEC 60870-5-104	Modbus TCP
IEC 60870-5-104	Modbus RTU/ASCII
IEC 60870-5-104	Modbus (RTU) profile for Horstmann Compass B
IEC 60870-5-104	Modbus (RTU) profile for Kries IKI-50
IEC 60870-5-101	Modbus RTU
IEC 60870-5-101	Modbus TCP
IEC 60870-5-101	Modbus (RTU) profile for Horstmann Compass B
IEC 60870-5-101	Modbus (RTU) profile for Kries IKI-50
Modbus TCP	Modbus RTU
TCP/IP	Serial gateway - serial port data stream (such as DNP3)

Table 36: Supported protocols for I/O controlling

Master protocol
IEC 60870-5-104
IEC 60870-5-101

Table 37: Default I/O configuration

Description		Value
Digital inputs (0...60 V DC, >18 V DC detected as 1) [1]	Digital inputs for the disconnector status control • Disconnector 1: Open/closed, local/remote use, grounding open/closed – 5 pcs • Disconnector 2: Open/closed, local/remote use, grounding open/closed – 5 pcs • Disconnector 3: Open/closed, local/remote use, grounding open/closed – 5 pcs	15
	Extra general purpose digital inputs reserved for other use	2
	Total number of digital inputs	17
Digital outputs (1 A/30 V DC continuous carry)	Digital outputs for the disconnector open/close command • Disconnector 1: Open/close – 2 pcs • Disconnector 2: Open/close – 2 pcs • Disconnector 3: Open/close – 2 pcs	6
	Digital output for the load cut (motor overload protection)	1
	Digital output for the test load of the battery test (test load)	1
	Digital output for the external heater	1
	Extra general purpose digital output reserved for other use	1
	Total number of digital outputs	10
Analog inputs (-5...+5 V measurement, ±300 mV for -10...+55°C, 0 V...+5 V)	Load measurement (DC motor load current)	1

Table continues on the next page

[1] Digital inputs are designed for reading the status of the feeder (open, traveling, closed) and not for detecting short-duration changes.

Description		Value
	Extra reserved for other use	1
	Total number of analog inputs	2

Table 38: I/O specifications

Description		Value
Digital inputs [1]	Number of digital inputs	17
	Operating range	18...60 V DC (>18 V DC detected as 1)
	Current drain	3.5...12.5 mA
	Power consumption/ input	<0.8 W
	Input polarity	bipolar
	Isolation	3 kV
Digital outputs	Number of digital outputs	10
	Output pin rated voltage	24 VDC
	Continuous carry 30 VDC	1 A

Table 39: Network interfaces

Description		Value
Ethernet ports	Ethernet/LAN	10/100 Base-T. Shielded RJ-45
		1.5 kV isolation transformer
		Ethernet IEEE 802-3, 802-2
Serial ports	Serial 1/Console	RS-232 DTE
		Male DB-9 connector
		IEC 60870-5-101 protocol support
		Full serial and modem signals
		300...460 800 bps
		Data bits: 7 or 8
		Stop bits: 1 or 2
		Parity: None, Even, Odd

Table continues on the next page

Description		Value
		Flow control: None, RTS/CTS
		Protection: 15 kV ESD and short circuit
		Console: RS-232, 19200 bps, 8 data bits, 1 stop bit, no parity (8N1)
	Serial 2	RS-232 DTE, RS-422, RS-485 (selectable)
		Male DB-9 connector
		IEC 60870-5-101 protocol support
		Full serial and modem signals
		300...460 800 bps
		Data bits: 7 or 8
		Stop bits: 1 or 2
		Parity: None, Even, Odd
		Flow control: None, RTS/CTS
		Protection: 15 kV ESD and short circuit

Table 40: Electromagnetic compatibility tests

Description		Reference
Emission tests according to the test specification IEC 61850-3 (Edition 2.0 2013-12)	Radiated disturbance	CISPR 16-2-3
	Conducted disturbance	CISPR 16-2-1
Immunity tests according to the test specification IEC 61850-3 (Edition 2.0 2013-12)	Electrostatic discharge (ESD)	EN 61000-4-2 (2008-12)
	Radiated radiofrequency electromagnetic field	EN 61000-4-3 (2006-02)
	Electrical fast transient (EFT)	EN 61000-4-4 (2012-04)
	Surge	EN 61000-4-5 (2005-11)
	Conducted radiofrequency electromagnetic field	EN 61000-4-6 (2008-10)
	Power frequency magnetic field	EN 61000-4-8 (2009-09)
	Voltage dips	EN 61000-4-11 (2004-03)

Table 41: RoHS and REACH compliancy

Description	Reference
Directive	RoHS directive 2002/95/EC
	REACH directive 2006/1907/EC

14 Appendix Installation and mounting instructions

14.1 Unpacking the device

The device is delivered in a package containing the device itself, a short antenna and four connectors. Accessories such as null-modem cables, hall-effect current transducers, test load resistors and roof antennas can be ordered separately.

1. Remove the transport packing carefully without force.

All packaging materials are recyclable. Follow the environmental regulations regarding the disposal of materials.

2. Examine the delivered products to ensure that they were not damaged during the transport. If any of the items is missing or damaged, inform the nearest ABB office or representative. ABB should be notified immediately if there are any discrepancies in relation to the delivery documents.

Handle the device carefully before installation on site.

14.2 Installing the device

- Install the device on the cabinet's DIN-rail with the mounting clips.
- As the device has a cellular network connection, consider the high-frequency radio waves it uses for data transmission and choose the installation site accordingly.
  - If the device with antenna is mounted directly to the antenna connector, avoid placing the device where nearby obstacles might disturb the radio signal.
  - In case of metal racks or surfaces, use an external antenna with an appropriate cable.

Walls with metallic structures, such as cabling or concrete iron, may degrade the antenna performance.

The protective earth screw terminal is located next to the DIN-rail mounting clips. The earth lead must always be properly connected, at least 6.0 mm^2 and as short as possible.

Use 1.5...2.5 mm^2 conductors for the device’s power supply connection.

Use a miniature circuit breaker (MCB) to disconnect ARC600 from the supply. The preferred rating for MCB is 16 A.

14.3 Installing the SIM card

Standard 3 V SIM cards (2 FF) can be used with the device's IEC 60870-5-104 gateway. A SIM card holder is located on the top panel near the antenna connector.

If the PIN code query is enabled, check that the correct PIN code is entered in the ARC600 configurator wireless WAN submenu.

1. Switch off power from the device.
2. Eject the SIM card holder by pushing the **Eject** button.
3. Remove the tray from the holder and place the SIM card onto the tray.
4. Insert the tray carefully back to the holder and press the tray until it is locked.

15 Glossary

AC	Alternating current
APN	Access Point Name
CHAP	Challenge handshake authentication protocol
CTS	Clear to send
DC	1. Direct current 2. Disconnector 3. Double command
DCD	Data carrier detect
DHCP	Dynamic Host Configuration Protocol
DI	Digital input
DIN rail	A standardized 35 mm wide metal rail with a hat-shaped cross section
DIP	Dual in-line package
DIP switch	A set of on-off switches arranged in a standard dual in-line package
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DNS	Domain Name System
DSR	Data set ready
DTE	Data Terminal Equipment
DTR	Data terminal ready
EMC	Electromagnetic compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
GND	Ground/earth
HMI	Human-machine interface
HTML	Hypertext markup language
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/output
IEC	International Electrotechnical Commission
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-104	Network access for IEC 60870-5-101
IP	Internet protocol
LAN	Local area network
LED	Light-emitting diode
MCB	Miniature circuit breaker

Modbus	A serial communication protocol developed by the Modicon company in 1979. Originally used for communication in PLCs and RTU devices.
Modbus ASCII	Link mode using 7-bit ASCII characters
Modbus RTU	Link mode using 8-bit binary characters
NT	Non-topical
NTC	Negative Temperature Coefficient
NTP	Network time protocol
PAP	Password authentication protocol
PIN	Personal Identification Number
RAM	Random access memory
RI	Ring Indicator
RISC	Reduced Instruction Set Computer
RJ-45	Galvanic connector type
RMU	Ring main unit
RS-232	Serial interface standard
RS-422	Serial communication standard (EIA–422)
RS-485	Serial link according to EIA standard RS485
RTS	Ready to send
RTU	Remote terminal unit
RXD	Received exchange data
SCADA	Supervision, control and data acquisition
SIM	Subscriber identity module
SMS	1. Short Message Service 2. Station monitoring system
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TXD	Transmit exchange data
UDP	User datagram protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide area network

ABB Distribution Solutions
Digital Substation Products
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11

www.abb.com/mediumvoltage
www.abb.com/relion
www.abb.com/substationautomation

1MRS758459 J