

RELION® PROTECTION AND CONTROL

REX615

IEC 60870-5-104 Communication Protocol Manual





Document ID: 2NGA001859

Issued: 2024-03-22

Revision: A

Product version: 1

© Copyright 2024 ABB. All rights reserved.

Copyright

ABB is the owner of the copyright in this document. This document or any parts thereof must not be reproduced or copied without the written permission from ABB and the contents thereof must not be used to any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB and Relion are registered trademarks of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Open Source Software

This product contains open source software. For license information refer to product documentation at www.abb.com.

Warranty

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

www.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 antivirus 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 following directive and regulations.

Directives of the European parliament and of the council:

- Electromagnetic compatibility (EMC) Directive 2014/30/EU
- Low-voltage Directive 2014/35/EU
- RoHS Directive 2011/65/EU
- RoHS Directive (EU) 2015/863 amending Annex II

UK legislations:

- Electromagnetic Compatibility Regulations 2016
- Electrical Equipment (Safety) Regulations 2016
- The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

These conformities are the result of tests conducted by the third-party testing in accordance with the product standard EN / BS EN 60255-26 for the EMC directive / regulation, and with the product standards EN / BS EN 60255-1 and EN / BS EN 60255-27 for the low voltage directive / safety regulation.

The product is designed in accordance with the international standards of the IEC 60255 series.

Contents

1	Introduction.....	10
1.1	This manual.....	10
1.2	Intended audience.....	10
1.3	Product documentation.....	11
1.3.1	Product documentation set.....	11
1.3.2	Document revision history.....	11
1.3.3	Related documentation.....	11
1.4	Symbols and conventions.....	11
1.4.1	Symbols.....	11
1.4.2	Document conventions.....	12
2	IEC 60870-5-104 overview.....	13
2.1	IEC 60870-5-104 protocol.....	13
2.2	Standard documentation.....	13
2.3	Communication link modes.....	13
2.4	Basic protocol functionality.....	14
3	Vendor-specific implementation.....	15
3.1	Protocol instances.....	15
3.2	IEC 60870-5-104 data objects.....	15
3.2.1	Single-point information.....	15
3.2.2	Double-point information.....	16
3.2.3	Measured value, short floating point.....	16
3.2.4	Measured value, scaled integer.....	17
3.2.5	Integrated totals.....	17
3.2.6	Step position.....	17
3.2.7	Single command.....	18
3.2.8	Double command.....	18
3.3	Value change detection.....	19
3.3.1	IEC104 protocol cyclic reporting.....	19
3.3.2	IEC 60870-5-104 data object configuration.....	19
3.4	IEC 60870-5-104 internal event buffering.....	19
3.5	Control operations.....	20
3.5.1	Single command.....	20
3.5.2	Double command.....	20
3.6	Integrated totals objects.....	21
3.6.1	Integrated totals object grouping.....	21
3.6.2	Freeze operation alternatives.....	22

3.7	Secure communication.....	22
3.7.1	Secure authentication setup.....	22
3.7.2	TLS encryption.....	23
3.7.3	Relay user and key management (IEC 60870-5-104 client).....	23
3.7.4	Secure authentication settings.....	24
3.7.5	Statistics and security events.....	25
3.7.6	Troubleshooting.....	25
3.8	Commissioning.....	25
3.8.1	Communication link settings.....	25
3.8.2	Secure communication settings.....	28
3.8.3	IEC 60870-5-104 application level settings.....	29
3.8.4	Update rate of analog and indication protocol data.....	31
3.8.5	Diagnostic values.....	32
3.8.6	Advanced protocol customization.....	33
4	IEC 60870-5-104 interoperability.....	35
4.1	Overview.....	35
4.2	System or device.....	35
4.3	Network configuration.....	35
4.4	Link layer.....	36
4.5	Application layer.....	37
4.6	Basic application functions.....	42
5	Secure authentication conformance statement.....	47
5.1	Overview of clause.....	47
5.2	Required algorithms.....	47
5.3	MAC algorithms.....	47
5.4	Key wrap algorithms.....	47
5.5	Use of error messages.....	48
5.6	Update key change methods.....	48
5.7	User status change.....	48
5.8	Configurable parameters.....	49
5.9	Configurable statistic thresholds and statistic information object addresses.....	50
5.10	Critical functions.....	50
6	IEC 60870-5-104 parameters.....	53
6.1	IEC 101-104 General settings.....	53
6.2	Secure communication parameters.....	54
6.2.1	IEC 101-104 Secure settings.....	54
6.2.2	IEC 101-104 Secure statistics thresholds settings.....	55
6.3	IEC 101-104 Monitored data.....	56
6.4	Monitored data for secure communication.....	56

6.4.1	IEC 101-104 Secure monitored data.....	56
7	Glossary.....	58

1 Introduction

1.1 This manual

The communication protocol manual describes a communication protocol supported by the protection relay. The manual concentrates on vendor-specific implementations.

1.2 Intended audience

This manual addresses the communication system engineer or system integrator responsible for pre-engineering and engineering the communication setup in a substation from a protection relay's perspective.

The system engineer or system integrator must have a basic knowledge of communication in protection and control systems and thorough knowledge of the specific communication protocol.

1.3 Product documentation

1.3.1 Product documentation set

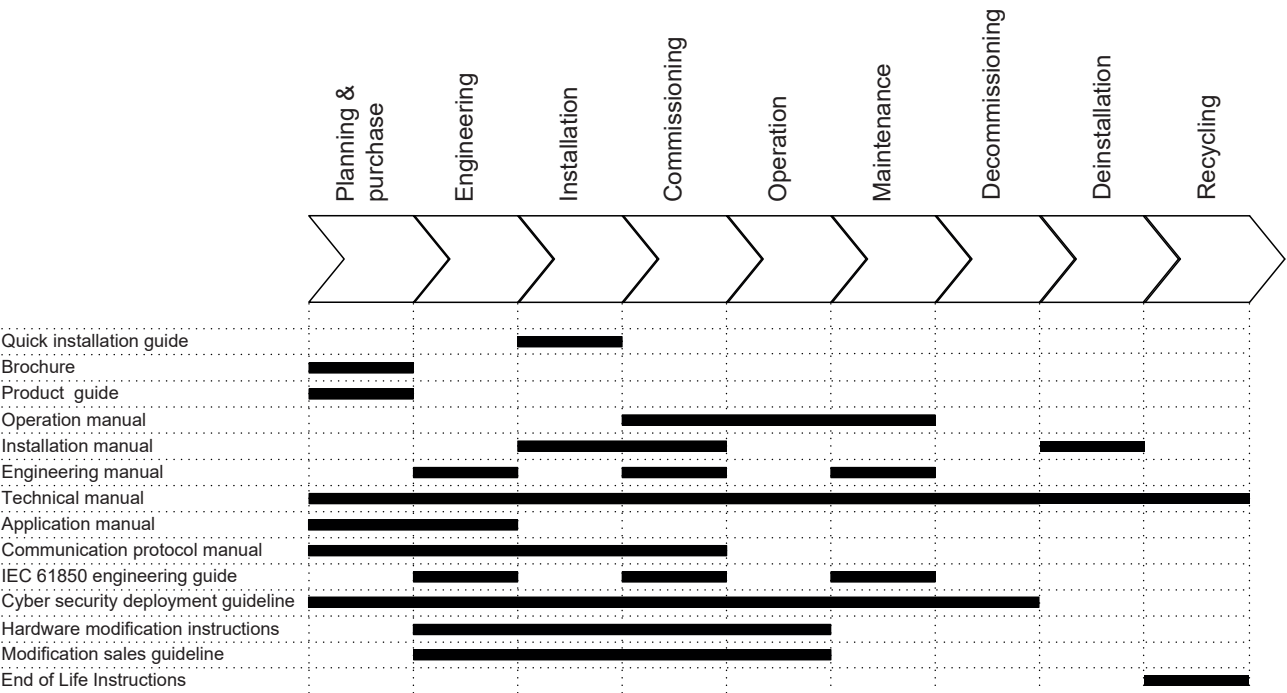


Figure 1: The intended use of documents during the product life cycle

1.3.2 Document revision history

Document revision/ date	Product release	History
A/2024-03-22	PCL1	First release

1.3.3 Related documentation



Download the latest documents from the ABB Web site www.abb.com/medium-voltage.

1.4 Symbols and conventions

1.4.1 Symbols



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".

- Input/output messages and monitored data names are shown in Courier font.

When the function starts, the *START* output is set to TRUE.

- Values of quantities are expressed with a number and an SI unit. The corresponding imperial units may be given in parentheses.
- This document assumes that the parameter setting visibility is "Advanced".

2 IEC 60870-5-104 overview

2.1 IEC 60870-5-104 protocol

The IEC 60870-5-104 protocol standard is officially named “Network access for IEC 60870-5-101 using standard transport profiles”. The protocol is based on existing IEC 61870-5-101 application and transport layer profiles while also including a network link layer specification for Ethernet/TCP communication. Sometimes IEC 60870-5-104 is referred to as IEC 60870-5-101 over Ethernet/TCP.

2.2 Standard documentation

Table 1: Standard documentation

Document	Description
IEC 60870-5-104: Network access for IEC 60870-5-101 using standard transport profiles.	This document includes combined definitions of the application layer parts of IEC 60870-5-101 used by the 104 protocol and the Ethernet TCP/IP transport functions used by the 104 protocol.
IEC 60870-5-101: Companion standard for basic telecontrol task (incl. amendments).	This document includes the application layer parts of the 101 standard which are used by the IEC 60870-5-104 protocol.
IEC 60870-5-1 Transmission frame formats IEC 60870-5-2 Link transmission procedures IEC 60870-5-3 General Structure of application data IEC 60870-5-4 Definition and coding of application data elements IEC 60870-5-5 Basic application functions IEC 60870-5-7 Transmission procedures, extension for secure communication	These documents include a detailed description of the protocol-related data and tasks.

2.3 Communication link modes

Two alternative communication link modes, unbalanced or balanced mode, are available for the communication between the client (controlling station) and the server (controlled station). In this case, since the IEC 60870-5-104 client establishes separate TCP (point-to-point) connections towards each IEC 60870-5-104 server, the balanced mode is the most commonly used.

In the balanced link mode, both the client and the server can initiate message transfers. In the unbalanced mode, the client initiates the transmission with a request to which the server responds.

2.4 Basic protocol functionality

The server (controlled station) delivers various data to the client.

- Data object values reported upon changes
- Data object values reported cyclically
- Responses to control commands
- Responses to read requests

The client can at any time request the present process data values by issuing interrogation commands. The command may be a general interrogation (GI) request, where all data objects with GI indication configured "ON" are reported. The data objects' GI indication configuration can also define that the data object belongs to a particular interrogation group, 1...16. In such a case, the client can request data interrogation values only from a specific interrogation group. A GI request reports values from all interrogation groups.

Integrated totals counter objects can be read on demand by the client using a counter interrogation request. Integrated totals objects can also be configured to report the counter values when counter freeze operations occur.

The client can issue single or double commands to single- or double-point control objects. Single controls are always direct control operations. For double command control objects (circuit breakers, controllable disconnectors), select-execute operations can be performed if the controllable target object allows it, but direct control of double-point objects is always possible. Controls can be given with or without time tags.

The client can additionally perform time synchronization commands and issue the corresponding delay acquisition request to the server.

3 Vendor-specific implementation

3.1 Protocol instances

The protocol can be started and run in up to five instances, one instance for each possible IEC 60870-5-104 client attached. The instances operate independently of one another, so it is possible to use different network link (TCP) and transport layer settings for each instance.

The protocol is not in use by default in the device. A function block I5CLPRT1... 5 representing the protocol instance must first be dragged to the application configuration sheet using Application Configuration. If only one instance is used, instance block 1 should be chosen. Additional instances can then be added freely.

After the function block has been added to the application configuration sheet, it needs to be enabled by assigning the protocol setting parameter *Operation* to "1-On".

In order for the protocol instance to populate its own database based on the point mapping defined by the *Map Select* parameter, the device must be restarted once. So, whenever *Operation* or *Map Select* settings are changed, the device must be restarted for the protocol instance to be properly set up according to the new configuration.



Figure 2: Function block

3.2 IEC 60870-5-104 data objects

Most of the device's internal IEC 61850 process data objects can be mapped to the IEC 60870-5-104 protocol. However, the potential protocol objects are not pre-mapped by default, so these objects should be mapped using Communication Management in PCM600.

The potential protocol objects have been pre-assigned into specific protocol ASDU types based on the source objects' IEC 61850 common data class (CDC) types. This pre-assignment cannot be changed.

3.2.1 Single-point information

Single-point information is derived from several IEC 61850 boolean data attributes (CDC.attribute/attribute/ ...).

- SPS.stVal
- SPC.stVal
- DPC.stSeld
- ACD.general/phsA/phsB/phsC/neut
- ACT.general/phsA/phsB/phsC/neut

Table 2: Single-point information

Type	ASDU		
GI	1	M_SP_NA_1	Single point
Event	30	M_SP_TB_1	Single point with CP56Time2a

3.2.2 Double-point information

Double-point information is derived from several IEC 61850 data attributes.

- DPS.stVal
- DPC.stVal

Table 3: Double-point information

Type	ASDU		
GI	3	M_DP_NA_1	Double point
Event	31	M_DP_TB_1	Double point with CP56Time2a

3.2.3 Measured value, short floating point

The short floating-point type (float32) is derived from the IEC 61850 data classes/ attributes defined for measurand values. The default scaling for the IEC 60870-5-104 value is 1, making it identical to the corresponding IEC 61850 measurand value (CDC.attribute/attribute/ ...).

- MV.instMag/mag.f
- CMV.cVal.mag.f/instCVal.mag.f
- DEL.phsAB.instCVal.mag.f/phsBC.instCVal.mag.f/phsCA.instCVal.mag.f
- DEL.phsAB.cVal.mag.f/phsBC.cVal.mag.f/phsCA.cVal.mag.f
- WYE.phsA.instCVal.mag.f/phsB.instCVal.mag.f/phsC.instCVal.mag.f
- WYE.neut.instCVal.mag.f/res.instCVal.mag.f/net.instCVal.mag.f
- WYE.phsA.cVal.mag.f/phsB.cVal.mag.f/phsC.cVal.mag.f
- WYE.neut.cVal.mag.f/res.cVal.mag.f/net.cVal.mag.f
- SEQ.c1.instCVal.mag.f/c2.instCVal.mag.f/c3.instCVal.mag.f

Table 4: Measured value, short floating point

Type	ASDU		
GI	13	M_ME_NC_1	Measurand, float32
Event	36	M_ME_TF_1	Measurand, float32 with CP56Time2a

3.2.4 Measured value, scaled integer

A scaled integer (int16) is derived from the IEC 61850 data classes/attributes defined for integer values, that is, the common data classes dealing with either integer or enumerat values. The default scaling for the IEC 60870-5-104 value is 1, making it identical to the corresponding IEC 61850 value (CDC.attribute/attribute/...).

- INS.stVal
- INC.stVal
- ENS.stVal
- ENC.stVal

Table 5: Measured value, scaled integer

Type	ASDU		
GI	11	M_ME_NB_1	Measurand, scaled integer
Event	33	M_ME_TE_1	Measurand, scaled integer with CP56Time2a

3.2.5 Integrated totals

Integrated totals counter values are derived from the IEC 61850 BCR (binary counter) class. Counter freezing means that the IEC 60870-5-104 stack latches the current BCR.actVal attribute to itself.

- BCR.actVal

Table 6: Integrated totals

Type	ASDU		
GI	15	M_IT_NA_1	Integrated totals
Event	37	M_IT_TB_1	Integrated totals with CP56Time2a

3.2.6 Step position

Tap changer step position information (-64...63) is derived from the IEC 61850 class BCS (binary controlled step position).

- BCS.ValWTr.stVal

Table 7: Step position

Type	ASDU		
GI	5	M_ST_NA_1	Step position
Event	32	M_ST_TB_1	Step position with CP56Time2a

3.2.7 Single command

Single-command control operations can be performed towards SPC (controllable single point) data class objects. Only direct controls are allowed.

- SPC.OperctlVal

Table 8: Single command

Type	ASDU		
Control	45	C_SC_NA_1	Single command
Control	58	C_SC_TA_1	Single command with CP56Time2a

3.2.8 Double command

Double-command control operations can be performed towards DPC (controllable double point) data class objects. Direct controls are always possible. Two-step select-execute controls are also possible if the target DPC object allows it. That is, the DPC control model setting must in such case be defined as SBO_WITH_ENHANCED_SECURITY. There are two different control objects available for the direct and select-execute alternatives.

- DPC.OperctlVal

Table 9: Double command

Type	ASDU		
Control	46	C_DC_NA_1	Double command
Control	59	C_DC_TA_1	Double command with CP56Time2a

3.3 Value change detection

The IEC 60870-5-104 data objects begin producing change events if the corresponding source IEC 61850 data objects reside in an IEC 61850 data set which is enabled for change reporting. Only the IEC 61850 data objects which reside in a data set are checked for value changes by the system.

Not all IEC 61850 data objects reside in data sets by default and not all data sets are enabled for reporting by default. The IEC 60870-5-104 protocol stack automatically checks the internal change reporting situation for all the single-point and double-point objects. If needed, the objects are assigned to an internal (hidden) data set. However, for measurand objects, the change reporting situation should be checked using Dataset editor in PCM600.

3.3.1 IEC104 protocol cyclic reporting

The IEC 61850 measurands are internally reported to the IEC 60870-5-104 protocol according to the rules stated in section [Chapter 3.8.4 Update rate of analog and indication protocol data](#). The IEC 60870-5-104 protocol has also a dedicated setting for its own cyclic transmission in **Configuration > Communication > Protocols > IEC 60870-5-101/104 (n) > Cyclical Period**. This cyclical period interval is not synchronized with the actual update rate of the measurement values, but only defines the sending rate of the cyclical reports. For adjusting the actual update rate of the analog value refer to chapter [Chapter 3.8.4 Update rate of analog and indication protocol data](#).

3.3.2 IEC 60870-5-104 data object configuration

1. The IEC 60870-5-104 data objects are selected and located in the address space using IEC 60870-5-104 Communication Management.
2. In Communication Management, the data objects' *Event enable* and *Interrogation* default settings are updated if necessary. If only general interrogation (GI) is performed, the point can be assigned to any interrogation group.
3. The corresponding IEC 61850 data objects are checked using Dataset editor. It must be ensured that the corresponding objects are located in a data set which is enabled for reporting.

An IEC 60870-5-104 data object works to some extent even if the object does not reside in a data set, or if it resides in a data set which is not enabled for reporting. In such a case, the IEC 60850-5-104 protocol does an internal, periodical polling of the native IEC 61850 value. If data object changes are noticed, the protocol reports them. However, this internal protocol polling cycle is slow, and thus value change updates are also slow.

3.4 IEC 60870-5-104 internal event buffering

The protocol stack instance internally stores change events based on ASDU event types. The event buffer size per ASDU type is 1000 events. However, this buffer is shared between all protocol instances activated in the relay. This means that with e.g. 1 instance active the full 1000 buffer is available, but with e.g. 5 instances only $1000 / 5 = 200$ events per instance can be queued at a given time until event buffer overflows. The protocol stack sends as many event data objects as possible of the same ASDU event type in one APDU frame.

3.5 Control operations

3.5.1 Single command

Single-command controls are performed towards SPC (controllable single point) IEC 61850 target objects. The command can be given with or without a time stamp (C_SC_NA_1, C_SC_TA_1). Only direct type operations are allowed.

If time-tagged commands are used, it is important to ensure the master and the relay times are synchronized. Also, time zone related settings need to be correct, such as the *Time zone* (UTC or local) setting and *local time offset* in general time settings if local time is used. The maximum accepted delay between the command time stamp and the relay time can be adjusted by the *Command delay* setting.

Many target SPC objects, such as acknowledgement or reset objects, are “transient only” objects. For these objects, only “On” control is relevant. If an “Off” control is performed to them, most often a positive acknowledgement is returned from the target function block, but the object’s action, for example, acknowledgement or reset, is not performed.

3.5.2 Double command

Double-command controls are performed towards DPC (controllable double point) IEC 61850 target objects, that is, circuit breakers and controllable disconnector objects. The command can be given with or without a time stamp (C_DC_NA_1, C_DC_TA_1).

If time-tagged commands are used, it is important to ensure the master and the relay times are synchronized. Also, time zone related settings need to be correct, such as the *Time zone* (UTC or local) setting and *local time offset* in general time settings if local time is used. The maximum accepted delay between the command time stamp and the relay time can be adjusted by the *Command delay* setting.

Each double-point DPC object has two predefined IEC 60870-5-104 control objects: one intended for direct operation and the other one for select-execute (select-before-operate) operation. The difference can be seen in the control object’s signal name trailing text.

...DPC-ctlVal-Direct

...DPC-ctlVal-SBO

3.5.2.1 Direct operation

Direct operation is possible for the double command if the controllable object has been configured to "Direct control" mode. If attempting to perform direct control for a controllable object in SBO mode, command is rejected and an error response is generated.

3.5.2.2 Select-execute operation

A two-step select-and-execute operation is possible only if the target DPC object's control model is configured as select-before-operate (SBO). For most target DPC objects, the default control model setting mode is SBO.

IEC 60870-5-104 selection timeout is defined by the protocol instance's *Selection Timeout* setting parameter. When a command is performed from the IEC 60870-5-104 instance, the selection timeout setting configured for the IEC 61850 DPC target object is overridden.

3.5.2.3 Cause of transmission and selected status

The relay's native IEC 61850 data model does not include any cause of transmission (COT) information data. Therefore, monitoring object transmissions from the IEC 60870-5-104 stack can only include the following cause of transmission values.

- 1 = Cyclical
- 3 = Spontaneous
- 20 = General interrogation
- 21...36 = Group 1...16 interrogation

The control command's response message returned to the controlling client includes COT value 11 = Remote command, but the controlled object value change in monitoring direction is always COT=3 (Spontaneous). While this information is not so important for the controlling client, it can be for another client in a multiple-client environment.

In IEC 61850, it is thought that the other client should monitor the DPC .stSeld (selected status) indication object. If the object goes ON, the DPC object has been selected for control operation. Based on the Local/Remote setting, this control selection is done either locally or remotely. The .stSeld indication object is activated only if the DPC object's control model is configured as SBO.

3.6 Integrated totals objects

Integrated totals objects M_IT_NA_1 (IT objects) are mainly cross-referenced from IEC 61850 binary counter (BCR) type objects. Forward or reverse energy is typically measured in these object types. The IT objects' time-tagged change reporting M_IT_TB_1 is optional and triggered by a freeze operation.

3.6.1 Integrated totals object grouping

The existing IT objects can individually be configured to belong to any IT object group 1...4. When an IT master command is performed, it can be directed only to a specific IT object group or to all IT object groups. There are two commands related to counter groups.

- Freeze counters, C_CI_NA_1 (FRZ) - Freezes/latches momentary counter values simultaneously and saves them as internal frozen counter values
- Read frozen counters, C_RD_NA_1 (RQT) - Requests the internally saved frozen counter values

3.6.2 Freeze operation alternatives

A freeze operation can be issued either by a master command C_CI_NA_1 (QCC=FRZ), or by an internal freeze pulse applied to the I5CLPRT function block's input IT_FRZ.

The new frozen counter values can be either sent spontaneously to the master, or they can remain internally in the protocol stack for later reading by the master using command C_CI_NA_1 (QCC=RQT).

A new freeze operation overwrites the previously stored frozen counter values.

The freeze command operation C_CI_NA_1 (QCC=FRZ) can be defined to be “freeze only” or “freeze and reset”. In the latter case, the protocol tries to reset the counters after the value freezing. Some IEC 61850 counters cannot be physically reset. The counters in this device are globally reset for all possible readers, for example, for other protocols and for reading via HMI.

Two setting parameters define how the freeze operation is handled.

- *Freeze mode* defines if the I5CLPRT function block's IT_FRZ input is used, and if the externally triggered operation is “freeze only” or “freeze and reset”.
- *Counter reporting* defines what happens after the counters have been frozen. Frozen counters can be configured for spontaneous reporting with this setting.



The IEC 60870-5 standard terms “memorize” and “memorize and increment” correspond to “freeze” and “freeze and reset”.

3.7 Secure communication

3.7.1 Secure authentication setup

The relay supports secure authentication based on the IEC 60870-5-7 standard with symmetric keys. The functionality follows the IEC 62351-5 security standard's authentication specification, but the “User Status Change” and “Update Key” functionality is not supported. The relay supports only one predefined user.

Secure application authentication can be used with or without TLS. The secure authentication is enabled in the relay by the setting parameter *Protocol Sec Mode* under **Configuration > Communication > Protocols > Secure IEC104 (n) > General**.

The relay supports one predefined user with user number 1 and username Common. This user has predefined OPERATOR access rights so the user can perform all the supported IEC 60870-5-104 protocol requests. The Update Key for this user must be predefined by Account Management in PCM600 using 'Configure Secure Communication'. The key length can be selected as 128 or 256 bits in the tool. When updating session keys for this user, only the MAC algorithm SHA256 / 16OCTET is supported.



When enabling secure communication in the relay, it is important to understand the expiration principles defined by the security standards! E.g. TLS certificate expiration, and user/key expiration + refreshing must be taken into account while designing the system and it's upkeep/maintenance, to keep communication live in the long run.

3.7.1.1

TCP port

The TCP port number 19998 is recommended by the security standard. The instance's default TCP port number does not change automatically into this value so it can be set with parameter *TCP Port* under **Configuration > Communication > Protocols > IEC 60870-5-101 > 104 (n)**.



After enabling security and writing the Predefined Update Key, reboot of the relay is required to start secure communication. PCM600 performs this reboot automatically.

3.7.2

TLS encryption

TLS (Transport Layer Security) is used for end-to-end cryptographic authentication at the application layer and is also supported by the IEC 60870-5-104 secure communication. TLS encryption for the IEC 60870-5-104 TCP communication can be enabled in the relay in several steps.

1. Importing of a public key certificate to the relay, which should be signed by a trusted certification authority (CA).
2. Configuring the IEC 60870-5-104 master to use TLS. A public key certificate must be signed by the same CA.
3. Setting the parameter *Protocol Sec Mode* to "TLS and appl. authentication" via **Configuration > Communication > Protocols > Secure IEC 104 (n) > General**.

See the cyber security deployment guideline for more information.

3.7.3

Relay user and key management (IEC 60870-5-104 client)

Only one predefined user is supported so it is not possible to add or modify the users in the relay. The predefined user Common has an Update Key with its bit length preset in PCM600 (128 or 256 bits). The IEC 60870-5-104 master can initialize the IEC 60870-5-104 communication for the Common user in two steps.

- Setting the matching Update Key in its User database for user Common/1
- Starting a Session Key Update sequence for the user in the client

If Session Key Update is successful, the relay responds with a SUCCESS status. If the configuration prevents the update of Session Key, the relay gives an error response and the relay's internal error diagnostic counters are incremented. Counters should be checked to troubleshoot the problem.

3.7.4 Secure authentication settings

3.7.4.1 Predefined behavior

Part of the secure authentication behavior is predefined in the relay.

Association Id

The relay supports up to five IEC 60870-5-104 protocol instances simultaneously. The Association Id for each instance corresponds to the protocol instance number in the menu structure and in Application Configuration.

Critical messages

The recommended listed (IEC 60870-5-7: 2003) mandatory Type Id (ASDU type) requests are critical commands for the relay. This list includes all control operations and time synch commands. A more comprehensive list can be found in the Protocol Implementation Conformance statement. These commands require additional authentication handshake (challenge-response) as defined by the standard.

User role

The relay supports only user Common, with OPERATOR rights providing access to all supported IEC 60870-5-104 requests.



Some IEC104 masters can use commands with time tags in secure mode. If time-tagged commands are used, check the relay and master time synchronization (for example, UTC/local settings). The time stamp difference that the relay accepts can be adjusted by the *Command delay* (ms) setting.

3.7.4.2 Security parameters

Various Secure Authentication parameters are configurable in the relay. The behavior of these parameters follows the IEC 62351-5 standard. The parameters and short descriptions are listed at the end of this manual. Here are explained some of the most relevant settings. Refer to the standard for more detailed information about these parameters.

Session Key Change Interval

This defines how often the master is expected to renew Session Keys. The interval is defined as number of messages or as time in seconds, whichever occurs first. Setting *Exp Sesn key Chg Intv* must be defined via **Configuration > Communication > Protocols > Secure IEC104 (n) > General** and setting *Exp Sesn key Chg Cnt* via **Configuration > Communication > Protocols > Secure IEC104 (n) > General**.

Reply Timeout

This setting defines the time the relay waits for responses to the authentication messages before reporting a timeout error. It is configured in milliseconds via **Configuration > Communication > Protocols > Secure IEC104 (n) > General**.

3.7.5 Statistics and security events

Security statistics counters analyze and diagnose authentication-related events. As required by the standard, the counters are preserved in the relay's memory during the device reboot. The statistics counters are available via **Configuration > Monitoring > Communication > Protocols > Secure IEC104 (n)**.

The security statistics are also readable as Typeld 41 (S_IT_TC) integrated totals data which is monitored by the IEC 60870-5-104 master. The master can obtain the counters by performing either a counter interrogation or a freeze command on the corresponding counter group. After a freeze command, the counters are reported to the master as spontaneous events if the *Counter reporting* parameter is set to "Spontaneous mode". Counter reset operation is not allowed due to security reasons.

The S_IT_TC objects' counter group and base IOA address are configured in **Configuration > Communication > Protocols > Secure IEC104 (n) > General > Sec Stat Cnt Grp** and **Configuration > Communication > Protocols > Secure IEC104 (n) > General > Sec Stat Cnt IOA**.

The IOA address of each security statistics counter is the base IOA address plus the standard index of the counter.

A threshold deadband can be set for the security statistics counters to filter reporting of counter values constantly as S_IT_TC events. The threshold setting is common to all security statistics counters and can be configured via **Configuration > Communication > Protocols > Secure IEC104 (n) > Statistics Thresholds**.

3.7.6 Troubleshooting

If the secure authentication communication cannot be successfully established, check the Pre-shared Update Key and MAC algorithm settings.

- Check that there is no mismatch between the Pre-shared Update Key and the Common user's update key of the IEC 60870-5-104 master or the user's Session Key is successfully updated.
- Check that the MAC algorithm settings match between the relay and the IEC 60870-5-104 master.

3.8 Commissioning

None of the available protocol instances are enabled by default. To take into use any instance (n), the setting *Operation* under **Configuration > Communication > Protocols > IEC60870-5-101/104 (n)** must be configured "On".

3.8.1 Communication link settings

Table 10: Communication link settings

Setting	Description
Operation	This enables the IEC 60870-5-104 protocol instance to work on the Ethernet link. This setting should be set to "On".
Client IP	The IP address of the IEC 60870-5-104 client for which this instance is intended. Only a TCP connection request from this client IP address is accepted for this instance. If the IP address is set to 0.0.0.0, any client is accepted. In such a case, it is possible to distinguish between different clients through different TCP connection port socket configurations for each instance.
TCP Port	TCP connection port socket used by this instance. The combination of the <i>Client IP</i> and <i>TCP Port</i> settings defines to which IEC 60870-5-104 client the instance is given.
Device address	Device address of this IEC 60870-5-104 instance. The default setting of <i>Link address length</i> parameter is "1" octet, which enables only Device address values 1...255.
ASDU address	Standard "Common address of ASDU". In most cases, this value should be the same as <i>Device address</i> . If it is set to another value, it may also have to be configured on the client side. The default setting of <i>ASDU address length</i> parameter is "1" octet, which enables only <i>ASDU address</i> values 1...255.
Link mode	Defines if the communication link is balanced or unbalanced. The default setting, balanced, is mostly used by IEC 60870-5-104 links. However, the unbalanced mode can also be used even though this link mode is more common for serial IEC 60870-5-101 links.
COT length	Length (number of octets used) of the Cause Of Transmission field. The default value is "2". The additional information included in the <i>COT length</i> = 2 alternative is however not supported by this IEC 60870-5-104 implementation.
IOA length	Information Object Address field length (number of octets used) definition. This means the object addresses of IEC 60870-5-104 data points. The default setting is "2" octets. In Communication Management of PCM600, 16-bit addresses are supported. Consequently, if this setting is changed to "1", it must be ensured that no point addresses higher than 255 are defined.
Link address length	Length (number of octets used) of the Link address field. The default setting is "1" octet. The length must match the configuration throughout the network. This field is filled with the <i>Device address</i> value.
ASDU address length	Length (number of objects used) of the "Common address of ASDU" field. The default setting is "1". This must be

Table continues on the next page

Setting	Description
	equal to <i>Link address length</i> because <i>Device address</i> and “Common address of ASDU” are equal. The length must also match the configuration throughout the network.
TX window (k)	Sliding window protocol (k) transmit window setting. This is the maximum difference between the receive sequence and the send state variable, that is, the maximum number of outstanding I (information) format APDUs. The default setting is "12". The value range is 1...20.
RX window (w)	Sliding window protocol (w) receive window setting. This is the maximum distance to the latest acknowledged I-format APDU. The default setting is "8". The value range is 1...20. The standard recommends that this setting should not exceed two thirds of the Tx window (k) setting.
TX timeout (t1)	Timeout for confirmation of application or test APDU messages. The default setting is 30 seconds [30000 ms]. Adjustable between 1 ms and 60 s.
RX timeout (t2)	Timeout for acknowledgements in case of no data messages. The default setting is 10 seconds [10000 ms]. Adjustable between 1 ms and 60 s. (t2) should be less than (t1).
Test interval (t3)	Timeout for sending test APDU frames in case of long idle state (no line activity). The default setting is 20 seconds [20000 ms]. Adjustable between 1 ms and 60 s.

3.8.1.1 Field length setting parameters

The client's field length configuration must match the setting of the IEC 60870-5-104 instance. Sometimes it may not be possible to configure these fields in the client. In such a case, the IEC 60870-5-104 settings must be forced to adjust to match the client. The default settings for COT length (1 octet) and IOA length (2 octets) are the most commonly used.

Regarding *Device address* and “Common address of ASDU”, a decision whether to use 1 or 2 octets addressing must be taken. The default setting of *Link address length* and *ASDU address length*, 1 octet, means that no higher addresses than 255 can be used.

IEC104 protocol has no built-in validation to check the field parameter lengths during encoding/decoding of packets. Thus, communication engineer must verify they are matching between client and server. Having field length parameter mismatch between the devices can lead to unexpected behavior. If, for example, *IOA length* is set to "1" octet, all configured data points with higher object addresses than 255 get their higher address byte masked out. For example, IOA address 4500 (Hex 1194) occurs as 148 (Hex 94). If another data point with address 148 has been created, these objects overlap one another.

3.8.1.2 Sliding window protocol and timeout settings

The link procedures are described in the standard IEC 60870-5-104/Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, [Chapter 4 IEC 60870-5-104 interoperability](#) and [Chapter 5 Secure authentication conformance statement](#).



If the IEC 60870-5-104 client disappears, the established TCP/IP socket connection is closed by the relay or server. This occurs either as a TCP socket keep-alive failure or as time-outs t1 and t2, whichever happens first.

3.8.2 Secure communication settings

The secure communication settings are found under **Configuration > Communication > Protocols > Secure IEC104(n) > General**.

Table 11: Secure communication settings

Setting	Description
Protocol Security Mode	Main selection for secure communication. Alternatives are "Off", "On" with application authentication or "On" with both TLS and application authentication.
Reply timeout	Reply time-out in milliseconds to the authentication messages before reporting a time-out error.
Exp Sesn key Chg Intv	Expected session key change interval in seconds. Value "0" indicates that an interval is not used.
Exp Sesn key Chg Cnt	Expected session key change count (number of messages).
Max Sesn key Stat Cnt	Maximum session key status count. Defines how many times a master can request session key status per key change interval. For security reasons, responses cease after this count.
Sec Stat Cnt Grp	The IEC 60870-5-104 secure communication diagnostic counters M_IT_TC belong to the same counter group, 1...4.
Sec Stat Cnt IOA	Information object address for secure communication statistic counters. The 16 counters occur sequentially starting from this object address. No other protocol data should be stored in this address range.

3.8.2.1 Statistic counters threshold configuration

The M_IT_TC secure communication diagnostic counters reporting over IEC 60870-5-104 are based on threshold values. The threshold for each counter can be configured under **Configuration > Communication > Protocols > Secure IEC104(n) > Statistics Thresholds**.

Table 12: Statistic counters threshold settings

Setting	Description
Unexpected Msgs	Counter threshold value for unexpected messages
Auth failures	Counter threshold value for authorization failures
Authn failures	Counter threshold value for authentication failures
Reply timeouts	Counter threshold value for reply time-outs
Rekeys Authn failure	Counter threshold value for rekeys due to authentication failure
Total Msgs Tx	Counter threshold value for transmitted messages
Total Msgs Rx	Counter threshold value for received messages
Total Crit Msgs Rx	Counter threshold value for received critical messages
Discarded Msgs	Counter threshold value for discarded messages
Error Msgs Tx	Counter threshold value for transmitted error messages
Error Msgs Rx	Counter threshold value for received error messages
Successful Authn	Counter threshold value for successful authentications
Sesn key Chg	Counter threshold value for session key changes
Failed Sesn key Chgs	Counter threshold value for failed session key changes
Upd key Chgs	Counter threshold value for update key changes
Failed Upd key Chgs	Counter threshold value for failed update key changes

3.8.3 IEC 60870-5-104 application level settings

The settings are located under **Application Configuration > Protocols > IEC 60870-5-101 > 104 (n)**.

Table 13: IEC 60870-5-104 application level settings

Setting	Description
Map Select	Selects one of the protocol data point mappings, 1 or 2, to be used by this instance. The data point mappings can be created using Communication Management in PCM600. Several IEC 60870-5-104 protocol instances can use the same mappings.
Show bad time	Enabled by default. The relay has an internal, fixed criterion for tagging change event's time stamps as "bad". It means that the relay has not been time-synchronized for a specific time period. The "bad" time stamp criterion is based on the accuracy demands stated for the native IEC 61850 standard change events. The IEC 60870-5-104 change events are derived from these native events. It is possible to discard the "bad time" tag for IEC 60870-5-104 events.
Time zone	The change event time stamps can be reported in either UTC or local time. The default setting is UTC time. This setting is also relevant when using IEC 60870-5-104 control commands

Table continues on the next page

Setting	Description
	with time tags. The client-provided time stamp must be given in this defined time format. The setup of the local time, meaning the relative time adjustment to be made between UTC (GMT) time and local time, is done elsewhere in the relay.
Overflow mode	In case of internal indication event buffer overflow, it is possible to define whether to keep the oldest or the newest events in the buffer. The default setting keeps the oldest events and also adds an overflow event as the last event. It is possible to omit overflow handling by setting this parameter to "Keep newest" and defining <i>OvInd IOA</i> to value "0".
OvInd IOA	Single-point object address for the overflow indication. The default value is address "60000". Value "0" means that no overflow indication object exists. When an overflow indication occurs, the client can trigger a GI request.
OvInd NoGI IOA	Single-point object address for overflow indications occurring in objects which are not subject to GI. If overflow from these objects occurs, a GI request from the client does not reveal any lost data and thus GI request is unnecessary. It is possible to make this address equal to the <i>OvInd IOA</i> address, and thus generate overflow indication for all data object types.
Selection timeout	Protocol-dependent timeout between select and execute control commands. The controllable object also has a timeout setting configured, mainly intended for local control operation. When the control command is performed remotely from this protocol, the configured timeout is temporarily overridden by this setting. The default timeout value is 30 seconds.
Counter reporting	Counter objects, that is, integrated totals, can be reported spontaneously or be read on demand by the client using a counter interrogation request. This setting enables or disables the spontaneous counter reporting based on freeze operation. The freeze operation can be given from the client as a request or also be triggered externally through the protocol function block's physical <i>EC_FRZ</i> control input.
Freeze Mode	Defines if the counter freeze operation should only freeze (latch) the current counter values or also reset the counters. The default setting is "Not in use", meaning that the client should read (interrogate) the counters on demand.
IT_FRZ	Control point for counter freeze operation. This control is logically connected to the function block's <i>EC_FRZ</i> input. For test purposes, it is possible to manually trigger a counter freeze operation and spontaneous transmission with this setting.
Cyclical period	Event-generating data objects can alternatively be configured for cyclical transmission. This data point specific configuration can be done by Communication Management in

Table continues on the next page

Setting	Description
	PCM600. The <i>Cyclical period</i> setting defines the periodical reporting time of these cyclical data objects.
Command delay	Defines the maximum delta time (internal delay) allowed for client control commands with time stamps.

3.8.4 Update rate of analog and indication protocol data

Update rate of protocol data depends on multiple factors that need to be considered when communication engineering is done. This chapter describes the mechanism how process data change is updated to IEC 60870-5-103, IEC 60870-5-104, Modbus and DNP3 communication protocols to process it further.

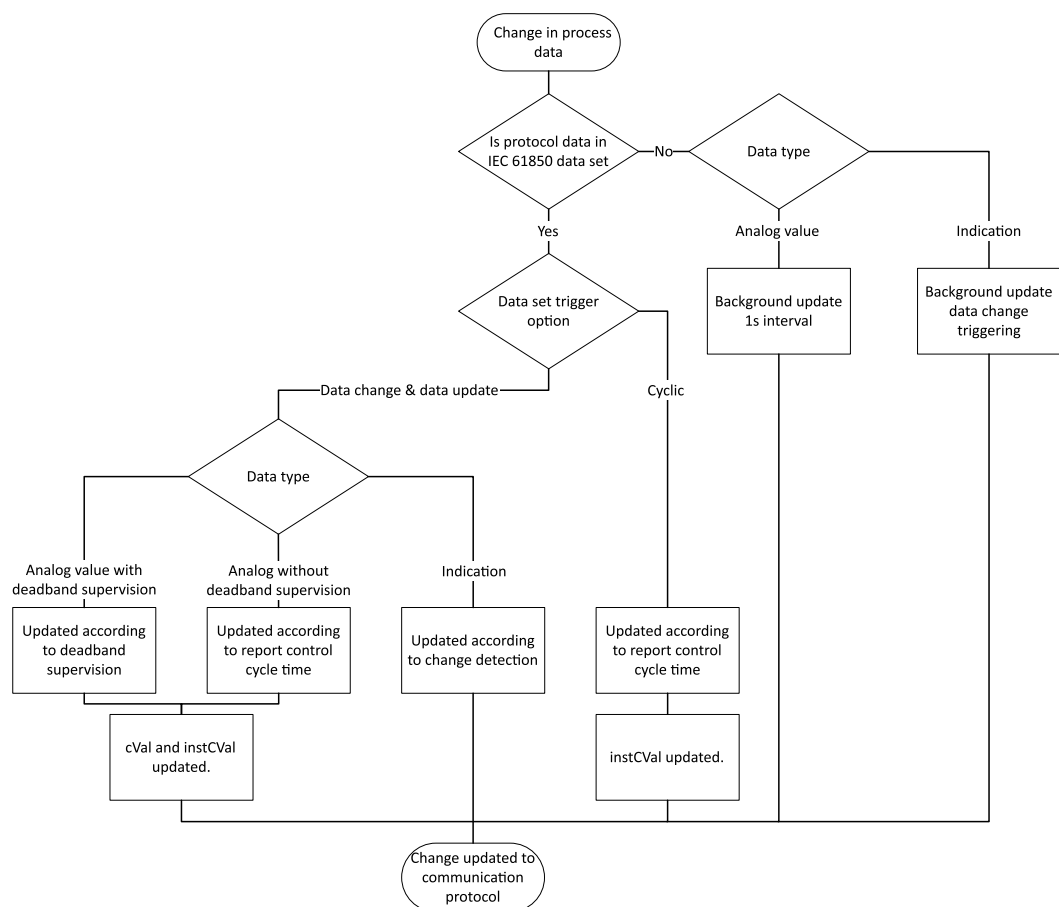


Figure 3: Data flow from process data change to communication protocol

Dataset and Report Control in IEC 61850

Data update rate is dependent of data set and report control engineering in IEC 61850 tool. In most cases default values are suitable, as typically essential measurement and indication data is by default mapped to IEC 61850 dataset and report control block. However, it may be necessary to understand all dependencies, if some customization or modification to update rates is needed:

- Data set content
- Trigger options for report control

- Signals selected in communication management (instantaneous or deadband supervised value)



Engineering of dataset and report control blocks is described in IEC 61850 Engineering Guide.

Measurement data

Typically, the commonly used measurement data, such as current/voltage measurement is included in IEC61850 default dataset with data_change + data_update trigger options. In this scenario the update rate depends on the set 'deadband' setting of the measurement function itself. This can be adjusted by the function specific deadband settings, described more in the Technical Manual. In addition, if the default report control trigger options have been changed, and cyclical triggering is used instead of data update + data change, the update rate is the integrity period IntgPd of the report control block. This may be useful for cyclical update of specific measurement data.

Some measurement functions do not have internal deadband supervision in the function. In this case the datasets integrity period IntgPd (see IEC61850 Engineering Manual) defines the update speed of the data.

Third possibility is, that the measurement data does not reside in a IEC61850 dataset. In this scenario the protocol internally polls the analog value once per second. If the one second poll period is more suitable for the application, it is also possible then to remove the specific measurement data points from dataset in IEC61850 tool.

Indication data

Commonly used indication data, such as protection start/trip and other important values are by default included in a IEC61850 dataset. If the protocol has CMT mappings of indication data that does not belong to a IEC61850 dataset, the protocol adds this data automatically to an internal update mechanism that enables still a fast update for the time-critical events.

3.8.5 Diagnostic values

The diagnostic values can be edited via **Application Configuration > Protocols > IEC 60870-5-101 > 104 (n)**.

Table 14: Diagnostic values

Setting	Description
STATUS	True if the protocol instance is active
Reset counters	Diagnostic counters reset. As defined by the standard, this does not reset the security diagnostic counters (see Table 16).
Received frames	Number of received IEC 60870-5-104 protocol frames
Transmitted frames	Number of IEC 60870-5-104 protocol frames
Link errors	Number of link layer errors
Physical errors	Number of physical layer errors

Table continues on the next page

Setting	Description
Transport errors	Number of transport layer errors
CnReject no sockets	Number of rejected TCP connections due to unavailable sockets
CnReject unregistered	Number of rejected TCP connections due to an unregistered client

3.8.5.1 Secure authentication diagnostic counters

The secure authentication diagnostic counters are located under **Monitoring > Communication > Protocols > Secure IEC104 (n)**.

Table 15: Secure authentication diagnostic counters

Counter	Description
Unexp Msgs Cnt	Number of unexpected messages
Auth Fail Cnt	Number of authorization failures
Authn Fail Cnt	Number of authentication failures
Reply timeouts Cnt	Number of reply time-outs
Rekey Authn Fail Cnt	Number of rekeys due to authentication failure
Total Msgs Tx	Number of messages transmitted
Total Msgs Rx	Number of messages received
Critical Msgs Rx Cnt	Number of critical messages received
Discarded Msgs Cnt	Number of discarded messages
Err Msgs Tx Cnt	Number of error messages transmitted
Err Msgs Rx Cnt	Number of error messages received
Successful Authn Cnt	Number of successful authentications
Session Key Chg Cnt	Number of session key changes
Fail Ses Key Chg Cnt	Number of failed session key changes
Upd Key Chgs Cnt	Number of update key changes
Fail Upd Key Chgs Cnt	Number of failed update key changes

3.8.6 Advanced protocol customization

Different advanced customization features are supported by the protocol; these features can be enabled via the Prtl Customization configuration parameter.

The Prtl Customization parameter is a 31-bit bitmask. Currently, bit zero (0) is in use. The setting value for each customization feature is calculated by the following formula: $2^{(\text{bit number})}$.

3.8.6.1 IEC104 advanced customization features

The following table summarizes each of the advanced features supported by the protocol.

Table 16: IEC104 Advanced customization features

Parameter	Value (Range)	Unit	Step	Default	Description		
Prtl Customization	0	-	1	0	Bit number (n)	Value (2*n)	Feature
						0	All customization is disabled
					0	1	Disables TCP keep-alive messages sending
					1	2	Disables TCP socket disconnection when the Link t1, t2 or t3 interval time expires after the set number of retries is reached
					2 - 30	4 - 107374 1824	Reserved for future use

In order to enable multiple features is it necessary to calculate the value for each required feature and add all of the afterwards. E.g. in order to disable the sending of TCP keep-alive messages and socket disconnection on Link Keep-Alive interval timer's expiration the setting value is calculated as $2^0 + 2^1, 3$.

The use of advanced customization features can be monitored in **Monitoring > Communication > Protocols > IEC60870-5-101/104(n)**.



Possible firmware version dependent expansions to customization parameter can be queried from ABB Customer support.

4 IEC 60870-5-104 interoperability

4.1 Overview

This companion standard presents sets of parameters and alternatives from which subsets have to be selected to implement particular telecontrol systems. Certain parameter values, such as the number of octets in the COMMON ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This Clause summarizes the parameters of the previous Clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers it is necessary that all partners agree on the selected parameters.

The selected parameters should be marked in the white boxes.

- ☐ Function or ASDU is not used
- ☒ Function or ASDU is used as standardized (default)
- ☐ R Function or ASDU is used in reverse mode
- ☐ B Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.



The full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

4.2 System or device

(System-specific parameter, indicate the station's function by marking one of the following with "X".)

- ☐ System definition
- ☐ Controlling station definition (client)
- ☒ Controlled station definition (server)

4.3 Network configuration

(Network-specific parameter, all configurations that are used are to be marked with “X”.)

- ☒ Point-to-point
- ☐ Multipoint-party line
- ☒ Multiple point-to-point
- ☐ Multipoint-star

4.4 Link layer

(Network-specific parameter, mark all used options with an “X”. Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the Type ID and COT of all messages assigned to class 2.)

Frame format FT 1.2, single character 1 and the fixed time-out interval are used exclusively in this companion standard.

- Link transmission procedure
- Address field of the link
- ☒ Balanced transmission

☐ Not present (balanced transmission only)

☒ Unbalanced transmission

☒ One octet

☒ Two octets

☒ Structured

☒ Unstructured

- Frame length
- Maximum length L (control direction)

Maximum length L (monitor direction)

Time during which repetitions are permitted (Trp) or number of repetitions

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

- ☐ The standard assignment of ASDUs to class 2 messages is used as follows:

Type identification	Cause of transmission

- ☐ A special assignment of ASDUs to class 2 messages is used as follows:

Type identification	Cause of transmission

4.5 Application layer

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

(System-specific parameter, mark all used configurations with an “X”.)

☒ One octet

☒ Two octets

Information object address

(System-specific parameter, mark all used configurations with an “X”.)

☒ One octet

☒ Structured

☒ Two octets

☒ Unstructured

☒ Three octets

Cause of transmission

(System-specific parameter, mark all used configurations with an “X”.)

☒ One octet

☒ Two octets (with originator address). Originator address is set to zero if not used

Selection of standard ASDUs

Process information in monitor direction

(Station-specific parameter, mark each Type ID with an “X” if it is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒	<1>:= Single-point information	M_SP_NA_1
☐	<2>:= Single-point information with time tag	M_SP_TA_1
☒	<3>:= Double-point information	M_DP_NA_1
☐	<4>:= Double-point information with time tag	M_DP_TA_1

Table continues on the next page

☒	<5>:= Step position information	M_ST_NA_1
☐	<6>:= Step position information with time tag	M_ST_TA_1
☐	<7>:= Bitstring of 32 bit	M_BO_NA_1
☐	<8>:= Bitstring of 32 bit with time tag	M_BO_TA_1
☐	<9>:= Measured value, normalized value	M_ME_NA_1
☐	<10>:= Measured value, normalized value with time tag	M_ME_TA_1
☒	<11>:= Measured value, scaled value	M_ME_NB_1
☐	<12>:= Measured value, scaled value with time tag	M_ME_TB_1
☒	<13>:= Measured value, short floating point value	M_ME_NC_1
☐	<14>:= Measured value, short floating point value with time tag	M_ME_TC_1
☒	<15>:= Integrated totals	M_IT_NA_1
☐	<16>:= Integrated totals with time tag	M_IT_TA_1
☐	<17>:= Event of protection equipment with time tag	M_EP_TA_1
☐	<18>:= Packed start events of protection equipment with time tag	M_EP_TB_1
☐	<19>:= Packed output circuit information of protection equipment with time tag	M_EP_TC_1
☐	<20>:= Packed single-point information with status change detection	M_SP_NA_1
☐	<21>:= Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>:= Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>:= Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>:= Step position information with time tag CP56Time2a	M_ST_TB_1
☐	<33>:= Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
☐	<34>:= Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>:= Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>:= Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1

Table continues on the next page

☒	<37>:= Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>:= Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>:= Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40>:= Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either ASDUs of the set <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <17> or of the set <30...40> are used.

Process information in control direction

(Station-specific parameter, mark each Type ID with an “X” if it is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒	<45>:= Single command	C_SC_NA_1
☒	<46>:= Double command	C_DC_NA_1
☐	<47>:= Regulating step command	C_RC_NA_1
☐	<48>:= Set point command, normalized value	C_SE_NA_1
☐	<49>:= Set point command, scaled value	C_SE_NB_1
☐	<50>:= Set point command, short floating point value	C_SE_NC_1
☐	<51>:= Bitstring of 32 bit	C_BO_NA_1
☒	<58>:= Single command with CP56Time2a	C_SC_TA_1
☒	<57>:= Double command with CP56Time2a	C_DC_TA_1

System information in monitor direction

(Station-specific parameter, mark with an “X” if it is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☐	<70>:= End of initialization	M_EI_NA_1
--------------------------	------------------------------	-----------

System information in control direction

(Station-specific parameter, mark each Type ID with an “X” if it is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒	<100>:= Interrogation command	C_IC_NA_1
☒	<101>:= Counter interrogation command	C_CI_NA_1

Table continues on the next page

☒	<102>:= Read command	C_RD_NA_1
☒	<103>:= Clock synchronization command (option see 7.6)	C_CS_NA_1
☒	<104>:= Test command	C_TS_NA_1
☐	<105>:= Reset process command	C_RP_NA_1
☒	<106>:= Delay acquisition command	C_CD_NA_1

Parameter in control direction

(Station-specific parameter, mark each Type ID with an "X" if it is only used in the standard direction, "R" if only used in the reverse direction, and "B" if used in both directions.)

☐	<110>:= Parameter of measured value, normalized value	P_ME_NA_1
☐	<111>:= Parameter of measured value, scaled value	P_ME_NB_1
☐	<112>:= Parameter of measured value, short floating point value	P_ME_NC_1
☐	<113>:= Parameter activation	P_AC_NA_1

File transfer

(Station-specific parameter, mark each Type ID with an "X" if it is only used in the standard direction, "R" if only used in the reverse direction, and "B" if used in both directions.)

☐	<120>:= File ready	F_FR_NA_1
☐	<121>:= Section ready	F_SR_NA_1
☐	<122>:= Call directory, select file, call file, call section	F_SC_NA_1
☐	<123>:= Last section, last segment	F_LS_NA_1
☐	<124>:= Ack file, ack section	F_AF_NA_1
☐	<125>:= Segment	F_SG_NA_1
☐	<126>:= Directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1

Type identifier and cause of transmission assignments

(Station-specific parameters)

Shaded boxes: option not required.

Blank: functions or ASDU not used.

Mark the Type Identification/cause of transmission combinations.

"X" if only used in the standard direction

"R" if only used in the reverse direction

"B" if used in both directions

Type identification		Cause of transmission																
		Periodic, cyclic	Background scan	Spontaneous	Initialized	Request or requested	Activation	Activation confirmation	Deactivation	Deactivation confirmation	Activation termination	Return info caused by a remote cmd	Return info caused by a local cmd	File transfer	Interrogated by group <number>	Request by group <n> counter request	Unknown type identification	Unknown cause of transmission
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45
<1>	M_SP_NA_1			X		X									X			
<2>	M_SP_TA_1																	
<3>	M_DP_NA_1			X		X									X			
<4>	M_DP_TA_1																	
<5>	M_ST_NA_1			X	X													
<6>	M_ST_TA_1																	
<7>	M_BO_NA_1																	
<8>	M_BO_TA_1																	
<9>	M_ME_NA_1																	
<10>	M_ME_TA_1																	
<11>	M_ME_NB_1	X		X		X									X			
<12>	M_ME_TB_1																	
<13>	M_ME_NC_1	X		X		X									X			
<14>	M_ME_TC_1																	
<15>	M_IT_NA_1															X		
<16>	M_IT_TA_1																	
<17>	M_EP_TA_1																	
<18>	M_EP_TB_1																	
<19>	M_EP_TC_1																	
<20>	M_PS_NA_1																	
<21>	M_ME_ND_1																	
<30>	M_SP_TB_1			X		X						X	X					
<31>	M_DP_TB_1			X		X						X	X					
<32>	M_ST_TB_1			X	X													
<33>	M_BO_TB_1																	
<34>	M_ME_TD_1																	
<35>	M_ME_TE_1			X		X												
<36>	M_ME_TF_1			X		X												
<37>	M_IT_TB_1			X												X		
<38>	M_EP_TD_1																	
<39>	M_EP_TE_1																	
<40>	M_EP_TF_1																	

Table continues on the next page

Type identification		Cause of transmission																
		Periodic, cyclic	Background scan	Spontaneous	Initialized	Request or requested	Activation	Activation confirmation	Deactivation	Deactivation confirmation	Activation termination	Return info caused by a remote cmd	Return info caused by a local cmd	File transfer	Interrogated by group <number>	Request by group <n> counter request	Unknown type identification	Unknown cause of transmission
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45
<45>	C_SC_NA_1						X	X	X	X	X						X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X
<47>	C_RC_NA_1																	
<48>	C_SE_NA_1																	
<49>	C_SE_NB_1																	
<50>	C_SE_NC_1																	
<51>	C_BO_NA_1																	
<58>	C_SC_TA_1						X	X	X	X	X						X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X
<70>	M_EI_NA_1 ¹																	
<100>	C_IC_NA_1						X	X	X	X	X						X	X
<101>	C_CI_NA_1						X	X			X						X	X
<102>	C_RD_NA_1					X												
<103>	C_CS_NA_1			X			X	X									X	X
<104>	C_TS_NA_1																	
<105>	C_RP_NA_1																	
<106>	C_CD_NA_1																	
<110>	P_ME_NA_1																	
<111>	P_ME_NB_1																	
<112>	P_ME_NC_1																	
<113>	P_AC_NA_1																	
<120>	F_FR_NA_1																	
<121>	F_SR_NA_1																	
<122>	F_SC_NA_1																	
<123>	F_LS_NA_1																	
<124>	F_AF_NA_1																	
<125>	F_SG_NA_1																	
<126>	F_DR_TA_1 ¹																	

¹ Blank or X only

4.6 Basic application functions

Station initialization

(Station-specific parameter, mark with an “X” if the function is used.)

☐ Remote initialization

Cyclic data transmission

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒ Cyclic data transmission

Read procedure

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒ Read procedure

Spontaneous transmission

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

☒ Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

(Station-specific parameter, mark each information type with an “X” where both a Type ID without time and a corresponding Type ID with time are issued in response to a single spontaneous change of a monitored object.)

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1

☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1

☐ Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)

☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1

Table continues on the next page

- ☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
- ☐ Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station interrogation

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☒ global
- | | | |
|---|--|--|
| ☒ group 1 | ☒ group 7 | ☒ group 13 |
| ☒ group 2 | ☒ group 8 | ☒ group 14 |
| ☒ group 3 | ☒ group 9 | ☒ group 15 |
| ☒ group 4 | ☒ group 10 | ☒ group 16 |
| ☒ group 5 | ☒ group 11 | |
| ☒ group 6 | ☒ group 12 | |

Information object addresses assigned to each group must be shown in a separate table.

Clock synchronization

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☒ Clock synchronization
- ☒ Day of week used
- ☐ RES1, GEN (time tag substituted/ not substituted) used
- ☒ SU-bit (summertime) used

Command transmission

(Object-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☒ Direct command transmission
- ☐ Direct set point command transmission
- ☒ Select and execute command

Table continues on the next page

- ☐ Select and execute set point command
- ☒ C_SE ACTTERM used
- ☒ No additional definition
- ☒ Short-pulse duration (duration determined by a system parameter in the outstation)
- ☒ Long-pulse duration (duration determined by a system parameter in the outstation)
- ☒ Persistent output

Transmission of integrated totals

(Station- or object-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☒ Mode A: Local freeze with spontaneous transmission
- ☐ Mode B: Local freeze with counter interrogation
- ☒ Mode C: Freeze and transmit by counter-interrogation commands
- ☒ Mode D: Freeze by counter-interrogation command, frozen values reported
- ☒ Counter read
- ☒ Counter freeze without reset
- ☒ Counter reset
- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Parameter loading

(Object-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☐ Threshold value
- ☐ Smoothing factor

Table continues on the next page

- ☐ Low limit for transmission of measured values
- ☐ High limit for transmission of measured values

Parameter activation

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☐ Act/deact of persistent cyclic or periodic transmission of the addressed object

Test procedure

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☐ Test procedure

File transfer

(Station-specific parameter, mark with an “X” if the function is used.)

File transfer in monitor direction

- ☐ Transparent file
- ☐ Transmission of disturbance data of protection equipment
- ☐ Transmission of sequences of events
- ☐ Transmission of sequences of recorded analogue values

File transfer in control direction

- ☐ Transparent file

Background scan

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☐ Background scan

Acquisition of transmission delay

(Station-specific parameter, mark with an “X” if the function is only used in the standard direction, “R” if only used in the reverse direction, and “B” if used in both directions.)

- ☒ Acquisition of transmission delay

5 Secure authentication conformance statement

5.1 Overview of clause

Implementers of this specification shall supply the information in this section on request. An “X” in a box means that the implementation supports the listed feature.

5.2 Required algorithms

If the implementer does not declare support for an algorithm marked “(required)”, interoperability cannot be guaranteed.

If an algorithm is not supported due to export restrictions, the implementer shall provide a copy of the export restriction that prohibits its export. This algorithm shall not be supported if and only if export restrictions do not allow any mechanism of exportation. If this algorithm is not supported, the implementation shall be clearly documented as adhering to the export restrictions, as supplied. The documentation shall also specify that the interoperable/base specification requirements are not supported. Samples of the documentation shall be provided.

5.3 MAC algorithms

- ☒ HMAC-SHA256
- ☐ Other _____
- ☐ Mandatory algorithm could not be provided. Reason: _____

5.4 Key wrap algorithms

- ☒ AES-256 Key Wrap (required)
- ☐ Other _____
- ☐ Mandatory algorithm could not be provided. Reason: _____

5.5 Use of error messages

☒ Transmits error messages

5.6 Update key change methods

☐ None permitted

☒ <4> Symmetric AES-256 /
HMACSHA- 256 (required)

☐ <5> Symmetric AES-256 / AESG-
MAC

☐ <68> Asymmetric RSA-2048 /
DSA SHA-256 (L=2048 N=256) /
HMAC-SHA-256

☐ <69> Asymmetric RSA-3072 /
DSA SHA-256 (L=3072 N=256) /
AES-SHA-256

☐ <70> Asymmetric RSA-2048 /
DSA SHA-256 (L=2048 N=256) /
HMAC-GMAC

☐ <71> Asymmetric RSA-3072 /
DSA SHA-256 (L=3072 N=256) /
AES-GMAC

☐ Other _____

☐ Mandatory algorithm could not
be provided.

Reason: _____

5.7 User status change

☒ Non-certificate method (required)

☐ Use IEC/TS 62351-8 Certificates

5.8 Configurable parameters

Parameter	Parameter Configured at station	Value
Reply Timeout (sec)	Both	2
Maximum Error Messages Sent	Both	
Session Key Change Interval (sec)	Controlling	
Session Key Change Count	Controlling	
Expected Session Key Change Interval (sec)	Controlled	1800
Expected Session Key Change Count	Controlled	4000
Maximum Session Key Status Count	Controlled	5
Update Key Change Method	Both	See Chapter 5.6 Update key change methods
Authentication Challenge Data Length	Both	4 octets
Key Status Challenge Data Length	Controlled	4 octets
Controlling Station Challenge Data Length	Controlled	
Controlled Station Challenge Data Length	Controlled	4 octets
Maximum Certificate Size	Both	-
Maximum Number of Users	Both	1
Update Key(s) ¹	Both, if Update Key Change Method is "None permitted".	Configuration Tool
User Number(s)	Both, if Update Key Change Method is "None permitted".	1
User Name(s)	Controlling station or at the Authority, if Update Key change is permitted.	Common
Outstation Name (s)	Both, if Update Key change is permitted.	Configuration Tool
Authority Public Key ¹ or Authority Certification Key ¹	Both, if Update Key change is permitted.	-
User Public Key(s) ¹	Controlling station or at the Authority	-
Outstation Public Key ¹	Controlling	-

¹ It is permitted to provide information about how to read or change the configured keys rather than entering the actual values of the keys in the PICS.

5.9 Configurable statistic thresholds and statistic information object addresses

Name	Default value of statistic	Configured value of statistic threshold	Information object address of the integrated total for the statistic
Unexpected Messages	3	3 (Configurable)	Configurable
Authorization Failures	5	5 (Configurable)	Configurable
Authentication Failures	5	5 (Configurable)	Configurable
Reply Timeouts	3	3 (configurable)	Configurable
Rekeys Due to Authentication Failure	3	3 (configurable)	Configurable
Total Messages Sent	100	100 (Configurable)	Configurable
Total Messages Received	100	100 (Configurable)	Configurable
Critical Messages Sent	100	-	Configurable
Critical Messages Received	100	100 (Configurable)	Configurable
Discarded Messages	10	10 (Configurable)	Configurable
Error Messages Sent	10	10 (Configurable)	Configurable
Error Messages Rxed	10	10 (Configurable)	Configurable
Successful Authentications	100	100 (Configurable)	Configurable
Session Key Changes	10	10 (Configurable)	Configurable
Failed Session Key Changes	5	5 (Configurable)	Configurable
Update Key Changes	1	1 (Configurable)	Configurable
Failed Update Key Changes	1	1 (Configurable)	Configurable
Rekeys Due to Restarts	3	-	Configurable

5.10 Critical functions

This table shows which functions are considered critical by the device as it is presently configured. An “M” in the “M/O” column means it is mandatory to consider this Type to be critical. An “O” means it is optional. A “-” in the “Configured as Critical” column means the type is not supported.

Table 17: Critical functions

Type identification		Description	IEC 60870-5-101	IEC 60870-5-104	M/O	Configured as critical (Y/N/-)
<1>	M_SP_NA_1	Single-point information without time tag	Yes	Yes	O	N
<2>	M_SP_TA_1	Single-point information with time tag	Yes	No	O	-
<3>	M_DP_NA_1	Double-point information without time tag	Yes	Yes	O	N
<4>	M_DP_TA_1	Double-point information with time tag	Yes	No	O	-
<5>	M_ST_NA_1	Step position information	Yes	Yes	O	-
<6>	M_ST_TA_1	Step position information with time tag	Yes	No	O	-
<7>	M_BO_NA_1	Bitstring of 32 bits	Yes	Yes	O	-

Table continues on the next page

Type identification		Description	IEC 60870-5-101	IEC 60870-5-104	M/O	Configured as critical (Y/N/-)
<8>	M_BO_TA_1	Bitstring of 32 bits with time tag	Yes	No	O	-
<9>	M_ME_NA_1	Measured value, normalized value	Yes	Yes	O	N
<10>	M_ME_TA_1	Measured value, normalized value with time tag	Yes	No	O	-
<11>	M_ME_NB_1	Measured value, scaled value	Yes	Yes	O	N
<12>	M_ME_TB_1	Measured value, scaled value with time tag	Yes	No	O	-
<13>	M_ME_NC_1	Measured value, short floating point number	Yes	Yes	O	N
<14>	M_ME_TC_1	Measured value, short floating point number with time tag	Yes	No	O	-
<15>	M_IT_NA_1	Integrated totals	Yes	Yes	O	N
<16>	M_IT_TA_1	Integrated totals with time tag	Yes	No	O	N
<17>	M_EP_TA_1	Event of protection equipment with time tag	Yes	No	O	-
<18>	M_EP_TB_1	Packed start events of protection equipment with time tag	Yes	No	O	-
<19>	M_EP_TC_1	Packed output circuit information of protection equipment with time tag	Yes	No	O	-
<20>	M_PS_NA_1	Packed single-point information with status	Yes	Yes	O	-
<21>	M_ME_ND_1	Measured value, normalized value without quality	Yes	Yes	O	N
<30>	M_SP_TB_1	Single-point information with time tag CP56Time2a	Yes	Yes	O	N
<31>	M_DP_TB_1	Double-point information with time tag CP56Time2a	Yes	Yes	O	N
<32>	M_ST_TB_1	Step position information with time tag CP56Time2a	Yes	Yes	O	-
<33>	M_BO_TB_1	Bitstring of 32 bits with time tag CP56Time2a	Yes	Yes	O	-
<34>	M_ME_TD_1	Measured value, normalized value with time tag	Yes	Yes	O	N
<35>	M_ME_TE_1	Measured value, scaled value with time tag	Yes	Yes	O	N
<36>	M_ME_TF_1	Measured value, short floating point number with time tag	Yes	Yes	O	N
<37>	M_IT_TB_1	Integrated totals with time tag CP56Time2a	Yes	Yes	O	N
<38>	M_EP_TD_1	Event of protection equipment with time tag CP56Time2a	Yes	Yes	O	-
<39>	M_EP_TE_1	Packed start events of protection equipment with time tag CP56Time2a	Yes	Yes	O	-
<40>	M_EP_TF_1	Packed output circuit information of protection equipment with time tag CP56Time2a	Yes	Yes	O	-
<45>	C_SC_NA_1	Single command	Yes	Yes	M	Y
<46>	C_DC_NA_1	Double command	Yes	Yes	M	Y
<47>	C_RC_NA_1	Regulating step command	Yes	Yes	M	-
<48>	C_SE_NA_1	Set-point command, normalized value	Yes	Yes	M	-
<49>	C_SE_NB_1	Set-point command, scaled value	Yes	Yes	M	-
<50>	C_SE_NC_1	Set-point command, short floating-point number	Yes	Yes	M	-
<51>	C_BO_NA_1	Bitstring of 32-bit	Yes	Yes	M	-
<58>	C_SC_TA_1	Single command with time tag CP56Time2a	No	Yes	M	Y

Table continues on the next page

Type identification		Description	IEC 60870-5-101	IEC 60870-5-104	M/O	Configured as critical (Y/N/-)
<59>	C_DC_TA_1	Double command with time tag CP56Time2a	No	Yes	M	Y
<60>	C_RC_TA_1	Regulating step command with time tag CP56Time2a	No	Yes	M	-
<61>	C_SE_TA_1	Set point command, normalized value with time tag CP56Time2a	No	Yes	M	-
<62>	C_SE_TB_1	Set point command, scaled value with time tag CP56Time2a	No	Yes	M	-
<63>	C_SE_TC_1	Set point command, short floating-point number with time tag CP56Time2a	No	Yes	M	-
<64>	C_BO_TA_1	Bitstring of 32 bits with time tag CP56Time2a	No	Yes	M	-
<70>	M_EI_NA_1	End of initialization	Yes	Yes	O	-
<100>	C_IC_NA_1	Interrogation command	Yes	Yes	O	N
<101>	C_CI_NA_1	Counter interrogation command	Yes	Yes	O	N
<102>	C_RD_NA_1	Read command	Yes	Yes	O	-
<103>	C_CS_NA_1	Clock synchronization command	Yes	Yes	M	Y
<104>	C_TS_NA_1	Test command	Yes	No	O	-
<105>	C_RP_NA_1	Reset process command	Yes	Yes	M	-
<106>	C_CD_NA_1	Delay acquisition command	Yes	No	O	N
<107>	C_TS_TA_1	Test command with time tag CP56Time2a	No	Yes	M	-
<110>	P_ME_NA_1	Parameter of measured value, normalized value	Yes	Yes	M	-
<111>	P_ME_NB_1	Parameter of measured value, scaled value	Yes	Yes	M	-
<112>	P_ME_NC_1	Parameter of measured value, short floating- point number	Yes	Yes	M	-
<113>	P_AC_NA_1	Parameter activation	Yes	Yes	M	-
<120>	F_FR_NA_1	File ready	Yes	Yes	M	-
<121>	F_SR_NA_1	Section ready	Yes	Yes	M	-
<122>	F_SC_NA_1	Call directory, select file, call file, call section	Yes	Yes	M	-
<123>	F_LS_NA_1	Last section, last segment	Yes	Yes	M	-
<124>	F_AF_NA_1	Ack file, ack section	Yes	Yes	M	-
<125>	F_SG_NA_1	Segment	Yes	Yes	M	-
<126>	F_DR_TA_1	Directory	Yes	Yes	M	-

6 IEC 60870-5-104 parameters

6.1 IEC 101-104 General settings

Table 18: Non group settings

Parameter	Values (Range)	Unit	Step	Default	Description
Operation	1=on 5=off			5=off	Selects if this protocol instance is enabled or disabled
Port	3=IEC104 - Ethernet			3=IEC104 - Ethernet	Port selection
Mapping select	1...2		1	1	Mapping select
ClientIP				0.0.0.0	IP address of the client
TCP Port	0...65535		1	2404	Server TCP port
Device Address	1...65535		1	1	Device address
ASDU Address	1...65535		1	1	Common address of ASDU
Link Mode	0=Balanced 1=Unbalanced			0=Balanced	Link mode setting
COT Length	1...2		1	1	Cause of transmission length
IOA Length	1...3		1	2	Information Object Address length
Link Address Length	1...2		1	1	Link Address Length
ASDU Address Length	1...2		1	1	ASDU Address Length
Single Char Resp	0=False 1=True			0=False	Single character response enabled/disabled
Show Bad Time	0=False 1=True			1=True	Enable/disable bad time quality indication in events
Time Format	1=Full 56bit			1=Full 56bit	Time stamp format 3 or 7 octet
Time Zone	0=Local 1=UTC			1=UTC	Selects between UTC/Local time
Overflow Mode	0=Oldest+indication 1=Keep newest			0=Oldest+indication	Event buffer overflow handling mechanism
OvInd IOA	0...16777215		1	60000	Overflow indication address for interrogated data
OvInd NoGI IOA	0...16777215		1	60000	Overflow indication address for non-interrogated data
Selection Timeout	1...65	s	1	30	Selection timeout for control SBO operations

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
Counter Reporting	0=Read by master 1=Spontaneous			0=Read by master	Counter reporting after freeze
Freeze mode	0=Not in use 1=Freeze only 2=Freeze and Reset			0=Not in use	Freezing mode for externally triggered integrated totals
TX window (k)	1...20		1	12	IEC60870-5-104 transmit window (k)
RX window (w)	1...20		1	8	IEC60870-5-104 receive window (w)
TX timeout (t1)	1...2147483647	ms	1	30000	IEC60870-5-104 transmit timeout (t1)
RX timeout (t2)	1...2147483647	ms	1	10000	IEC60870-5-104 receive timeout (t2)
Test interval (t3)	0...2147483647	ms	1	20000	IEC60870-5-104 link test interval (t3) - 0: Disables the transmission of test frames
Cyclical Period	1...604800	s	1	10	Cyclical period in seconds
IT_FRZ	0=False 1=True			0=False	Control point for freezing integrated totals
Command delay	0...65535	ms	1	5000	Maximum delay for timestamped commands in milliseconds.
Prtl Customization	0...2147483647		1	0	Customization parameter. Please, refer to the protocol manual.

6.2 Secure communication parameters

The IEC 60870-5-104 secure communication parameters can be accessed with PCM600 or via the HMI paths **Configuration > Communication > Protocols > Secure IEC104(1) > General and Configuration > Communication > Protocols > Secure IEC104(1) > Statistics Thresholds**.

6.2.1 IEC 101-104 Secure settings

Table 19: Non group settings

Parameter	Values (Range)	Unit	Step	Default	Description
Protocol Security Mode	1=App. authentication 2=TLS and appl. auth. 0=Off			0=Off	Protocol Security Mode - 0: Off; 1: Application authentication; 2: TLS and Application authentication
Reply timeout	100...120000	ms	1	2000	Reply timeout
Exp Sesn key Chg Intv	0...14400	s	1	1800	Expected Session key change interval - Value zero will in-

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
					icate that interval is not used
Exp Sesn key Chg Cnt	2...10000000		1	4000	Expected session key change count
Max Sesn key Stat Cnt	1...255		1	5	Maximum session key status count
Sec Stat Cnt Grp	1=Group 1 2=Group 2 3=Group 3 4=Group 4			4=Group 4	Secure statistics counter group
Sec Stat Cnt IOA	1...65535		1	61000	Information object address for secure statistics counters

6.2.2 IEC 101-104 Secure statistics thresholds settings

Table 20: Non group settings

Parameter	Values (Range)	Unit	Step	Default	Description
Unexpected Msgs	1...65535		1	3	Security statistics threshold for unexpected messages
Auth failures	1...65535		1	5	Security statistics threshold for authorization failures
Authn failures	1...65535		1	5	Security statistics threshold for authentication failures
Reply timeouts	1...65535		1	3	Security statistics threshold for reply timeouts
Rekeys Authn failure	1...65535		1	3	Security statistics threshold for re-keys due to authentication failure
Total Msgs Tx	1...65535		1	100	Security statistics threshold for total messages sent
Total Msgs Rx	1...65535		1	100	Security statistics threshold for total messages received
Total Crit Msgs Rx	1...65535		1	100	Security statistics threshold for total critical messages received
Discarded Msgs	1...65535		1	10	Security statistics threshold discarded messages
Error Msgs Tx	1...65535		1	10	Security statistics threshold error messages sent
Error Msgs Rx	1...65535		1	10	Security statistics threshold error messages received
Successful Authn	1...65535		1	100	Security statistics threshold for successful authentications
Sesn key Chg	1...65535		1	10	Security statistics threshold for session key changes

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
Failed Sesn key Chgs	1...65535		1	5	Security statistics threshold for failed session key changes
Upd key Chgs	1...65535		1	1	Security statistics threshold for update key changes
Failed Upd key Chgs	1...65535		1	1	Security statistics threshold for failed update key changes

6.3 IEC 101-104 Monitored data

Table 21: Monitored data

Name	Type	Values (Range)	Unit	Description
Customization Mode	Enum	0=Off/Normal 1=By Parameter 2=By File		Protocol Customization Mode
Reset counters	BOOLEAN	0=False 1=True		Reset counters
Received frames	INT32	-1...2147483646		Received frames
Transmitted frames	INT32	-1...2147483646		Transmitted frames
Physical errors	INT32	-1...2147483646		Physical layer errors
Link errors	INT32	-1...2147483646		Link layer errors
Transport errors	INT32	-1...2147483646		Transport layer errors
CnReject no sockets	INT32	-1...2147483646		Number of rejected connections due to no sockets available
CnReject unregistered	INT32	-1...2147483646		Connection rejected due to unregistered client

6.4 Monitored data for secure communication

The IEC 60870-5-104 monitored data for secure communication can be accessed via the HMI path **Monitoring > Communication > Protocols > Secure IEC104(1)**.

6.4.1 IEC 101-104 Secure monitored data

Table 22: Monitored data

Name	Type	Values (Range)	Unit	Description
Unexp Msgs Cnt	INT32	0...2147483646		Security statistics counter for unexpected messages
Auth Fail Cnt	INT32	0...2147483646		Security statistics counter for authorization failures

Table continues on the next page

Name	Type	Values (Range)	Unit	Description
Authn Fail Cnt	INT32	0...2147483646		Security statistics counter for authentication failures
Reply timeouts Cnt	INT32	0...2147483646		Security statistics counter for reply timeouts
Rekey Authn Fail Cnt	INT32	0...2147483646		Security statistics counter for rekeys due to authentication failure
Total Msgs Tx	INT32	0...2147483646		Security statistics counter for total messages sent
Total Msgs Rx	INT32	0...2147483646		Security statistics counter for total messages received
Critical Msgs Rx Cnt	INT32	0...2147483646		Security statistics counter for critical messages received
Discarded Msgs Cnt	INT32	0...2147483646		Security statistics counter for discarded messages
Err Msgs Tx Cnt	INT32	0...2147483646		Security statistics counter error messages sent
Err Msgs Rx Cnt	INT32	0...2147483646		Security statistics counter error messages received
Successful Authn Cnt	INT32	0...2147483646		Security statistics counter for successful authentications
Session Key Chg Cnt	INT32	0...2147483646		Security statistics counter for session key changes
Fail Ses Key Chg Cnt	INT32	0...2147483646		Security statistics counter for failed session key changes
Upd Key Chgs Cnt	INT32	0...2147483646		Security statistics counter update key changes
Fail Upd Key Chgs Cnt	INT32	0...2147483646		Security statistics counter for failed update key changes

7 Glossary

APDU	Application protocol data unit
ASDU	Application-layer service data unit
CA	Certification authority
COT	Cause of transmission
Data object	Also known as DO. Part of a logical node object representing specific information, for example status or measurement. From an object-oriented point of view, a data object is an instance of a class data object. DOs are normally used as transaction objects; that is, they are data structures.
Data set	The content basis for reporting and logging containing references to the data and data attribute values
DPC	Double-point control
EMC	Electromagnetic compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
GI	General interrogation
HMI	Human-machine interface
IEC	International electrotechnical commission
IEC 60870-5	IEC standard for telecontrol equipment and systems. Part 5 defines transmission protocols.
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 60870-5-4	
IEC 61850	International standard for substation communication and modeling
MAC	Media access control
PCM600	Protection and control IED manager
SBO	Select-before-operate
SI	Sensor input
SPC	Single-point status of a controllable object
TCP	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TLS	Transport layer security
UTC	Coordinated universal time



ABB Distribution Solutions
Digital Substation Products

P.O. Box 699

FI-65101 VAASA, Finland

Phone +358 10 22 11

abb.com/mediumvoltage

abb.com/reliion

go.abb/digitalsubstations