RELION® PROTECTION AND CONTROL

REX640

DNP3 Communication Protocol Manual

Document ID: 1MRS759119
Issued: 2023-02-03
Revision: D

Copyright

Trademarks

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 anti virus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

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

In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

Conformity

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

Contents

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

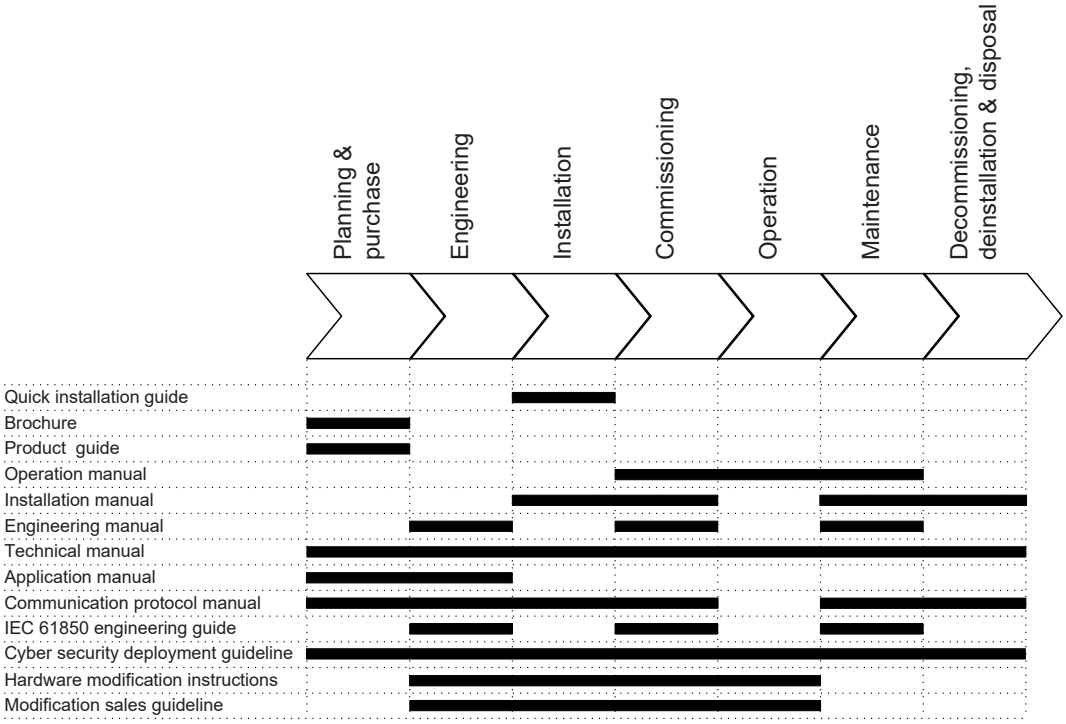

Figure 1: The intended use of documents during the product life cycle

1.3.2 Document revision history

Document revision/date	Product connectivity level	History
A/2018-12-14	PCL1	First release
B/2020-02-13	PCL2	Content updated to correspond to the product connectivity level
C/2020-12-10	PCL3	Content updated to correspond to the product connectivity level
D/2023-02-03	PCL4	Content updated to correspond to the product connectivity level

1.3.3 Related documentation

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

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 DNP3 overview

2.1 DNP3 standard

The DNP3 protocol was developed by Westronic based on the early versions of the IEC 60870-5 standard telecontrol protocol specifications. Now the protocol specification is controlled by the DNP3 Users Group at *http://www.dnp.org*.

The ISO/OSI based model supported by this protocol specifies physical, data link and application layers only. This reduced protocol stack is referred to as EPA. However, to support advanced RTU functions and messages larger than the maximum frame length as defined by the IEC document 60870-5-1, the DNP3 data link is intended to be used with a transport pseudo-layer. As a minimum, this transport layer implements message assembly and disassembly services.

3 Vendor-specific implementation

3.1 Protocol server instances

The word "client" refers to the protocol master. The protection relay is referred to as "server" or a slave device.

The protection relay can communicate with several protocol clients simultaneously. Furthermore, it is possible to configure the protection relay to provide different protocol data and data outlook for different clients. A protocol server communication entity which is configured to operate with a specific master or client is called an instance.

There are three server instance scenarios.

1. One client - One protocol instance - One protocol mapping. The protection relay is intended to operate toward one protocol client. The default protocol data mapping or data outlook can be modified freely.
2. Several clients - Several protocol instances - One protocol mapping. The protection relay is intended to operate toward several protocol clients. All the clients are able to access the same data or similar data outlook. The default protocol mapping or data outlook can be modified freely.
3. Several clients - Several protocol instances - Several protocol mappings. The protection relay is intended to operate toward several protocol clients. Some or all of the clients may access protocol data in a different manner, so several protocol mappings derived from the default protocol mapping need to be prepared.

3.1.1 Connection to clients

In the relay it is possible to activate up to five protocol server instances, each represented by a separate function block in the relay configuration. The five blocks are named DNPLPRT1...5. For each connected client, a protocol instance has to be activated by dragging the function block into the relay configuration. When the function block is active, its setting and monitoring parameters are visible in the HMI. An exception is protocol instance 1, which is always visible in the HMI, and which can be activated without dragging its function block instance into the relay configuration.

Figure 2: Function block

The protection relay restricts communication clients to five, regardless of the protocols to which the clients belong. This includes the MMS clients and other communication protocol clients. The available five DNP3 instances may be freely

activated. However, it is recommended to activate the instances in chronological order. For example, instance 1 is to be used if there is only one client connection and instances 1 and 2 when there are two clients.

First setup and configuration upload

Dragging the protocol instance function block into the relay configuration is only the first step of the protocol activation. When a protocol instance is added for the first time, it is inactive by default, meaning that it has not been assigned to a physical link port. Neither has any DNP3 data point configuration been loaded for the instance. Next step is to do these setups.

Each time the protocol instance setting parameter *InUse* is changed between "Off" and "On", a relay restart is needed. A configuration upload write from PCM600 is not sufficient in this case.

3.1.2 Protocol server attachment to a client

After its activation, an instance should be attached to the intended client.

If the client is in a serial connection, the instance must be attached to the intended serial port.

In case of a TCP client, the instance must be first attached to the physical Ethernet port. If there are several TCP client connections, the protection relay must be able to distinguish between the clients. There are two setting parameters in an instance.

- *Client IP*: When the client makes the TCP connection, its IP address is checked. This instance is given to the client with this IP address. It is also possible to use the address “0.0.0.0” if no client IP address is to be defined. In this case, the client's IP address is ignored.
- *TCP port*: This parameter can be used in conjunction with the *Client IP* setting, thus allowing only a certain IP address at a specific TCP socket port number.

3.1.3 Several identical client connections

If several clients access the same protocol data, the client connections must still be kept apart. Also the number of each instance used for each client must be noted so that if there are problems with the communication, the line diagnostic data for instances follows the same instance number rule.

In case of a sequential event data transaction and a TCP client connection, it is essential that a reconnecting client is given back the same instance to which it was attached before disconnecting. This way, the event reading resumes from the point where the client left off, provided that no event overflow has occurred while the client was absent. If multiple client connections are used, they must be distinguished by using the *Client IP* and *TCP port* parameters.

3.1.4 Protocol data mapping to server instances

There are two different types of data mappings for the protocol. The mappings are identified and numbered, starting from one. This number is not related to the protocol instance number.

In PCM600, it is necessary to always define the mappings to be edited or viewed.

Each protocol instance has the setting parameter *Mapping select*, which defines the protocol mappings to be used by this instance. Several protocol instances can use the same mapping. By default, the *Mapping select* parameter for all the instances is set to use the mapping number one.

Reboot the protection relay after changing the mapping number.

3.2 Link modes

DNP3 can be configured to operate in serial or Ethernet mode. The operation mode is configured with the *Port* parameter.

3.2.1 Serial link mode

DNP3 serial can be assigned to a serial communication port in the protection relay. Serial communication ports are named COM1...COMn, depending on how many serial ports the protection relay hosts.

The DNP3 protocol ignores any parity setting in the COM settings group. DNP3 is defined as an 8-bit/no parity protocol with a 16-bit CRC every 16 bytes. These characteristics are automatically configured by the protection relay's software when a serial port is taken into use by DNP3. However, some characteristics of the serial port must be set: baud rate, serial mode (RS-485 2/4-wire) and fiber mode. They are located in the serial port settings.

- **Configuration** > **Communication** > **COMn** > **Fiber mode**
- For the RS-485 link, the biasing and bus terminations are selected from the DIP switch located on the communication card.
- **Configuration** > **Communication** > **COMn** > **Baud rate**

For the serial port parameter settings and hardware setup, see the technical manual.

The COM port connection type, optical ST or EIA-485 connection, star or loop topology and the idle state (light on or light off) are selected using the parameter settings in **Configuration** > **Communication** > **COMn**. The bias and bus termination are settable via the COM card hardware's DIP switch. See the technical manual for further details.

3.2.2 TCP/IP mode

The DNP3 TCP/IP link mode is supported by the protection relay.

The protection relay listens for a connection from a DNP3 client on the port specified by the user. The default values for the TCP port number range from 20000...20004 depending on the instance number. A different port can be selected with the *TCP Port* parameter.

3.2.3 UDP modes

A specification of the UDP implementation is found in the DNP3 standard, part7, IP-networking. The relay's implementation supports the UDP communication alternatives described by the standard.

DNP3 protocol supports UDP mode communication also. UDP mode can be activated by the *Port* -parameter setting. Two UDP modes are supported, "Ethernet TCP+UDP" and "Ethernet UDP".

"Ethernet TCP+UDP" mode can be used in TCP mode with additional possibility to accept UDP broadcast messages. The relay does not send any UDP responses. In TCP+UDP mode an active TPC client connection is required to accept UDP broadcast messages from that client. UDP broadcast messages should have DNP3 broadcast address from 0xfffd to 0xffff, to reach multiple relays with the same broadcast command. The relay accepts UDP broadcast messages from the port defined by the *UDP Rx Port* -parameter.

"Ethernet UDP" mode is meant for UDP only communication, meaning relay only accepts UDP datagrams and responds using UDP datagrams. In this mode the relay accepts UDP request in port defined by the *UDP Rx Port* parameter, and sends responses to the learned client IP address to port defined by *UDP Tx Port* parameter. If the *UDP Tx Port* parameter is set to zero (0), the relay learns the response port from the last UDP datagram received from the UDP client (source port of the sender). The *UDP Tx Port Ini* parameter defines the port the relay sends Initial Unsolicited Response to, in case client port is yet unknown. This parameter is relevant only if relay is configured to Unsolicited Mode via the *UR mode* parameter and configured to send initial Unsolicited message via the *Legacy Master UR* parameter setting.

Client holdover in UDP only mode

In *Ethernet UDP* mode, the relay memorizes the UDP client IP address from the first UDP frame received. Connections from other clients can be denied if desired during a keep-alive period. If the *Link keep-alive* setting is non-zero, the relay denies any UDP request from other sources than the recently learned client IP address during period of ("Link keep-alive" + ("Data link retries" * "Data link confirm TO")) seconds.

If this period passes without out any UDP requests from the memorized UDP client IP address, then another UDP client IP address could be accepted. If the *Link keep-alive* setting is zero, the relay does not lock the client IP address, but allows UDP requests from any IP address. In addition, the *Client IP* parameter setting can be used in UDP only -mode also, to lock the relay to only accept requests from one specific pre-defined IP address.

More information on TCP/UDP communication modes can be found in *www.dnp.org*.

3.3 Communication setup

3.3.1 Communication modes

DNP3 communication can be set up in two alternative modes.

- Polled mode, also called “polled report by exception”. In this mode the DNP3 client always initiates the transaction with a read or write request to the DNP3 server. The server must reply with a response message.
- Unsolicited mode, called also “Unsolicited reporting mode”. In this mode the DNP3 server may spontaneously send changed class events to the client. The client can make additional read or write requests to the server.

By default, DNP3 operates in polled mode. Unsolicited reporting mode can be activated with the *UR mode* parameter.

3.3.2 DNP3 layer acknowledgements, retries and timeouts

It is possible to set up acknowledgements on both DNP3 link layer and application layer. The settings should be equal on both the client and the server sides of the communication. The timeouts must be set so that the other side has enough time to prepare a positive acknowledgement. If an acknowledgement is received after the configured timeout, it is discarded.

Confirmations, retries and timeouts can be configured via parameters.

- **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)** > **Data link confirm**
- **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)** > **Data link confirm TO**
- **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)** > **Data link retries**
- **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)** > **App layer confirm**
- **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)** > **App confirm TO**

DNP3 link layer acknowledgements should not be used in TCP/IP link mode, since the DNP3 message transport (link) is then encapsulated and secured by the Ethernet protocol.

Link layer acknowledgements are seldom used in serial mode. The application layer acknowledgements also cover the link layer acknowledgements. This means that if the application message was successfully delivered, then the link layer must also have been successful. Furthermore, it is easier to perform a whole application layer retransmission rather than link layer retransmissions. Otherwise the application layer timeout must be prepared to cover all the timeouts and retransmissions performed by the link layer.

3.3.3 Polled mode

In the polled mode the client station initiates a connection and polls periodically for static data (Class 0), and events (Class 1/2/3) from the server. Data must be polled frequently enough to prevent event overflow. If event overflow takes place, this is indicated in the IIN bits in the response message. This means that events have been lost.

3.3.4 Unsolicited reporting mode

The unsolicited mode can be enabled in the relay by the *UR mode* parameter. The operating principle is that the server sends event data spontaneously to the client. When the unsolicited mode has been activated by the setting parameter, the client station must activate UR reporting by *Enable unsolicited* Application function (20). After activation the server begins sending Class 1/2/3 events spontaneously.

The client must acknowledge the unsolicited events reported by the server to ensure the communication is fully operative. If the server does not receive acknowledgement in time, defined by the *UR TO* and *App confirm TO* parameters, it does a count of resends defined by the parameter *UR retries*. If the client station does not send acknowledgement during the count of retries, the server goes to offline mode. This means that spontaneous events are not sent for a period of time. The length of this period is defined by the parameter *UR offline interval*, (default 15 minutes). If the server should not go to offline mode, limitless retries can be achieved by setting the *UR retries* to “65535”.

Class event reporting can be buffered in the unsolicited mode by setting the Class buffer [x=1...3] dependent parameters *UR Class x Min event* and *UR Class x TO*. The event parameter UR Class x Min defines how many events must be buffered in the device before unsolicited report is sent out. The UR Class x TO parameter defines the minimum waiting time the device buffers events before sending them out after an event occurs. These parameters are useful for controlling the flow of events from the device and combining them into bigger reports.

Legacy master UR provides compatibility to some older DNP3 clients. When disabled, the server follows the DNP3 standard, sending its first unsolicited message after a connection has been established following relay reboot. The client is expected to send the Enable/Disable Unsolicited messages command to the relay. When *Legacy master UR* is enabled, the relay does not send the initial unsolicited message. Unsolicited responses are sent without the need of the Enable Unsolicited command. The client still needs to open a connection for the server to start sending unsolicited messages.

Unsolicited reporting mode is not recommended in half-duplex (RS-485 2-wire mode or optical ST mode) serial bus due to possibility of collisions in the serial bus. Especially in a system where event reporting is frequent, collisions can cause failed DNP3 requests/responses and thus retransmissions. If unsolicited mode is used, application level confirmations should be enabled to ensure that transmission is successful. In half-duplex serial bus, polled mode is recommended.

3.3.5 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^(bit number).

3.3.5.1

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

Table 1: DNP3 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 Keep-Alive interval time expires after the set number of retries is reached
					2 - 30	4 - 1073741824	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** > **DNP3.0 (n)**.

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

3.3.6 Description of UDP mode

3.3.6.1 UDP port setting parameters

Three setting parameters are defined for the UDP socket port definitions. The settings additionally defines how in practice receive and transmit will be handled over UDP. (Since value 0 in some cases means that the port is not in use at all.)

UDP Rx Port

This is the UDP port on which the DNP3 slave instance expects UDP DNP3 client datagrams to arrive. This port must always exist. The possible setting range of this parameter is 1 … 65535.

UDP Tx Port

This is the UDP port on which the DNP3 slave instance could send its responses to the client. However, an option exists between using this port or the return (source) port of the **UDP Rx Port** messages for the responses. Therefore is the setting range of this parameter 0…65535. Possibilities are then:

0 =	This port is ***not used***. Responses are routed back to the DNP3 client's local (listening) port, which is learned from UDP datagrams received from the client through *UDP Rx Port*. This (listening) return port is memorized and "refreshed" after each UDP datagram received from the client.
1…65535 =	This port is used as destination port for the response messages.

UDP Tx Port Ini

This is the UDP port on which the DNP3 slave would send out its initial unsolicited message according to the DNP3 standard description. This setting is only relevant if the DNP3 instance is configured for unsolicited reporting (*UR Mode* = Enabled). The setting range for this parameter is also 0…65535, meaning that an option (0) to ***not use this port*** is also possible. See this description later.

3.3.6.2 DNP3 client-slave communication alternatives (when unsolicited reporting is not enabled)

In the cases below we assume setting *UR Mode* =Disabled.

One predefined DNP3 client:

The DNP3 slave instance could be predefined to only accept UDP datagrams from a specific DNP3 client. If the instance setting *Client IP* is set to a valid IP address, then only UDP datagrams arriving on *UDP Rx Port* from this source IP address are accepted.

One random DNP3 client:

Alternatively could the DNP3 slave instance have the *Client IP* address set to 0.0.0.0, meaning "not defined". Furthermore *Link keep-alive* is set to 0 (not in use). In this case will the instance not check the client's source IP address in UDP datagrams arriving on the *UDP Rx Port* . All messages are accepted and responded to.

Switching between several random DNP3 clients:

Client IP address is set to 0.0.0.0 and additionally the DNP3 link keep-alive operation is taken in use. This is done via the setting parameter *Link keep-alive* , with a value > 0. Now the client IP address of the first client request on *UDP Port Rx* is memorized and accepted. After this only requests from this client IP address will be accepted.

Later:

If the once accepted DNP3 client disappears from the physical link, then a link keep-alive timeout will eventually occur in the slave. When this happens the DNP3 slave will forget the memorized client IP address. Another DNP3 client (or also the same client as before) could thereafter be accepted through *UDP Rx Port* .

3.3.6.3 DNP3 client-slave communication alternatives (when unsolicited reporting is enabled)

If setting *UR Mode* =Enabled, then there are two communication options:

- Either the instance is predefined to operate towards one specific DNP3 client IP address.
- or the instance has no client IP address predefinition, and instead "learns" (memorizes) the client IP address based on the first message arriving from the client. DNP3 link keep-alive must be in used in this case, and a switchover to another client will only be possible after a link keep-alive timeout happens.

One predefined DNP3 client:

The *UDP Tx Port Ini* setting could now be taken in use. After restart will the DNP3 slave instance start sending initial unsolicited responses through the *UDP Tx Port Ini* to the predefined *Client IP* -address DNP3 client. Observe that the *UDP Tx Port Ini* setting could be equal to *UDP Tx Port* . Meaning that these ports would then be one and the same.

Intention is then that the DNP3 client will respond to this message through *UDP Rx Port* . The *UDP Tx Port Ini* is thereafter not used anymore. Communication will resume as defined in 3.2.

Alternative:

If the *UDP Tx Port Ini* is set to 0, then the DNP3 instance will not send any initial unsolicited responses at restart. Instead it will wait for the client to make the first request through *UDP Rx Port* , which then should be to enable the UR class reporting.

Switching between several random DNP3 clients:

The *UDP Tx Port Ini* could be taken in use (1...65535) or not (0).

If it is taken in use, the DNP3 slave has initially no knowledge of the client's IP address. **[1]** The initial unsolicited responses are sent out on *UDP Tx Port Ini* using the subnetwork broadcast IP address. A DNP3 client listening to this port will recognize the specific DNP3 slave's message source IP address and acknowledge the message on the DNP3 slave's *UDP Rx Port* (which then also has to be known by the client). This client IP address is then memorized by the slave, and hereafter only this *Client IP* is accepted and used in all forthcoming UDP traffic.

If the configured keep-alive timeout elapses, then the memorized client IP address is forgotten, and the slave instance will go back in to phase **[1]** of this description.

If the *UDP Tx Port Ini* is not taken in use (0), then **[2]** the DNP3 slave will after client's first *UDP Rx Port* request internally consider the "initial unsolicited message" confirmed, and the client's IP address is memorized. The slave could now be in the state where no unsolicited class reporting is yet enabled. The client should always as the first command enable the class reporting.

If the configured keep-alive timeout occurs, then the memorized client IP address is forgotten, and the slave instance will go back in to phase **[2]** of this description.

3.3.6.4 DNP3 link layer keep-alive timeout vs. UR confirmation timeouts and retransmissions

The DNP3 slave's configured link keep-alive timer is reset every time a valid DNP3 client frame is received. The DNP3 client frame could be a client request or the client's confirmation to an unsolicited response message. If a link keep-alive timeout happens in the slave, then the slave will make some DNP3 link status requests*) to the client, and if no responses are received, then the slave will consider the client lost.

If, before the keep-alive timeout happens, the DNP3 slave's configured application layer retransmissions are exhausted, then the slave could**)enter OFF LINE state.

***) Settings involved are:**

Data link confirm	= This setting is only relevant for variable DNP3 link frames (=application data frames). Link confirmations could then be omitted, since the application confirmation will also cover these. For fixed frame DNP3 request (f.ex. "Request DNP3 Link Status") link confirmations are always used.
Data link confirm TO	= Timeout for the confirmation.
Data link retries	= How many times the request is repeated.

****) Settings involved are:**

App layer confirm	= Application layer confirmations are always automatically enabled for all event (polled- or UR) transmissions. This setting then rather concerns all other application message types.
App confirm TO	= Timeout for the application confirmation.
UR retries	= How many retransmissions are done for a UR telegram.
UR TO	= This value is added to the configured *App confirm TO* value. And the sum is the time we wait for a confirmation to a UR telegram. Reason for this construction is to avoid possible UR re-collisions, by setting this value differently in each slave.
UR offline interval	= After the UR retries has been done, the slave could enter an OFF LINE state for the amount of minutes defined by this setting. During the OFF LINE time no UR transmissions are done. If this setting is 0, then the slave never enters this state, and instead immediately starts all over with the UR retries.

It is recommended to set the *UR offline interval* =0 and let the *Link keep-alive* timeout happen instead of OFF LINE when the client has disappeared.

Also. Do not in this case use DNP3 link confirmations for application messages. Rely here only on application confirmations. This is done in the slave by setting *Data Link Confirm* =Never. Of course, also the DNP3 client should not request data link confirmations from the slave when doing application data requests.

3.3.7 Communication supervision and diagnostics

3.3.7.1 Communication supervision status

The DNP3 protocol provides a link to a keep-alive mechanism which can be used in both Ethernet (TCP/IP) and serial communication modes. When the client has successfully established connection to the protection relay, keep-alive messages are sent periodically by the client or protection relay, depending on which one has a lower keep-alive interval setting. Keep-alive timer is also restarted by any normal DNP3 frame, so keep-alive messages are only being transmitted after a longer idle time between frames. In the protection relay, the keep-alive timeout can be set with the *Link keep-alive (seconds)* parameter.

Default value “0” means that no keep-alive messages are sent by the protection relay. Keep-alive requests sent by the client are still responded to. If a keep-alive message is not responded to, the connection is considered broken. In case of TCP/IP connection the protection relay closes the associated TCP socket connection, and a new connection must be initiated by the client.

The DNP3 link status (True/False) is updated in the Monitoring data Status, which can also be used in Application Configuration in PCM600 for additional logic connection, for example, to a LED. DNP3 link status exists separately for each DNP3 protocol instance. True (value 1) means that the connection is active. False (value 0) means the connection has timed out. The status can be found via **Monitoring** > **Communication** > **Protocols** > **DNP3.0 (n)** > **Status**.

In Application Configuration, the DNP3 protocol instance is represented by a function block DNPLPRTn, where n is the protocol instance number 1…5.

Use of TCP/IP connection keep-alive timeout only

When the DNP3 link keep-alive mechanism is not used in TCP/IP case, the Ethernet stack TCP socket keep-alive mechanism is still in use. If there is a TCP socket keep-alive timeout, the protection relay closes the associated TCP socket connection and updates the DNP3 link status.

3.3.7.2 Diagnostic communication counters

The diagnostic communication counters dependent on protocol instance n are provided in the protection relay. These counters can be accessed via **Monitoring** > **Communication** > **Protocols** > **DNP3.0 (n)**.

Table 2: Diagnostic communication counters

Diagnostic counter	Description
Received frames	Total amount of received DNP3 frames
Transmitted frames	Total amount of transmitted DNP3 frames
Physical errors	Total amount of physical layer errors noticed
Link errors	Total amount of link layer errors noticed

Table continues on the next page

Diagnostic counter	Description
Transport errors	Total amount of transport layer errors noticed
Mapping errors	Total amount of protocol mapping errors noticed
Status	Shows the value "True" if the TCP/IP or serial instance is active. This means that a DNP3 client has connected to the TCP socket and DNP3 messages are received regularly at least within
	<Link keep-alive> second interval or faster. In all other cases this value is "False".
Reset counters	True = Reset all diagnostic counters

For non-activated instances n, no communication diagnostic values are shown by the HMI. Diagnostic counter values are initially set to “-1” to indicate that no messages have yet been processed by the active instance. As soon as a message is received or transmitted, the counters initialize to “0”.

In a serial bus troubleshooting case, if no DNP3 diagnostic counter is running, the COMn serial driver settings and driver diagnostic counters should be checked.

3.4 Data objects

3.4.1 Readable data objects

DNP3 data objects in the protection relay are all unmapped by default. Using Communication Management in PCM600, the objects can be freely added into the DNP3 memory map.

The available DNP3 data objects are taken (mapped) entirely from the native IEC 61850 application data available in the protection relay.

The DNP3 point configuration can be completed only after the protection relay's application configuration has been created.

- If a function block is removed from the configuration, the DNP3 objects belonging to the function block are automatically deleted from the DNP3 point list. If the points were mapped to DNP3 object addresses, the mapping contains gaps. However, those can be modified with Communication Management in PCM600.
- If a function block is added, the DNP3 points from this function block appear by default as unmapped in Communication Management.

3.4.2 Event classes

DNP3 objects that are not of “Static-only” type can be assigned by Communication Management in PCM600 into DNP3 event classes 1...3. Event buffering is defined per DNP3 object type and not by DNP3 event class.

Only native IED objects that reside in an IEC 61850 data set are reported upon change. When a DNP3 object is added to an event class, a data set of the corresponding native object is automatically checked. If the object does not reside in a public IEC 61850 data set yet, it is automatically added to an internal, non-public data set. Consequently, if the object is assigned to a DNP3 event class, it is also generated upon change from the native IEC 61850 application.

Different DNP3 object types are often assigned to different DNP3 event classes. This has no consequence if the client performs class polling simultaneously to all the three classes. Outstation still responds to the events in chronological order. However, there are some advantages.

- The event buffering is handled by DNP3 object type, but a possible event overflow signal is in turn given from the DNP3 event class. If a class only contains a particular object type, the overflow occurs for that DNP3 object type.
- In unsolicited reporting mode, the controlling station enables the outstation event classes that are subject to spontaneous event reporting. One or some of the event classes could then be left disabled.

3.4.3 Writable data objects

Writable objects belong to object types 10 (binary outputs) and 40 (analog outputs). Outputs are controlled through the control relay output block or analog output block commands. From the DNP3 output objects, the commands are propagated further to the native IEC 61850 control objects.

3.4.3.1 Control relay output block parameters

Controlling of the native IEC 61850 objects differs from the way that an RTU control operation is defined by DNP3. In DNP3 standard, it is assumed that the controlling station decides the control type (pulse or persistent), pulse lengths and possible pulse trains (number of pulses). These control parameters are given to the RTU outstation in the CROB command. In the IEC 61850 standard, the same parameters and few additional parameters are configured as properties of the control objects. The control command issued to the control object is only a trigger. In a protection relay, the control object knows how to perform the physical control operation.

In CROB data, the given pulse type and pulse length values are ignored by the outstation. The only data that is checked by the outstation is the direction (ON or OFF). If the IEC 61850 data object is of persistent type, OFF is also possible. When controlling a double-pole IEC 61850 data object, the direction information is used.

DNP3 protocol stack only accepts the standard combinations of OpType/TCC fields. This means in practice only specific combinations are supported, and the rest of the combinations are discarded and "not supported" return value is responded. *Table 3* describes the operation direction for the combinations.

Table 3:

TCC	OpType	DPC	SPC
NULL	PulseOn	Close	1
NULL	LatchOn	Close	1
NULL	LatchOff	Trip	0

Table continues on the next page

TCC	OpType	DPC	SPC
Close	PulseOn	Close	1
Trip	PulseOn	Trip	0

3.4.3.2 Direct operate and select before operate

Both direct-operate and select-before-operate DNP3 control functions are supported for binary outputs.

In the native IED IEC 61850 data, these control operation differences are referred to as the control model. The control model is in turn configured as a property of the control object. Thus an IEC 61850 control object can be either in “Direct” or “SBO” mode. This is applicable for double-point control objects. Single-point control objects in the protection relay always work in “Direct” mode. Depending on the control model setting of the native IEC 61850 control object, various DNP3 control functions can be performed.

Table 4: Available control models

IEC 61850 control model	Supported DNP3 control function
Direct	Direct only
SBO	Direct or SBO

When making a DNP3 direct command to an SBO configured object, the desired behavior can be defined in Communication Management. In case the direct control mode property is set to “Always allowed”, the DNP3 stack automatically performs the two needed commands to the native control object. Direct control is always allowed. In case the direct control mode property is set to “Control model”, the DNP3 control command must follow the native IEC 61850 objects' control model. SBO control must be used in the SBO mode.

The DNP3 stack has a protocol-dependent parameter setting for the timeout between Select and Operate commands. The default value is "10 seconds" but it can be changed via *CROB select timeout* parameter. Also, the native control object has a configured timeout for the SBO operation. Since the control object may also be available for Local (manual) control, a longer timeout is often required. The DNP3 timeout should be set lower than the native control object's timeout.

3.4.3.3 Command blockings

According to the DNP3 standard, an outstation is considered to have the states “Local” or “Remote”. The IEC 61850 IED in turn can be in “Local”, “Station”, “Remote”, “Off”, or “All” state. A DNP3 controlling station can perform control operations in “Station”, “Remote”, and “All” protection relay states. However, it is the controlled protection relay's application in the outstation that rejects or accepts control operations based on the control allowance states and not the DNP3 protocol stack. In an RTU (non-intelligent outstation) application, the DNP3 stack rejects the commands.

[1] Configurable with the Communication Management tool

3.4.4 Data object mapping

As REX640 is a freely configurable device, almost all internal IEC 61850 data objects can be mapped to DNP3. The internal native IEC 61850 objects have been assigned with potential (empty) DNP3 mappings according to the general rules based on IEC 61850 common data classes (CDC).

The following data is unmapped: the Beh and Mod attributes of every logical node and some redundant data objects within the generic function blocks.

Table 5: Mapping rules

Class	Description	Attribute [1]	DNP3 data type
SPS	Singe point status	stVal	BI data
SPC	Controllable single point status	stVal	BI data
		Oper.ctlVal	BO data
DPC	Controllable double point status	stVal [2]	Double Point and AI data
		Oper.ctlVal	BO data
ACD	Protection activation detection (Start)	general	BO data
		dirGeneral	AI data
		phsA	BI data
		phsB	BI data
		phsC	BI data
		neut	BI data
ACT	Protection activation (Operate)	general	BI data
		phsA	BI data
		phsB	BI data
		phsC	BI data
		neut	BI data
INS	Integer value	stVal	AI data
INC	Controllable integer value	stVal	AI data
		Oper.ctlVal [3]	AO or set of BO data
ENS	Enumeral value	stVal	AI data
ENC	Controllable enumeral value	stVal [4]	AI data or set of BI data
		Oper.ctlVal [3]	AO or set of BO data
MV	Meas value	mag.f	AI data
		instMag.f	

Table continues on the next page

[1] A data object need not contain all data attributes that are listed for the object class in question.
[2] Switchgear position data is available as either Double Point or AI data for backward compatibility.
[3] AO data is supported. In some cases, there is also an alternative BO mapping for this kind of objects.
[4] AI data is supported. In some cases, there is also an alternative set of BI data mapping for this kind of objects.

Class	Description	Attribute [1]	DNP3 data type
CMV	Complex meas value	instCVal.mag.f	AI data
		cVal.mag.f	
DEL	Phase-to-phase measurements	phsAB.instCVal.mag.f	AI data
		phsAB.cVal.mag.f	AI data
		phsBC.instCVal.mag.f	AI data
		phsBC.cVal.mag.f	AI data
		phsCA.instCVal.mag.f	AI data
		phsCA.cVal.mag.f	AI data
WYE	Phase-to-ground measurements (filtered)	phsA.instCVal.mag.f	AI data
		phsA.cVal.mag.f	AI data
		phsB.instCVal.mag.f	AI data
		phsB.cVal.mag.f	AI data
		phsC.instCVal.mag.f	AI data
		phsC.cVal.mag.f	AI data
		neut.instCVal.mag.f	AI data
		neut.cVal.mag.f	AI data
		net.instCVal.mag.f	AI data
		net.cVal.mag.f	AI data
		res.instCVal.mag.f	AI data
		res.cVal.mag.f	AI data
SEQ	Sequence of components	c1.instCVal.mag.f	AI data
		c1.instCVal.ang.f	AI data
		c2.instCVal.mag.f	AI data
		c2.instCVal.ang.f	AI data
		c3.instCVal.mag.f	AI data
		c3.instCVal.ang.f	AI data
BCR	Binary counter	actVal	Counter data
ISC	Integer controlled step position	valWTr.posVal	AI data
BCS	Binary controlled step position	valWTr.posVal	AI data
		Oper.ctlVal	AO data

3.4.5 Update rate of analog and indication protocol data

Update rate of protocol data depends on multiple factors that needs to be considered when communication engineering is done. This chapters 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.

[1] A data object need not contain all data attributes that are listed for the object class in question.

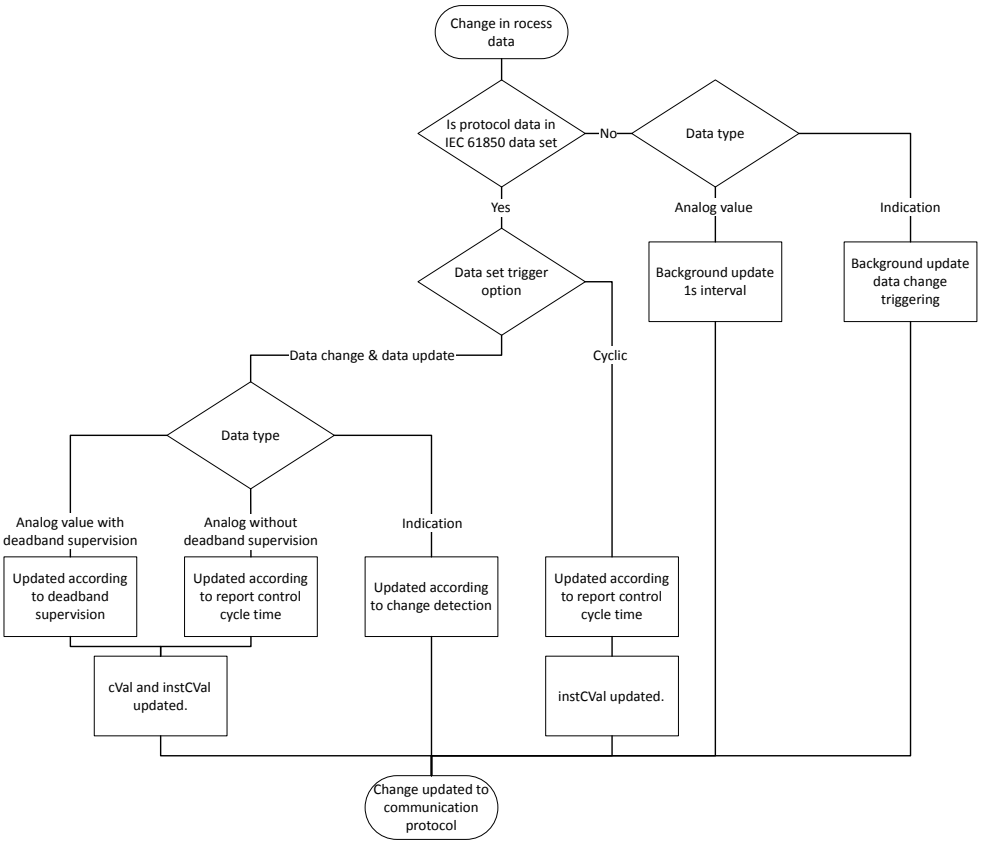

Figure 3: Data flow from process data change to communication protocol

Report Control in IEC 61850

Data update rate is dependent of data set and report control engineering in IEC 61850. In the most cases default values are suitable, but it is necessary to understand all dependencies when modifications are needed.

- Data set content
- Trigger options for report control
- Signals selected in communication management (instantaneous or deadband supervised value)

Engineering of event reporting is described in IEC 61850 Engineering Guide.

Application function deadband supervision

The deadband supervision function reports the measured value according to integrated changes over a time period. The sensitivity of reporting can be adjusted with the *X deadband* parameter of a measurement function. By default, deadband supervision defines update rate of analog values to communication protocol. Technical manual describes dead band supervision in more details.

3.5 Standard data object types

3.5.1 Binary inputs

DNP3 object type 1, binary input objects are derived from IEC 61850 data object's boolean type attributes, mainly from data classes SPS, SPC, ACD and ACT. Also, few binary input objects have been converted from enumeral INS and INC classes (ENS and ENC classes in Edition 2).

The circuit breaker and disconnector double point data objects, containing open and close bits, also exist in the DNP3 map as normal single binary input alternatives. These are intended for DNP3 controlling stations that do not support the double bit input DNP3 data type alternative (Object group 3).

DNP3 object type 2, binary input change events can buffer up to 200 events. When the buffer becomes full, the new events are discarded until more space is available in the event buffer.

Binary inputs which are not of "Static-Only" type can be assigned to any DNP3 event class. Furthermore, it is possible to invert the signals if necessary, for example, generic input data.

The default variation for all binary input values can be set with the *Default Var Obj 01* parameter.

3.5.2 Double point inputs

Double Bit input (object type 3) is supported by the protection relay. Double point objects are derived from the protection relay's internal data class DPC, that is, circuit breaker and disconnector position data. An alternative DNP3 analog input data always exists for the double point data. If the DNP3 client does not support object type 3, the analog input is the only other alternative for representing the double point value in one DNP3 data object.

The size of the DNP3 Double Bit input event buffer is 100.

3.5.3 Analog inputs

DNP3 analog input data (Object type 30) is mainly derived from the protection relay's IEC 61850 measurand object classes MV and CMV. Since the MV and CMV source values are of float32 type, the default setting for the default variation of DNP3 analog data is float32.

If needed, the default variation can be changed to integer 16 or 32 bit types. In such a case, re-scaling of the original data has to be applied.

There are four scaling options associated with analog input reporting.

- None: The value is presented as it is. None of the configured values in Communication Management columns Min Source Value, Max Source Value, Min Dest Value and Max Dest Value has any effect.
- Multiplication: The process value is multiplied by a constant. An offset is added producing the reported value. In Communication Management the constant is found in the Max Dest Value column and the offset in the Min Dest Value column.

- Division: The process value is divided by a constant. An offset is added by producing the reported value. In Communication Management the constant is found in the Max Dest Value column and the offset in the Min Dest Value column.
- Ratio: The four configured values *Min Source Value*, *Max Source Value*, *Min Dest Value* and *Max Dest Value* are all used. With ratio scaling it is possible to define a new linear scaling (including possible offset) and to set value limits for the measurand.

Consider this example:

- The source value (SourceValue) range of a secondary current value is defined as 0.00…60.00 x In
- In = 500 A and we want to present the DNP3 value in primary Amperes.
- Furthermore, we want not to show any DNP3 value larger than 4.00 x In, meaning that all source values larger than this saturate at 4.00 x In (= 4 x 500 A).

Table 6: Ratio scaling

Setting	Value
Min Source Value	0
Max Source Value	4
Min Dest Value	0
Max Dest Value	2000

The reported DNP3 value can be expressed as:

$$(SourceValue - MinSourceValue) \cdot \left(\frac{(MaxDestValue - MinDestValue)}{(MaxSourceValue - MinSourceValue)} \right) + MinDestValue$$

(Equation 1)

Some DNP3 analog input points, such as CT or VT measurement values, support primary and secondary scaling. This selection can be done in PCM600 by selecting either "Primary value" or "Secondary value" for *Representation*. If the analog input object does not support primary and secondary scaling, the selection has no effect.

Analog Input events can be set in two operating modes by the *An In Evt Mod* parameter. In *SOE* (Sequence of Events) mode all detected Analog Input changes are queued in the event buffer, so event buffer can have multiple events of the same Analog Input point. In the *Most Recent* mode only the most recent changed value is preserved in the event buffer, per Analog Input point. This mode can be used if there is no need to know historical events/timestamps of the Analog Input values and event buffer space needs to be used sparingly.

3.5.3.1 DNP3 analog input change events

The DNP3 analog input event buffer size is 150.

The DNP3 stack is dependent on the IEC 61850 change detection system to generate change events for the corresponding mapped DNP3 AI objects. The IEC 61850 change detection functionality is based on certain factors.

- The corresponding IEC 61850 AI object must reside in a Meas data set, and the data set must be enabled for reporting.

- If the data set is set to use cyclical reporting, all the AI data in the data set are updated with the data set's defined cycle time. Only changed AI data is propagated further to the DNP3 stack.
- If the data set is set to use change reporting, the AI data in the data set can belong to two predefined categories.
  1. Measurand AI values for which the value update changes are triggered by the AFL function block. These values are propagated to the DNP3 stack immediately when the function block triggering occurs.
  2. Measurand AI values without an AFL change triggering mechanism. These AI values are scanned for changes using the data set's configured cycle time. If changes are noticed, the AI objects are propagated further to the DNP3 stack.

Consequently, AI events arriving from the IEC 61850 level to the DNP3 stack are always changed values. The sampling rate and deadband can be modified for the DNP3 AI points through Communication Management in PCM600.

- If a DNP3 analog input points' additional *Deadband* value is set to "0.0", the IED system analog events are propagated as such through the DNP3 protocol.
- The sampling rate of the DNP3 AI value can also be reduced through the points' *Deadband Time* setting. This means that the events are transmitted less frequently. If *Deadband Time* is, for example, set to "2", analog events are produced less frequently than every two seconds from the DNP3 AI object.

3.5.4 Counter objects

DNP3 counter objects (object type 20) are derived from the relay's IEC 61850 object class BCR. For each counter, there is also a frozen counter value available for reading as object type 21.

There are two types of counters in the relay.

- BCR class is an integrated totals type counter, typically used for energy values.
- INC class counters are operational counters, for example, circuit breaker control counters.

It is possible to freeze and reset the DNP3 counters in this relay. However, the original BCR counters are also reset. Another method is to read the cumulative values and not reset the counters.

The DNP3 Counter, and Frozen Counter event buffer size is 30.

3.5.5 Binary outputs and control relay output block

DNP3 binary outputs (Object group 10) are cross-coupled with the protection relay's IEC 61850 control data classes SPC and DPC. The DNP3 stack automatically handles the conversion between the two protocols' control models.

DNP3 control is never done directly to the binary outputs but rather indirectly using the Control Relay Output Block (CROB) function. The CROB function contains some additional information regarding the control sequence, for example, pulse length and number of control pulses. These parameters are intended for RTU type (non-intelligent) DNP3 devices. However, in this protection relay, all the required control parameters are already configured properties of the control object. Therefore most control parameters given in the DNP3 CROB command are ignored by the protection

relay. Only the control direction is noticed. Most single point objects, like resets and acknowledgements, can only be controlled using ON. However, there may also be single point objects that have two states, ON or OFF. Double-point objects may be controlled using ON or OFF.

3.5.5.1 Control modes

All DNP3 binary outputs support direct control at any time. Double-point objects (circuit breakers and disconnectors) also support select-before-operate controls, provided that the native IEC 61850 control objects are in SBO control model mode. A double-point control is represented with one binary output point on DNP3 even if there are two separate control relay outputs (open and close) from the protection relay.

3.5.5.2 Accessing of physical outputs

Unlike an RTU device, the protection relay's physical output relays cannot be controlled directly with remote communication. However, this can be done using generic control points and dedicated Application Configuration application connections.

3.5.5.3 Control feedback

When the binary output values are read from the protection relay, the last written value is returned. However, while controlling an object, the final status change of the object should be verified from the corresponding binary input object, if available.

In case of double-point control, the IEC 61850 standard defines a value attribute named *stSeld* to be always available for the control object. In case of SBO, this value shows if the control object is selected, for example, by another controlling source. This value is found in the DNP3 memory map as a regular DNP3 binary input. The *stSeld* value goes on (“1”) and off (“0”) during a control operation and is always held in true state (“1”) by the protection relay until the control operation is terminated.

In case of a long-lasting control operation, for example, a motor-controlled disconnector, the *stSeld* value can stay true for several seconds after the control operation is acknowledged and started. A new control operation cannot be started by the protection relay until the previous one has finished.

3.5.6 Analog outputs

Analog outputs are cross-referenced to the .Oper.ctlVal attribute of the protection relay's object class INC, controllable integer. If the INC object is readable, the .stVal attribute of the object is mapped to DNP3 AI data.

The protection relay platform contains a few controllable analog objects, for example, parameter setting group selection, tap changer control and fault record read selection. All analog objects are of integer type. The values do not have to be scaled.

The Analog Output Block DNP3 object group (41) is used for writing to a DNP3 analog output. Analog output can be also read from the protection relay, as object group 40. Reading an analog output returns the last written value to the object.

Class events are generated for changed Analog Output values. The DNP3 Analog Output event buffer size is 100.

3.6 Fault records

Fault record data objects contain registered values captured simultaneously by the relay's protection at the moment of a fault. The fault record objects internally belong to IEC 61850 logical node FLTRFRC1.

The FLTRFRC1 objects can be found as DNP3 analog input values in the DNP3 point list. There are two alternative DNP3 data objects for each captured fault record object in the point list. A different trailing text for the objects is shown in the object's name, either “Ev-Upd” (event updated) or “Record” (read on demand).

3.6.1 Ev-Upd type objects

A freely selectable part of the “Ev-Upd” objects, or all objects can be added to the DNP3 analog input data memory map. These objects can also be enabled for DNP3 class events. Each time a new fault record capture is done by the protection relay, the objects are sent as DNP3 class events to the controlling station. Every object captured at the same time (belonging to the same record) has the same time tag. The controlling station can also read fault record objects from the outstation at any time. The most recent captured value is always returned.

The deadband setting for the “Ev-Upd” objects should be “0”. This means that every update of the object from the protection relay level is propagated as a DNP3 class event, regardless of the change in value. By default, all analog inputs have deadband setting of 0.0, that is, the event is always reported when a system event is generated. In the fault record, the next captured value can be identical to the previous one, therefore the recommended deadband value is 0.0.

3.6.2 Record type objects

The protection relay saves the latest 128 captured fault records internally. On demand, these older records can be read by the DNP3 controlling station.

A freely selectable part of the “Record” objects can be added to the DNP3 analog input data memory map. These objects are by default defined as ‘Static only’. This means that they can only be read on demand by the controlling station. The analog output object from the same logical node named FLTRFRC1.SelRow.ctlVal ‘- Select record’ should also be added to the DNP3 analog output area.

The stored fault records are internally saved in indexes numbered 1...128. When the controlling station writes a value 1...128 to the “Select record” object, the entire set of fault record values belonging to that record is copied to the “Recorded” fault record DNP3 AI values. Thereafter, the controlling station can read the fault record values.

3.6.3 Time stamp for record type objects

One disadvantage of the DNP3 protocol is that static data read does not include any time stamps for the static values. It is impossible to know when the value of the DNP3 data object was updated. Therefore, the time stamp of the record itself is recoded into a set of seven DNP3 analog input objects. The objects contain the year, month, day, hour, minute, second, and millisecond values of the time stamp.

3.6.4 Additional fault record implementation details

The protection relay's native fault record application can be configured to make captures at an operate situation or during start situations (not leading into operate). The latter alternative often causes more captures. The DNP3 protocol has no part in the setup of the fault record application. The chosen fault record setup is reflected to all readers of the fault record data, including HMI. If the values are intended to be available for several readers, a fault record clear operation from any reading source is not recommended. There are several alternatives for any remote client, including DNP3, to access the captured fault record data.

Alternative 1, buffering on the DNP3 client side

The easiest alternative is that the client receives the time-tagged fault record values as events at the moment when they are captured in the protection relay. The client system must then observe that all fault record values with identical event time tag belong to the same capture. A new fault record capture can take place in the protection relay right after the previous one. The new fault record values are again sent as events to the client. The client system is responsible for buffering up these values, in case it is necessary to later look at older captures.

Alternative 2, buffering on the DNP3 outstation side

If fault records' values are not sent as events to the client, the latest record capture values can be read directly from the outstation's DNP3 AI area. In this case, also the older captures are to be read out from the outstation, but the client must perform a control action towards the server.

There are up to 128 fault records stored in the protection relay. The records are located chronologically in a circular buffer indexed from 1...128. If the client makes a DNP3 AO write with an index value (1...128) to the object FLTRFRC1.SelRow.ctlVal, then the values from that particular record are copied into the FLTRFRC1 fault record values. Thereafter the DNP3 client can read them using regular DNP3 AI reading.

The latest record is stored at index (row) 1, and the oldest record at index 128. Records are stored in a FIFO buffer, that is, the oldest record is dropped out from index 128, and latest record always stored at index 1.

The fault record also has an increasing counter for record number which can be used to track different fault records. This value is derived from data FLTRFRC1.OpCnt.stVal, it counts 1...999999 and rolls over at maximum. If OpCnt = 0, there is no fault record data available.

If the FLTRFRC1.OpCnt.stVal object is added as an "Ev-Upd" object to the DNP3 AI data, and then enabled for class events, it serves as an indication on the client side that a new fault record has been captured.

It is also possible that the client has stored the latest fault record index value it used in the previous reading. When starting to read out new records, it could simply continue from the memorized index + 1 onwards.

3.7 Secure communication

3.7.1 Secure Authentication setup

The relay supports DNP3 Secure Authentication version 5 (SAv5), with symmetric keys. The secure authentication is described in the DNP3 standard part 7 “IP Networking”, chapter “Secure authentication”. DNP3 Secure Authentication follows the IEC 62351-5 security standard authentication specification.

The secure application authentication can be used with or without TLS encryption. The secure authentication can be enabled in the relay via **Configuration** > **Communication** > **Protocols** > **SDNP3.0 (n)** > **General** with the setting parameter *Protocol Sec Mode*.

Several setting and configuration steps are needed to take into use the secure authentication feature. For better understanding of the overall functionality, it is recommended to first get familiar with the standard document mentioned above.

A common preset key, the authority certification key, needs to be set both in the client and in the outstation (the relay). Depending on the system layout, this key can be obtained in different ways, but preferably it is obtained from some third party acting as the authority. This key must then be written to the relay by PCM600 Account Management. See the PCM600 documentation for more details on writing the certification key.

The authority certification key length can be 128 or 256 bits, and is freely selectable in the configuration tool. In the relay, the selected authority certification key length dictates the used key change method and MAC algorithm. The settings must be configured accordingly in the DNP3 client in order to match the relay settings.

Table 7: Dependency between the authority certification key length and the algorithms supported

Authority certification key length [Bits]	Update key method	MAC algorithm	
		TCP	Serial
128	<3> AES-128 / SHA-1	SHA1 / 10OCTET	SHA1 / 8OCTET
256	<4> AES-256 / SHA-256	SHA256 / 16OCTET	SHA256 / 8OCTET

Additionally, the “Outstation name” must be set correctly in the DNP3 client to match the relay. In the relay there is no separate setting for “Outstation name”. Instead, the name is the same as the relay's technical key.

After enabling the security authentication and writing the authority certification key, relay reboot is required to start the secure communication. PCM600 performs this reboot automatically.

3.7.2 TLS encryption

Before enabling TLS encryption in the relay, it is necessary to import a public key certificate to the relay which should be signed by a trusted certification authority (CA). In order for a TLS communication link to be established with the relay, the DNP3 client must also be configured to use TLS and a public key certificate signed by the same CA.

For more information, see the cyber security deployment guideline.

TLS encryption can be enabled for the relay's DNP3 TCP communication by selecting the option "TLS and appl. authentication" in setting parameter *Protocol Sec Mode* under **Configuration** > **Communication** > **Protocols** > **SDNP3.0 (n)** > **General**.

In addition to end-to-end cryptographic authentication at the application layer, TLS is also supported by DNP3 secure communication.

3.7.3 User and key management in the relay

After the configuration setup, the client is able to manage the users and keys in the relay.

The DNP3 SA users and keys can be updated to the relay by the client using the DNP3 object type 120 user management command (variations 10...15). As defined by the DNP3 standard, a user named “Common”, with SINGLEUSER privileges, is predefined in the relay as user number 1. The update keys for the users are not set by default and need to be updated by the client. However, once they are set, the users and the update keys are retained during a relay reboot.

When communication is first initialized by the DNP3 client, the user list defined in the client needs to be synchronized with the relay using the User Status Change (obj120v10) and Update Key Change (obj120v11 to obj120v15) commands. The relay responds to the user change command requests with the assigned user number and a success status. The DNP3 client needs to receive and memorize the assigned user number to its own user database. After the client’s user database is updated and users and session keys are updated, the client can start sending secure DNP3 requests to the relay, using the desired user numbers.

If the user update process between the client and the relay fails, the relay indicates this by responding with DNP3 error 120v7, and incrementing its error diagnostic counters.

The relay supports a maximum of 50 DNP3 users per protocol instance. The maximum user name length is 20 characters.

DNP3 UDP broadcast messages are not authenticated. To have full secure authentication, use the “TCP only” port mode.

3.7.4 Secure authentication settings

3.7.4.1 Predefined behavior

Some secure authentication behavior is predefined in the relay.

Association Id

The relay supports up to five DNP3 protocol instances simultaneously. The Association Id for each instance corresponds to the protocol instance number seen in the menu structure name and in Application Configuration.

Critical messages

The relay considers all DNP3 requests performing write and control functions as critical operations which require an additional authentication handshaking (challenge-response). Controls include binary output and analog output controls and time synchronization. For a definite list, see the conformance statement that is separately published at ABB website.

User roles

The relay supports the default secure authentication user roles as defined by the IEC 62351-5 standard.

Table 8: Default secure authentication user roles

User role	Monitor (read) data	Operate (write) data
VIEWER	Yes	No
OPERATOR	Yes	Yes
ENGINEER	Yes	No
INSTALLER	Yes	No
SECADM	No	No
SECAUD	Yes	No
RBACMNT	Yes	No
SINGLEUSER	Yes	Yes

To create a DNP3 user with access rights for all the supported DNP3 operations, either SINGLEUSER or OPERATOR permission should be applied.

3.7.4.2 Security parameters

Several secure authentication setting parameters are adjustable in the relay. The behavior of these parameters follows the DNP3 standard. See the Secure Authentication chapter in the DNP3 specification for more detailed information about these parameters.

All the parameters with short descriptions are listed at the end of this manual. Here are explained some of the more important settings.

Aggressive mode

The relay supports DNP3 authentication aggressive mode, which can be enabled via **Configuration** > **Communication** > **Protocols** > **SDNP3(n)** > **General** with the parameter *Aggressive mode enable*.

Session key change interval

Settings *Exp Sesn key Chg Cnt* and *Exp Sesn key Chg Intv* define how the relay expects the client to renew the session keys: either after a number of messages, or after a time interval in seconds, whichever occurs first. The settings are stored under **Configuration** > **Communication** > **Protocols** > **SDNP3 (n)** > **General**.

Reply timeout

Parameter *Reply Timeout (ms)* defines the time the relay waits for a response to an authentication message before it reports a timeout error. The parameter is stored under **Configuration** > **Communication** > **Protocols** > **SDNP3(n)** > **General**.

3.7.5 Statistics and security events

The relay offers security statistics counters for analyzing and diagnosing authentication-related events. As required by the standard, the statistics counters are preserved in the relay memory during a device reboot. The statistics values are available via **Configuration** > **Monitoring** > **Communication** > **Protocols** > **SDNP3 (n)**.

The relay also offers the security statistics values to be monitored by the DNP3 client: Object type 121 for static data and object type 122 as change events. The object type 122 event class and variation are configurable via **Configuration** > **Communication** > **Protocols** > **SDNP3 (n)** > **General** with the settings *Event Class obj 122* and *Default Var obj 122*.

Additionally, a threshold deadband can be set for each security statistics counter to filter reporting of counter values constantly as DNP3 object type 120 events. The threshold settings are located under **Configuration** > **Communication** > **Protocols** > **SDNP3 (n)** > **Statistics Thresholds**.

3.7.6 Troubleshooting

If the secure authentication communication cannot be successfully established, several settings should be checked.

1. Authority certification key

   If there is mismatch between the DNP3 client and the relay, the relay increments Err Msgs Tx Cnt during update requests, and responds to the requests with obj120v7 Error Code 10.

2. Outstation name

   This name must be configured in the DNP3 client to match the relay's technical key.

3. Update key method / MAC algorithm

   These settings are derived from the authority certification key length in the relay.

   These settings must match the ones configured in the DNP3 client.

4 DNP3 parameters

4.1 Link and application layer parameters

The DNP3 parameters can be accessed with PCM600 or via the HMI path **Configuration** > **Communication** > **Protocols** > **DNP3.0 (n)**.

Some parameters are not visible in the “Basic” setting visibility mode. To view all parameters, use “Advanced” setting visibility mode in Parameter Setting in PCM600 and HMI.

Some DNP3 parameters, such as *Operation*, *Port*, *Mapping select*, and *Protocol Security Mode*, require a relay reboot. The HMI notifies about the boot need for these parameters.

4.1.1 DNP 3.0 Settings

Table 9: Non group settings

Parameter	Values (Range)	Unit	Step	Default	Description
Operation	1=on 5=off			5=off	Operation Off / On
Port	1=COM 1 2=COM 2 3=Ethernet - TCP 1 4=Ethernet TCP+UDP 1 5=Ethernet - UDP 1			3=Ethernet - TCP 1	Communication interface selection
Unit address	0...65519		1	1	DNP unit address
Master address	0...65519		1	3	DNP master and UR address
Mapping select	1...2		1	1	Mapping select
ClientIP				0.0.0.0	IP address of client
TCP port	20000...65535		1	20000	TCP Port used on ethernet communication
UDP Rx Port	1...65535		1	20000	UDP Port for accepting data from client/master
UDP Tx Port Ini	1...65535		1	20000	UDP Port for initial NULL response to client/master
UDP Tx Port	0...65535		1	0	UDP Destination Port for client/master
Client control authority	0=No clients 1=Reg. clients 2=All clients			2=All clients	0=no client controls allowed; 1=Controls allowed by registered cli-

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
					ents; 2=Controls allowed by all clients
Link keep-alive	0...1000000	s	1	0	Link keep-alive interval for DNP
Validate master addr	1=Disable 2=Enable			1=Disable	Validate master address on receive
Self address	1=Disable 2=Enable			2=Enable	Support self address query function
Need time interval	0...65535	min	1	30	Period to set IIN need time bit
Time format	0=UTC 1=Local			1=Local	UTC or local. Coordinate with master.
CROB select timeout	1...65535	s	1	10	Control Relay Output Block select timeout
Data link confirm	0=Never 1=Only Multiframe 2=Always			0=Never	Data link confirm mode
Data link confirm TO	100...65535	ms	1	3000	Data link confirm timeout
Data link retries	0...65535		1	3	Data link retries count
Data link Rx to Tx delay	0...255	ms	1	0	Turnaround transmission delay
Data link inter char delay	0...20	char	1	4	Inter character delay for incoming messages
App layer confirm	1=Disable 2=Enable			1=Disable	Application layer confirm mode
App/UR confirm TO	100...65535	ms	1	5000	Application layer confirm and UR timeout
App layer fragment	256...2048	bytes	1	2048	Application layer fragment size
UR mode	1=Disable 2=Enable			1=Disable	Unsolicited responses mode
UR retries	0...65535		1	3	Unsolicited retries before switching to UR offline mode
UR retry delay	0...65535	ms	1	5000	Additional delay kept after App/UR confirm TO before sending new unsolicited retry
UR offline interval	0...65535	min	1	15	Unsolicited offline interval
UR Class 1 Min events	0...999		1	2	Min number of class 1 events to generate UR
UR Class 1 TO	0...65535	ms	1	50	Max holding time for class 1 events to generate UR
UR Class 2 Min events	0...999		1	2	Min number of class 2 events to generate UR
UR Class 2 TO	0...65535	ms	1	50	Max holding time for class 2 events to generate UR

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
UR Class 3 Min events	0...999		1	2	Min number of class 3 events to generate UR
UR Class 3 TO	0...65535	ms	1	50	Max holding time for class 3 events to generate UR
Legacy master UR	1=Disable 2=Enable			1=Disable	Legacy DNP master unsolicited mode support. When enabled relay does not send initial unsolicited message.
Legacy master SBO	1=Disable 2=Enable			1=Disable	Legacy DNP Master SBO sequence number relax enable
Default Var Obj 01	1=1:BI 2=2:BI&status			1=1:BI	1=BI; 2=BI with status.
Default Var Obj 02	1=1:BI event 2=2:BI event&time			2=2:BI event&time	1=BI event; 2=BI event with time.
Default Var Obj 03	1=1:DBI 2=2:DBI&status			1=1:DBI	1=DBI; 2=DBI with status.
Default Var Obj 04	1=1:DBI event 2=2:DBI event&time			2=2:DBI event&time	1=DBI event; 2=DBI event with time.
Default Var Obj 20	1=1:32bit Cnt 2=2:16bit Cnt 5=5:32bit Cnt no-flag 6=6:16bit Cnt no-flag			2=2:16bit Cnt	1=32 bit counter; 2=16 bit counter; 5=32 bit counter without flag; 6=16 bit counter without flag.
Default Var Obj 21	1=1:32bit FrzCnt 2=2:16bit FrzCnt 5=5:32bit FrzCnt&time 6=6:16bit FrzCnt&time 9=9:32bit FrzCnt noflag 10=10:16bit FrzCnt noflag			6=6:16bit FrzCnt&time	1=32 bit frz counter; 2=16 bit frz counter; 5=32 bit frz counter with time; 6=16 bit frz counter with time; 9=32 bit frz counter without flag;10=16 bit frz counter without flag.
Default Var Obj 22	1=1:32bit Cnt evt 2=2:16bit Cnt evt 5=5:32bit Cnt evt&time 6=6:16bit Cnt evt&time			6=6:16bit Cnt evt&time	1=32 bit counter event; 2=16 bit counter event; 5=32 bit counter event with time; 6=16 bit counter event with time.
Default Var Obj 23	1=1:32bit FrzCnt evt 2=2:16bit FrzCnt evt 5=5:32bit FrzCnt evt&time 6=6:16bit FrzCnt evt&time			6=6:16bit FrzCnt evt&time	1=32 bit frz counter event; 2=16 bit frz counter event; 5=32 bit frz counter event with time; 6=16 bit frz counter event with time.
Default Var Obj 30	1=1:32bit AI 2=2:16bit AI 3=3:32bit AI noflag			5=5:AI float	1=32 bit AI; 2=16 bit AI; 3=32 bit AI without flag; 4=16 bit AI without flag; 5=AI float; 6=AI double.

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
	4=4:16bit AI noflag 5=5:AI float 6=6:AI double				
Default Var Obj 32	1=1:32bit AI evt 2=2:16bit AI evt 3=3:32bit AI evt&time 4=4:16bit AI evt&time 5=5: float AI evt 6=6:double AI evt 7=7:float AI evt&time 8=8:double AI evt&time			7=7:float AI evt&time	1=32 bit AI event; 2=16 bit AI event; 3=32 bit AI event with time; 4=16 bit AI event with time; 5=float AI event; 6=double AI event; 7=float AI event with time; 8=double AI event with time.
Default Var Obj 40	1=1:32bit AO 2=2:16bit AO 3=3:AO float 4=4:AO double			2=2:16bit AO	1=32 bit AO; 2=16 bit AO; 3=AO float; 4=AO double.
Default Var Obj 42	1=1:32bit AO evt 2=2:16bit AO evt 3=3:32bit AO evt&time 4=4:16bit AO evt&time 5=5:float AO evt 6=6:double AO evt 7=7:float AO evt&time 8=8:double AO evt&time			4=4:16bit AO evt&time	1=32 bit AO event; 2=16 bit AO event; 3=32 bit AO event with time; 4=16 bit AO event with time; 5=float AO event; 6=double AO event; 7=float AO event with time; 8=double AO event with time.
An In Evt Mod	0=0:SOE 1=1:Most Recent			0=0:SOE	Analog Input Event Mode - 0: Sequence of Events, 1: Most Recent
Prtl Customization	0...2147483647		1	0	Customization parameter. Please, refer to the protocol manual.

4.2 Secure communication parameters

4.2.1 DNP 3.0 Secure settings

Table 10: Non group settings

Parameter	Values (Range)	Unit	Step	Default	Description
Protocol Security Mode	1=App. authentication 2=TLS and appl. auth.			0=Off	Protocol Security Mode - 0: Off; 1: Aplication authentication; 2: TLS and

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
	0=Off				Aplication authentication
Aggressive mode enable	1=Disable 2=Enable			1=Disable	Aggressove mode - 1: disable; 2: enable
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 indicate 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
Max Authn Fail Thres	1...65535		1	5	Maximum authentication failures threshold
Max Reply Tm Thres	1...65535		1	3	Maximum reply timeouts threshold
Max Authn Rekey Thres	1...65535		1	3	Maximum authentication rekeys threshold
Max Err Msg Tx Thres	1...65335		1	10	Maximum error messages sent threshold
Event Class Obj 122	1=1 2=2 3=3 4=1&2 5=1&3 6=2&3 7=1&2&3			1=1	Event Class for Obj 122
Default Var Obj 122	1=32bit SecStat evt 2=32bit SecStat evt&time			1=32bit SecStat evt	1=32bit Secure Statistics event; 2=32bit Secure Statistics event with time
Clear User List	0=False 1=True			0=False	Clear DNP Secure authentication User List

4.2.2 DNP 3.0 Secure statistics thresholds settings

Table 11: 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

Table continues on the next page

Parameter	Values (Range)	Unit	Step	Default	Description
Rekeys Authn failure	1...65535		1	3	Security statistics threshold for rekeys 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
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

4.3 Monitored data, general

4.3.1 DNP 3.0 Monitored data

Table 12: 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
Mapping errors	INT32	-1...2147483646		Mapping errors

4.4 Monitored data for secure communication

4.4.1 DNP 3.0 Secure monitored data

Table 13: 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
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

Table continues on the next page

Name	Type	Values (Range)	Unit	Description
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

5 Glossary

ACD	Start/pickup status
ACT	1. Application configuration tool in PCM600 2. Trip status in IEC 61850
AI	Analog input
Beh	Behavior
BI	Binary input
BO	Binary output
CA	Certification authority
CRC	Cyclical redundancy check
CROB	Control relay output block
Data set	The content basis for reporting and logging containing references to the data and data attribute values.
DIP switch	A set of on-off switches arranged in a standard dual in-line package
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DPC	Double-point control
EIA-485	Serial communication standard according to electronics industries association
EMC	Electromagnetic compatibility
EPA	Enhanced performance architecture
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN.
FIFO	First in, first out
HMI	Human-machine interface
IEC	International electrotechnical commission
IEC 60870-5	IEC standard for telecontrol equipment and systems. Part 5 defines transmission protocols.
IEC 61850	International standard for substation communication and modeling.
IED	Intelligent electronic device
IP	Internet protocol
IP address	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/IP protocol.
ISO	International Standard Organization
MMS	1. Manufacturing message specification 2. Metering management system

OSI	Open systems interconnection
PCM600	Protection and control IED manager
REX640	Protection and control relay
RS-485	Serial link according to EIA standard RS485
RTU	Remote terminal unit
SBO	Select-before-operate
SI	Sensor input
SPC	Single-point status of a controllable object
SPS	Single-point status
ST	Connector type for glass fiber cable
TCP	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TLS	Transport layer security
UDP	User datagram protocol
UR	Unsolicited response

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

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

1MRS759119 D