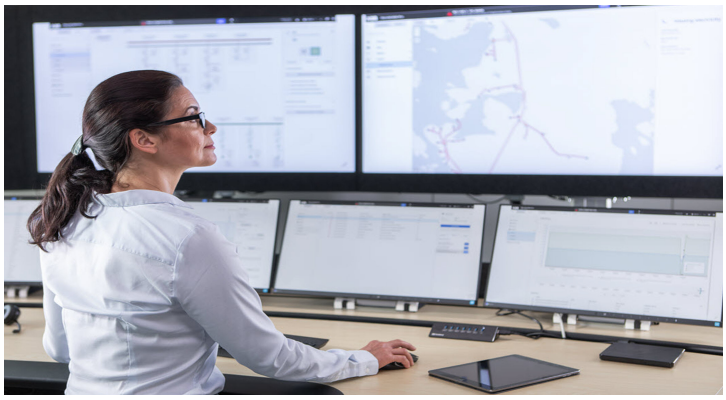
GRID AUTOMATION PRODUCTS

MicroSCADA X SYS600 10.2

IEC 60870-5-104 Master Protocol



Document ID: 1MRK 511 492-UEN
Issued: March 2021
Revision: A
Product version: 10.2

Table of contents

Section 1 Copyrights

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Power Grids. Hitachi Power Grids assumes no responsibility for any errors that may appear in this document.

In no event shall Hitachi Power Grids be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Power Grids be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Power Grids, and the contents thereof must not be imparted to a third party nor used for 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 is a registered trademark of ABB Asea Brown Boveri Ltd. Manufactured by/for a Hitachi Power Grids company. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

Please inquire about the terms of guarantee from your nearest Hitachi Power Grids representative.

Third Party Copyright Notices

List of Third Party Copyright notices are documented in "3rd party licenses.txt" and other locations mentioned in the file in SYS600 and DMS600 installation packages.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (https://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Section 2 Introduction

2.1 This manual

This manual provides thorough information on the use of IEC 60870-5-104 Master Protocol and information related to it. It describes how to configure the base system and the communication system to establish communication to IEC 60870-5-104 slave devices.

In addition to this configuration, the base system needs to be configured for data storage and processing. For information on this subject, see other manuals, for example, SYS600 Application Objects and SYS600 System Objects.

2.1.1 IEC 60870-5-104 Master Protocol

The IEC 60870-5-104 Master protocol is used in LAN and WAN networks to connect central stations and substations to each other. Figure 1 shows the communication between SYS600 and a Substation Control System (SCS).

This protocol can also be used for communication between SYS600 and a remote-controlled line disconnector.

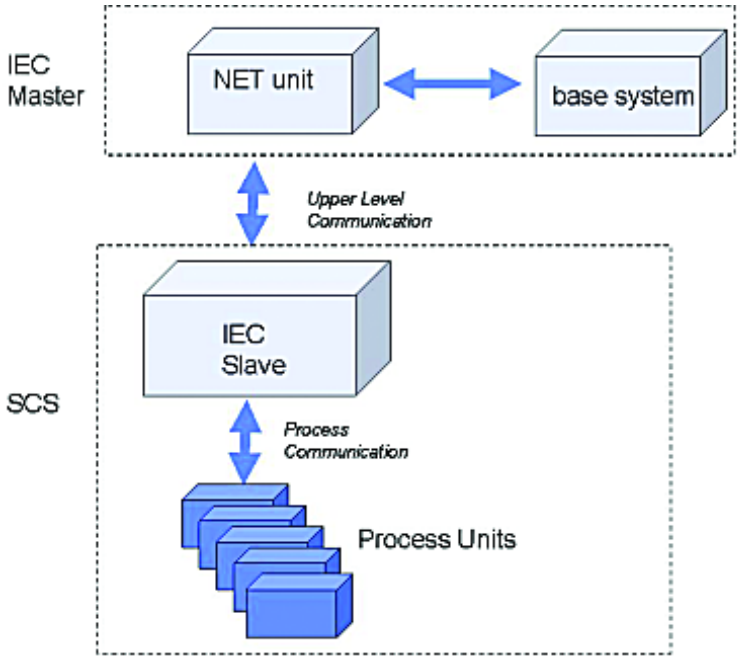


Figure 1: The IEC master sees the Substation Control System (SCS) as an IEC slave

2.2 Use of symbols

This publication includes warning, caution and information symbols where appropriate to point out safety-related or other important information. It also includes tips to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

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

Caution icon indicates important information or a 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/property.

Information icon alerts the reader to relevant factors and conditions.

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

Although warning hazards are related to personal injury, and caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warnings and caution notices.

2.3 Document conventions

The following conventions are used for the presentation of material:

- The words in names of screen elements (for example, the title in the title bar of a dialog, the label for a field of a dialog box) are initially capitalized.
- Capital letters are used for file names.
- Capital letters are used for the name of a keyboard key if it is labeled on the keyboard. For example, press the CTRL key. Although the Enter and Shift keys are not labeled, they are written in capital letters, for example, press ENTER.
- Lowercase letters are used for the name of a keyboard key that is not labeled on the keyboard. For example, the space bar, comma key and so on.
- Press CTRL+C indicates that the user must hold down the CTRL key while pressing the C key (in this case, to copy a selected object).
- Press ALT E C indicates that the user presses and releases each key in sequence (in this case, to copy a selected object).
- The names of push and toggle buttons are boldfaced. For example, click **OK**.
- The names of menus and menu items are boldfaced. For example, the **File** menu.
    - The following convention is used for menu operations: **Menu Name/Menu Item/ Cascaded Menu Item**. For example: select **File/Open/New Project**.
    - The **Start** menu name always refers to the **Start** menu on the Windows Task Bar.
- System prompts/messages and user responses/input are shown in the Courier font. For example, if the user enters a value that is out of range, the following message is displayed: `Entered value is not valid`.
  The user may be told to enter the string MIF349 in a field. The string is shown as follows in the procedure: `MIF349`
- Variables are shown using lowercase letters: sequence name

2.4 Related documents

The following SYS600 manuals should be available for reference during the use of this manual:

Name of the manual	Document ID
SYS600 10.2 IEC 60870-5-101 Master Protocol	1MRK 511 489-UEN
SYS600 10.2 IEC 60870-5-104 Slave Protocol	1MRK 511 493-UEN
SYS600 10.2 System Configuration	1MRK 511 481-UEN
SYS600 10.2 System Objects	1MRK 511 482-UEN
SYS600 10.2 Application Objects	1MRK 511 467-UEN

2.4.1 Other referenced manuals

The IEC 60870-5-104 protocol is based on the following documents by the IEC Technical Committee 57:

IEC 60870-5-1	Transmission Frame Formats
IEC 60870-5-2	Data Link Transmission Services
IEC 60870-5-3	General Structure of Application Data
IEC 60870-5-4	Definition and Coding of Information Elements
IEC 60870-5-5	Basic Application Functions
IEC 60870-5-101	Companion standard for the IEC 60870-5-101 Protocol
IEC 60870-5-104	Companion standard for the IEC 60870-5-104Protocol

2.5 Document revisions

Revision	Version number	Date	History
A	10.2	31.03.2021	New document for SYS600 10.2

Section 3 Safety information

This section has information on the prevention of hazards and taking backups from the system.

3.1 Backup copies

3.1.1 Taking backup copies

We recommend taking backup copies before making any changes, especially ones that might have side effects. Software and data need to be copied to another place.

Backup copying makes it easier to restore the application software in case of disk crash or other severe failure where stored data is lost. It is therefore recommended that backup copies are taken regularly.

There should be at least two system backup copies and two application copies. A new backup is copied over the oldest backup. This way the latest version is always available, even if the backup procedure fails.

Detailed information on how to take backup copies should be delivered to the customer with the application.

3.1.2 System backup

Usually a system back up is taken after the application is made. It should be taken again when changes are made to the SYS600 system. This is required when the driver configuration or the network setup is changed.

3.1.3 Application backup

An application backup is also taken at the same time with the system backup, after the application is made. It should be taken again when changes are made to the application, for example, if pictures or databases are edited or new pictures are added.

3.2 Fatal errors

A fatal error is an error that causes a breakdown or a locked situation in the SYS600 program execution.

3.2.1 Handling

In case of a fatal error:

1. Write down the possible SYS600 error messages.
2. Shut down the SYS600 main program. If this cannot be done in the SYS600 Control Panel, try to end the task in Windows Task Manager.

Files may be damaged if the base system computers are shut down by switching the power off.

3. The data kept in the main memory at the moment of a fatal error is placed in the drwtsn32.log file with Windows 2003 Server, Windows XP and earlier. By default, it is placed under %SYSTEMDRIVE%\Documents And Settings\All Users\Application Data \Microsoft\Dr Watson. Log and dump file paths can be checked with the drwtsn32 application. (Start -> run -> drwtsn32.exe). Analyze and copy the data in these files. Starting with Windows Server 2008 and Windows 7 the crash handling has changed. The location of the dump files can be read from the registry under the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting \LocalDumps. The DumpFolder value tells the location of the dump files. Collect the data from this location.
4. Restart the system.

Report the program break-down together with the possible SYS600 error messages and the information from the drwtsn32.log file to the SYS600 supplier.

3.2.2 Status codes

Error messages in SCIL are called status codes. A list of status codes and short explanations for them can be found in SYS600 Status Codes.

Section 4 Instructions

4.1 Communication

In SYS600 the IEC 60870-5-104 Master protocol is implemented only in the PC-NET software. PC-NET unit communicates over an INTEGRATED link and via the Ethernet ports of the base system computer.

Setting the attributes of SYS600 system objects can modify the communication parameters.

The base system sees each IEC device as a station (STA object) that has been created to a line of a NET unit. Each IEC station works as a protocol converter that converts data between the internal protocol of SYS600 and the IEC 60870-5-104 protocol.

4.2 Installation

The SYS600 installation is required.

4.3 Configuration

Configuration can be made either by using the System Configuration Tool or by using SCIL statements. For more information on the System Configuration Tool, see SYS600 System Configuration manual, chapter "PC-NET start-up with System Configuration Tool" and "System Configuration Tool". The usage of the System Configuration Tool is recommended, but if there is a need to create the communication configuration using SCIL, it is instructed in the following chapters. In this case, the configuration can be divided into two parts:

The configuration can be divided into two parts:

- Base system configuration
- Communication system configuration

The attribute descriptions presented in chapter 'Communication system configuration' are the same for configurations created with System Configuration Tool or with SCIL.

4.3.1 Base system configuration

It is assumed here that the base system configuration for objects other than the communication has been made according to the instructions in the System Configuration manual.

The extra steps needed to configure the communication are:

1. Define a node number for a PC_NET instance.
2. Reserve a link number for a PC_NET instance. Creating the link as instructed in step 6 starts the PC_NET instance.
3. Create the base system STA object for each remote IED (master function) or for each NCC connection (slave function).
   - IEC 60870-5-104 Master protocol uses the station type IEC (STY type 29)

   The STA objects are created to SYS_BASCON.COM using the template or with a separate creation sequence. If the template is not used, the sequence should contain the line:

```
#create STA'Sta_Nb':B = %Sta
```

where 'Sta_Nb' is the number of the station object in the base system. %Sta is a list object which should contain at least the following settings: TT = "EXTERNAL", ST = station type, ND = node number defined in step 1 and TN = translated object number (usually the same as 'Sta_Nb'. See SYS600 System Objects manual for more information on the base system object attributes for STA object).

4. Edit the PC_NET.CF1 according to the description in chapter "Start-up definition file PC_NET.CF1" in the SYS600 System Configuration manual
5. Create a command procedure which creates the lines and stations to the NET object (= pc_net instance) using the S-attributes.
   See Section 4.3.2 for more information on the attribute setting. A sample creation script is presented at the end of this manual.
6. Create a command procedure which creates the link of type 'INTEGRATED' to the base system. This procedure should contain the line:

   ```
   #set LIN'i_Integrated_Link_Number':BLT = "INTEGRATED"
   ```

   where 'i_Integrated_Link_Number' is the number of the link reserved in step 2. The PC_NET executable is defined with the SC attribute of the link and it must set before setting of the LT attribute.

The testing of the communication system can be done as follows:

1. Execute the procedure created in step 6. This starts the PC_NET instance and enable the setting of the S-attributes.
2. Execute the procedure created in step 5. If the lines and stations are set to IU = 1 (that is, they are in use) and the configuration is correct and complete in both ends, the communication starts.

For automatic start-up of the communication, the created command procedures must be attached to the APL_INIT_1:C procedure.

4.3.2 Communication system configuration

Each NET instance contains a set of system objects which specify the existence and the usage of the communication lines and the station objects connected to those lines. These objects can be created, modified, and deleted by SCIL, and setting the attributes defines the functionality of these objects.

Access to the attributes can be one of the following:

- **Read-only**: The attribute can only be read. There are still a few exceptions in which the values can be reset.
- **Write-only**: The attribute can only be written (set).
- **Read, conditional write**: The attribute can be both read and written, but the object must be set out of use (IU = 0) before writing.
- **No limitations**: The attribute can be both read and written without limitations.

The configuration of the communication system in SYS600 can be divided into two layers: line layer and station layer. Both of these layers have a specific functionality and a set of attributes of their own.

The purpose of the communication system configuration is to:

- Create all the system objects needed to establish communication between the master and the slave. Related attributes for creation are PO (Line) and DV (Station).
- Adjust the values of the system object attributes to match the physical communication channel and the properties of the remote partner/partners. The menu selection

'Configuration->Preview->PC_NET' in the System Configuration Tool may provide an example of the SCIL based configuration script of any setup.

4.3.2.1 Setting the attribute values

All the line and station attributes have sensible default values, but the value of each attribute must be checked against the requirements of the actual communication system.

The attribute values depend on:

- The physical communication media (for example leased telephone line, radio link, power line carrier), which affects the attributes of the line, such as the baud rate and parity.
- The network topology used (point-to-point, multi-drop), which affects the link type.
- The size (number of stations) of the system, which affects the timeout parameters; the slower the media and larger the system, the longer timeouts are needed.
- The remote system(s), which affects both the line and station attributes, and the message types used.

4.3.2.2 Network topologies

The IEC 60870-5-104 master protocol in MicroSCADA uses the Ethernet connection, and IEC60870 slaves communicate with a master using TCP/IP. One or more slaves in different IP-address can be connected to one master. Figure 2 illustrates the multidrop network topology.

As default, IEC60870-5-104 master establishes one TCP/IP connection to the each IED operating as a IEC60870-5-104 slave. It is also possible that the same TCP/IP connection is shared by multiple logical remote units (LRUs). In this case there must be a separate STA object for each LRU. The LRUs are identified using station attribute SA (Common Address of ASDU) and the IP address is defined with the station attribute IA.

If multiple connections are needed, for example, across different LANs, the redundancy extensions defined with line attribute LD and station attribute IA can be used. If there are two LANs which are accessing the same IEDs, at least two logical connections are needed for each IED. If there are two LANs which are accessing IEDs operating as a hot-standby pair, the recommended amount of logical connections is four. In a redundancy configuration, the connection which is used in data transfer is selected using the station attribute AC.

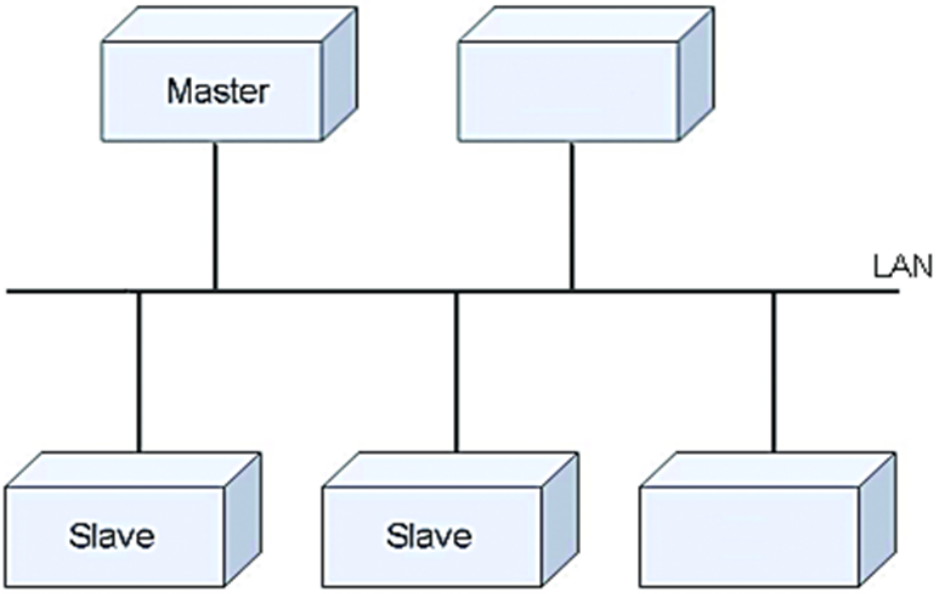


Figure 2: Multidrop network topology

When making the IEC connection, an agreement about the used communication parameters should be made with the supplier or owner of the master system.

4.3.2.3 IEC 60870-5-104 line layer

The line process of a NET unit performs the functions of the line layer. The purpose of the line layer is to send and receive messages to/from external devices using the IEC 60870-5-104 protocol.

According to the IEC 60870 standards, the line layer performs the following functions:

- Provides access to the transmission medium. For example, TCP/IP.
- Recognizes frames addressed to a designated station.
- Reports on persistent transmission errors.
- Reports on the status of link configuration.
- Supports initiation and maintenance functions.

Line layer attributes
The following attributes can be used for configuring IEC 60870-5-104 master lines in SYS600.

IU	In Use
Indicates whether the line is in use (value 1) or not in use (value 0).	
Data type:	Integer
Value:	0 or 1
Index range:	1...12 (NET line numbering)
Default value:	0
Access:	No limitations

LD	Local Address

The IP address that is used locally. It is necessary to set this attribute when the computer has multiple IP addresses and it is defined which address the created line must use. This attribute must be set before the line has been taken into use for the first time. An empty string in LD means that the default IP address of the computer is used. The value of LD cannot be modified after the line has been taken into use for the first time. Multiple IP addresses can also be given to support redundancy, refer to the station attributes IA and AC.

Data type:	Text
Value:	String containing a valid IP address, max 230 characters.
Default value:	Empty string
Index range:	1... 12 (NET line numbering)
Access:	Read, conditional write

This attribute accepts the IP address in form:

```
#SET NET1:SLD1="192.168.1.10"
```

If multiple IP addresses have to be assigned for redundancy purposes, separate the addresses with a space, for example

```
#SET NET1:SLD1="192.168.1.10 192.168.1.20 192.168.1.30"
```

There is an internal limitation which prohibits the use of the same local IP address and the same line number multiple times. This applies to all PC_NET protocols using LAN.

Example:

It is not possible to have

IEC104 master in Line 1 in PC_NET 1 with LD="192.168.1.1"

and

DNP3.0 slave in Line 1 in PC_NET 2 with LD="192.168.1.1"

the configuration must be changed to

IEC104 master in Line 2 in PC_NET 1 with LD="192.168.1.1"

and

DNP3.0 slave in Line 1 in PC_NET 2 with LD="192.168.1.1"

or to

IEC104 master in Line 1 in PC_NET 1 with LD="192.168.1.1"

and

DNP3.0 slave in Line 1 in PC_NET 2 with LD="192.168.1.2"

The limitation is present only when the same local IP address is used. An easy workaround is to configure multiple IP-addresses which are using the same adapter. If this is not possible, setting a unique value for the NET node attribute LP redefines the internally used ports for the NET node and no conflict takes place. See SYS600 System Objects manual for more information about the NET Node attribute LP.

PO	Protocol

The data transfer protocol used on the line. The line is defined to the NET by setting this attribute. By setting the attribute to 0 the line definition including all the line attributes are deleted.

Data type:	Integer
Value:	0...45 Value with IEC 60870-5-104 Master protocol: 44 (Controlling station)
Index range:	1...12 (NET line numbering)
Access:	Read, conditional write

PS	Buffer Pool Size

Specifies the number of message buffers reserved for the line. Fixed buffer poll sizes are used in versions 9.3 FP1 and newer and this attribute is retained because of the backward compatibility. Setting the value for PS is not possible anymore. See the attributes PS, NB and PB from the System Objects manual for more information.

Data type:	Integer
Value:	1...250
Index range:	1...12 (NET line numbering)
Access:	Read (conditional write accepted but has no effect)

PD	Polling Delay

The delay between the communication test polling messages U(TESTFR) (as described in the IEC 60870-5-104 standard). If no transmission occurs within the time specified with this attribute, the frame U(TESTFR) is sent (t3). No test poll is sent when the value is 0.

Data type:	Integer
Value:	0... 255
Unit:	Seconds
Index range:	1... 12 (NET line numbering)
Default value:	20 s
Access:	Read, write

HT	Connect Timeout

This attribute defines the timeout of the TCP Connect operation. This attribute is meaningful especially in multidrop configurations, since no other station is served while the master is connecting to an unconnected station. The value of this attribute may depend on the network structure and load, station count, etc. The value should be defined together with the value of the ET attribute of the station object(s). Value 0 means that a blocking Connect is used. In this case, the used timeout value depends on the used TCP/IP stack implementation.

Data type:	Integer
Value:	0...65535
Unit:	Milliseconds
Default value:	1000
Access:	Read, conditional write

TI	Response Timeout

The time in seconds that the IEC link waits for the response to sent messages. If no acknowledgment is received within this timeout, the station closes the connection (t1) (as described in the IEC 60870-5-104 standard).

Data type:	Integer
Value:	0...255

Table continues on next page

TI	Response Timeout
Unit:	Seconds
Index range:	1...12 (NET line numbering)
Default value:	15 s
Access:	Read, Write

EN	Enquiry Limit

The Enquiry Limit attribute defines the amount of consecutive unsuccessful TCP connection attempts before the status of the IED is set to the SUSPENDED state. Values bigger than 0 provide a possibility to filter out occasional suspensions caused by network errors. The connection attempt is treated as successful when the IED has responded to a "start dt act" message with "start dt con". If the TCP disconnections are continuous, it is recommended to extract the reason for these instead of using values bigger than 0 in the EN attribute. The value of EN applies to all station objects connected to a line.
The TCP connection message can also be retransmitted by the TCP stack of the operating system.

Data type:	Integer
Value:	0...3
Index range:	1...12 (NET line numbering)
Default value:	0
Access:	Read, conditional write

MI	Message Identification

Object address of system messages.

Data type:	Integer
Value:	1...32760
Index range:	1...12 (NET line numbering)
Default value:	6000 + (100 * NET number) + line number
Access:	Read, conditional write

MS	Message Application

The number of the application that is the receiver of the system messages generated by the line.

Data type:	Integer
Value:	1...250
Default value:	1
Index range:	1...12 (NET line numbering)
Access:	Read, conditional write

DC	Diagnostic Counters

The line protocols gather statistical information about the events on the lines by incrementing a number of diagnostic counters. All the major events and error situations of the communication have their own counters. When accessing diagnostic counters, the attribute is indexed according to the formula:
100 * (line number) + (diagnostic counter number)
The IEC 60870-5-104 Master protocol supports the following counters:

1. Transmitted telegrams
2. Failed transmissions
4. Transmitted commands
5. Transmitted replies
6. Transmitted U (Unnumbered control function) format messages
7. Received I format messages
8. Received S format messages

Table continues on next page

DC	Diagnostic Counters
	9. Received U format messages
	11. Received messages
	12. TCP Connect count
	13. TCP Accept count
	14. TCP Close count
	15. Duplicates and losses
	16. Buffer overflow errors
Data type:	Integer
Value:	0...30000
Index range:	See above
Access:	Read-only, the values can be reset

OM	Operating Mode
A bit pattern which defines the operating mode of the line.	
Value:	See below
Default value:	0
Access:	Read, conditional write
Bit 0:	Process messages with invalid CAA. If this bit is 1 and the Common Address of ASDU (CAA) of the incoming message does not match any of the configured STAs for the IP address of the sender of the message, the message is passed for processing to the STA object, which is the first station which used the IP address in its IA. When System Configuration Tool is used, this STA number is the lowest STA number having the IA equal to the IP address of the sender of the message. The setting of this bit is necessary when the remote slave is a gateway which collects data from multiple IEDs that have separate CAAs, and there is no need to process all this data in the MicroSCADA application. If this bit 0, incoming messages with Common Address of ASDU (CAA) values that do not match the configuration are not processed.
Bit 1:	Ignore errors in application responses. If this bit is 1 and MicroSCADA application responds with errors indicating that the station configuration (STA:BTN) or the application numbers are incorrect, the responses are handled as valid responses. If this feature is used, the communication of the IEC60870-5-104 is normal but the received data may be lost. If the configuration of the MicroSCADA base system is correct, this bit is meaningless. If this bit is 0 and MicroSCADA application responds with errors, the data is buffered and the IEC60870-5-104 communication to the IED is interrupted until the configuration is valid again. This is the default mode of operation.

UI	UAL event Identification
The UI attribute is used to define the name for the line object, and it is used to identify the source of the UAL (user activity logging) events. This string is added to the identification information of all user activity events from this line object. A unique value within the node is preferred. The node level module name (also in attribute UI) is added to form the full identification information for the user activity event. If a line identifier is not needed, an empty string should be assigned to this attribute.	
Data type:	String
Value:	String containing a line level identifier with maximum length of 16 characters
Indexing:	1..12 (if not used, node attribute will be referred)
Default value:	”.LINEx”, where x = line number
Access:	Read, write

4.3.2.4 IEC 60870-5-104 station object

The main purpose of the station layer is the protocol conversion between the IEC 60870-5-104 and the internal protocol of SYS600. The station objects also take care of the application level communication with the slave.

The STA objects created in a NET unit perform the functions of the station object. Several STA objects of the type IEC devices are allowed on the same line. It is also possible that multiple stations share the same remote IP address. If a converter from IEC60870-5-101 to IEC60870-5-104 is used in the remote IP address, special configuration using the station object attribute CE and the line object attribute OM, bit 0 may be needed.

The STA objects created in a NET unit perform the functions of the station object. Some attributes are used for the station configuration and others are used for device communication. The configuration attributes are presented in this chapter and the communication attributes are presented in the next one.

Station objects can be configured to use secure authentication using the attributes described in chapter 'Authentication attributes'. IEC 60870-5-104 Secure Authentication is based on IEC technical specifications 62351-5 and 60870-5-7. Users and their roles and keys are created to slave device on-line with IEC 60870-5-104 using symmetric or asymmetric methods.

The databases for user sets and necessary keys are created using separate tools (see SYS600 System Configuration manual, chapter 'Secure authentication using IEC/TS 62351-5' for more information). This database is called "key storage" in the descriptions of the authentication attributes. The key storage which is used by the PC-NET instance is defined with NET Node attribute KS (see System Objects manual for a detailed description). Key storage file is always encrypted.

Chapter 'Security attributes' describes available options for communication encryption and certificate validation using TLS (Transport layer security). Functionality follows IEC technical specifications 62351-3 and 60870-5-7.

Station attributes
The following attributes can be used for configuring the IEC 60870-5-104 Master stations in SYS600. For compatibility reasons the attributes have been retained from the IEC 60870-5-101 standard.

IU	In Use
Indicates whether the station is in use (value 1) or not in use (value 0).	
Data type:	Integer
Value:	0 or 1
Default value:	0
Access:	No limitations

LI	Line Number
The number of the NET line the station is connected to.	
Data type:	Integer
Value:	1...12 (NET line numbering)
Access:	Read, conditional write

Setting this attribute is not needed, when the station is created by using the DV attribute.

SA	Station Address

The station address of the IEC 60870-5-104 station, the common address of ASDU in an IEC message.

Data type:	Integer
Value:	0...255 , when SL attribute = 1 0...65535, when SL attribute = 2
Default value:	1
Access:	Read, conditional write

IA	Internet Address

The IP address or the hostname of the remote host. The connection is established with the slave device in this address by connecting to port number 2404 in the slave device.
A unique set of IA values form a redundancy group. If multiple STA objects are using exactly same set of IA values, same TCP connection is used to transfer data with multiple Common Address of ASDUs. Changing the active connection (attribute AC) on one STA object has an effect on all STA objects within the same redundancy group. If one STA object has unique IA values, it is a redundancy group using one Common Address of ASDU only.

The line needs to have been taken into use at least once before writing to this attribute.

Value:	Any string, max 29 characters
Index:	1...12 (optional, defines the connection number)
Access:	Read/write

When written, this attribute accepts the IP address in the following form:

```
#SET STA1:SIA=”192.162.1.120”
```

or as an alias name:

```
#SET STA1:SIA=”GRACE”
```

When an alias name is used, it must be defined in the TCP host file: %windir\system32\drivers \etc\hosts.

In case there is a need to assign multiple IP addresses for the redundancy purposes, the addresses must be given with an index. Each given index defines a logical connection.

If the remote slave device uses a non-standard port for communication, it can be specified as follows:

```
#SET STA1:SIA="192.168.1.11;2405" ; remote device uses port 2405
```

No spaces are allowed between the address and the port number. The port number must be in the range 1..65535.

Examples:

#SET STA1:SIA1="192.168.1.11:2"

Defines that the first logical connection of STA1 is defined to be to/from the IP address using the second local address given with line attribute LD.

A setup in which there are four logical connections to master and two local IP addresses connected to two separate LANs would result following configuration:

```
#SET NET1:SLD1="192.168.1.10 192.168.1.20" ; first LAN second LAN
.
.
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.12:1"
```

```
#SET STA1:SIA3="192.168.1.21:2"
#SET STA1:SIA4="192.168.1.22:2"
```

If the logical connections are using the same IP addresses but non-standard TCP ports, the configuration could be:

```
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.11;2405:1" ;server in non-standard port 2405
#SET STA1:SIA3="192.168.1.21:2"
#SET STA1:SIA4="192.168.1.21;2405:2" ;server in non-standard port 2405
```

The port number must be given before the index of the local address, no spaces allowed.

SL	Station Address Length

The length of the station address (common address of ASDU) in octets.

Data type:	Integer
Value:	1 or 2
Default value:	2
Access:	No limitations

The default values of the SL, IL and CL attributes follow the IEC 60870-5-104 standard. It is strongly recommended to use these values, otherwise compatibility cannot be guaranteed.

IL	Information Address Length

The length of the information object address in octets.

Data type:	Integer
Value:	1...3
Default value:	3
Access:	Read, conditional write

CL	Length of Cause of Transmission Information

The length of the cause of transmission field in an IEC 60870-5-104 message in octets.

Data type:	Integer
Value:	1 or 2
Default value:	2
Access:	No limitations

AL	Allocation

Allocates the station to an application. When the AL attribute has the value 1, the station is reserved by the application specified by the AS attribute. All spontaneous messages from the station are sent to this application.

Data type:	Integer
Value:	0 or 1
Access:	No limitations

AS **Allocating Application**

Specifies the allocating application of the station (see the AL attribute). The allocating application gets all spontaneous process data from the station. This application is also the only one that is allowed to set the device communication attributes.

Data type:	Integer
Value:	0...250, 0 = no application
Access:	Read-only, conditional write

When the AL attribute is set to 0, AS also gets the value 0.

MI **Message Identification**

Object address of system messages.

Data type:	Integer
Value:	1...32760
Default value:	29000 + station number
Access:	No limitations

MS **Message Application**

The number of the application, that is the receiver of the system messages generated by the station.

Data type:	Integer
Value:	1...250
Default value:	1
Access:	No limitations

SE **System Messages Enabled**

Specifies whether the system messages generated by the NET and related to the station are sent to applications (value 1) or not (value 0). By using this attribute, it is possible to disable the system messages related to the station.

Data type:	Integer
Value:	0 or 1
Default value:	1
Access:	No limitations

CA **Command Address**

The object address of the bit stream process object in the SYS600 process database, where unidentified messages are sent. If the value of the CA attribute is 0, the address of the updated bit stream process object is the first IOA (information object address) of each received unknown message.

Data type:	Integer
Value:	0...65535
Default value:	32000
Access:	No limitations

The unit number (UN attribute) of the bit stream process object must be the same as the STA object number.

ML **Maximum Message Length**

The maximum length of a transmitted message in octets.

Data type:	Integer
Value:	20...255
Default value:	230
Access:	No limitations

In practice, this attribute is meaningless in the IEC 60870-5-104 master. The length of the incoming messages can always be at their maximum.

CF **ConFirmation Mode**

The wait for the activation termination message. With value 0, the timer defined with the CT attribute is not started. Value 0 is needed with some IEC 60870-5-104 Master implementations, which do not send activation termination messages at all.

Data type:	Integer
Value:	0 = Activation termination is not waited 1 = Activation termination is waited
Default value:	1
Access:	No limitations

RM **Running Mode**

Consists of a set of flags that control the behavior and functionality of the IEC Master station. Each flag is one bit of this attribute. The bits are as follows:

Bit 0:	The hour transmission method of events to the master. When this bit is 0, the master gets the year, date and hour from the slave as an hourly clock synchronization (ASDU 103). When this bit is 1, the master adds the year, date and hour from its internal clock to the events. Minutes and seconds should be provided in time-tagged events by the slave.
Bit 3:	Handling of unrecognized commands. When this bit is 0, unrecognized command messages are ignored. When this bit is 1, unrecognized messages sent by the slave are forwarded to a bit stream process object with an address as defined by the CA attribute.
Bit 4:	Sending of the general interrogation command when the master receives ASDU 70. When this bit is 0, a general interrogation command is always sent when the end of initialization message (ASDU 70) is received from the IEC slave. When this bit is 1, a general interrogation is not sent automatically when receiving ASDU 70.
Bit 5:	Sending of the general interrogation command when the master gets the zero (OK) status. When this bit is 0, a general interrogation command is always sent when the object status of the IEC master station gets the value zero, for example, when it is set in use or after a suspension. When this bit is 1, a general interrogation is not sent automatically at zero status.
Bit 6:	Parallel commands. When this bit is 1, sending parallel commands is possible. The control is returned immediately back to SCIL and the return status of a command must be checked from the command termination process object. When this bit is 0, sending another command is not possible before the previous command has been completed or a confirmation timeout has occurred. This is the default way of operation.
Bit 7:	Private ASDU handling. When this bit is 1, the private range ASDUs 146, 148 and 160 are handled as unknown ASDUS. The contents of these ASDUs are sent to a bitstream process object, if the bit 3 of RM is set. When bit 7 is 0, the ASDUs are interpreted in the following way: ASDU 146 is similar to ASDU 30, single point information with full time tag ASDU 148 is similar to ASDU 31, double point information with full time tag ASDU 160 is similar to ASDU 37, integrated totals with full time tag

Data type:	Integer
Value:	0...65535, see above
Default value:	0
Access:	Read, conditional write

Example:

Enable general interrogation at zero status and disable other features, RM value = 0*8+0*16+1*32=32.

DC **Diagnostic Counters**

The values of the diagnostic counters which the NET unit keeps for the station. The counters have the following meaning:

1. Suspension information (0 = OK, 1 = suspended)
2. Suspension counter
3. Transmitted data messages
4. Transmitted command messages
5. Transmitted confirmation messages
6. Received data messages
7. Received command messages
8. Received confirmation messages
9. Received unknown messages
10. Received too long messages
11. Link timeouts
12. TCP connects
13. TCP accepts
14. TCP accepts
15. Application response timeouts

Data type:	Integer
Value:	1...65535
Index range:	1...15
Access:	No limitations

OS **Object Status**

The current status of the IEC station object. When value 1 is written to this attribute, the station object retransmits its current status code to the system message process object.

Data type:	Integer
Value:	when Read, 0 = OK_STATUS or non-zero value = communication is not normal at the moment
Access:	No limitations (write is possible only with value 1)

ST **SYS Waiting Time**

The maximum time that the slave station waits for a reply from the base system.

Data type:	Integer
Value:	0...60000
Unit:	Milliseconds
Default value:	5000
Access:	No limitations

RT **Activation Reply Timeout**

The maximum time the IEC master station waits for an activation confirmation message from the IEC slave.

Data type:	Integer
Value:	0...255

Table continues on next page

RT	Activation Reply Timeout
Unit:	Seconds
Default value:	10
Access:	No limitations

CT	Activation Termination Timeout

The maximum time the IEC master station waits for an activation termination message from the IEC slave.

Data type:	Integer
Value:	0...255
Unit:	Seconds
Default value:	60
Access:	No limitations

CE	Connection Event

Defines the information object address of the data item which is used to indicate the connection loss or recovery to the logical remote unit. The usage of this feature is needed when the actual IED is connected through a gateway or a converter, and the converter reports the connection state with a separate data message. If the information object address defined with CE (index=1) is non-zero and the data value in the message matches the given value (index=2) meaning "connected", the station object is reported to be RUNNING. All other values cause reporting of SUSPENDED and process objects are set to OS=2 state. If the information object address defined with the CE index 1 is 0, this feature is not used (default behavior). The mode defined with index 3 controls whether command sending is allowed to the suspended station or the automatic GI is sent when the station object is taken into use. Any ASDU type used to transfer analog or binary data can be used, but the possible timestamp in the message is not used.

Value: 0..16777215

Indexing
1: Information object address of the data (0=feature not used)
2: Value meaning 'connected'
3: Mode as bit pattern

Bit 0 = 0 : Commands from application are not allowed when station is suspended because of the connection event
Bit 0 = 1 : Commands from application are allowed when station is suspended because of the connection event
Bit 1 = 0 : If automatic GI is enabled, it is sent when STA is taken into use even though the STA has been suspended because of the connection event
Bit 1 = 1 : Although automatic GI is enabled, it is not sent when STA is taken into use and it has been suspended because of the connection event
Bit 2 = 0 : Station is not set to running state if process data is received when the station has been suspended because of the connection event
Bit 2 = 1 : Station is set to running state if process data is received when the station has been suspended because of the connection event

4: Initial status of the station (until reported by the converter)

0 = Running
1 = Suspended

Default values:

1: 0 (=feature not used)
2: 0 (=value = 0 means 'connected')
3: 0
4: 0 (= connection to the station is ok when connection to the converter is established)

Access: No limitations

Example 1:

```
#SET STA1:SCE1 = 20000 ; data item with IOA=20000, default value = 0
means 'connected'
```

Example 2:

```
#SET STA1:SCE1 = 5001 ;data item with IOA=5001,
#SET STA1:SCE2 =1 ;value = 1 means 'connected'
#SET STA1:SCE3 =6 ;automatic GI is not sent when STA:SIU->1, next data
sets to RUNNING
#SET STA1:SCE4 =1 ;status is SUSPENDED until reported by converter (or
data is received, index 3 bit 2 is set)
```

AT **Acknowledge Timeout**

The timeout for sending an acknowledgement, if the amount of APDUs defined by the UR attribute is not received. The timer is restarted when an APDU is received and cancelled when an acknowledge is sent (t2) (as described in the IEC 60870-5-104 standard). If no index is given, the currently active logical connection is accessed.

Value:	1... 255 s
Index:	1..12 (optional, defines the connection number)
Unit:	Seconds
Access:	Read/Write
Default:	10 s

SU **Summer Time**

States whether summer time is used or not.

Data type:	Integer
Value:	0 or 1
Default value:	0 (summertime not used)
Access:	No limitations

US **Unacknowledge Send**

The count of unacknowledged APDUs stored in the transport layer. The transport layer accepts the ASDUs from the station object up to this amount before the acknowledgement from the remote host must take place (k) (as described in the IEC 60870-5-104 standard). If no index is given, the currently active logical connection is accessed.

Value:	1... 65535
Access:	Read/Write
Index:	1..12 (optional, defines the connection number)
Default:	12

UR **Unacknowledge Receive**

The count of unacknowledged APDUs forwarded to the station object but not yet acknowledged to the remote host. The transport layer receives the APDUs from the remote host up to this amount before an acknowledgement is sent to the remote host (w) (as described in the IEC 60870-5-104 standard). If no index is given, the currently active logical connection is accessed.

Value:	1... 65535
Index:	1..12 (optional, defines the connection number)
Access:	Read/Write
Default:	8

If there are communication problems, try to set the values of the US and UR attributes to 1.

In order to get the optimized ratio for the limits of unacknowledged messages sent to the master and received messages by the slave, the size of the received messages should be 2/3 of the size of sent messages (k/w).

ET	REconnecting Timeout

The interval or reconnecting attempt while communication is not established. If no index is given, the currently active logical connection is accessed.

Value:	1... 255 s
Unit:	Seconds
Access:	Read/Write
Default:	30 s
Index:	1...12 (optional, defines the connection number)

The value of this attribute has to be bigger than the value of the HT attribute.

AC	Active Connection

Indicates which of the logical connections defined with the index of the IA attribute is active. Value 0 means that none of the configured connections are active. The connection is switched automatically if redundancy priorities has been set using attribute RP. If automatic selection is not used, connection selection should be made from the SCIL application by setting the value of the AC attribute. When connection is selected using attribute AC, selection is locked to this connection and automatic selection is not enabled until value 0 is written to AC. Attribute LC indicates whether the connection is locked or not.

Value:	Integer (0...12), value 0 enables automatic selection
Index:	No
Access:	Read, write

Example:

```
#SET NET1:SLD1="192.168.1.10 192.168.1.20"
; first LAN second LAN
.
.
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.12:1"
#SET STA1:SIA3="192.168.1.21:2"
#SET STA1:SIA4="192.168.1.22:2"
```

When STA1:SAC returns 3, it means that the data transmission takes place to address 192.168.1.21 using local address 192.168.1.20.

If value 1 is written to STA1:SAC, the data transmission is locked to use the remote address 192.168.1.11 and the local address 192.168.1.10. It should be noted that the logical connections do not need to access the same physical device but may also access a hot-standby pair or IEDs. See attribute RP how this is configured when automatic connection selection is used.

All STA objects within the same redundancy group use same logical connection for data transmission.

There may be only one connection from the one IP address in slave to one IP address in master. This means that it is not possible to have:

```
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.11:1"
```

but it is possible to have:

```
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.11:2"
```

and (as mentioned before):

```
#SET STA1:SIA1="192.168.1.11:1"
#SET STA1:SIA2="192.168.1.12:1"
```

CS	Connection State

Indicates the state of the specified logical connection. The given index refers to the connection number specified with IA attribute. The returned values are same for all STA objects within one redundancy group.

Value:	0 = Connection is undefined 1 = IP Address is not resolved 2 = Not connected 3 = Connecting 4 = Connected 5 = Closing
Index:	1..12 Defines the connection number
Access:	Read

Example:

If STA1:SCS3 returns 4, it means that TCP connection to address specified with STA1:SIA3 is in state Connected.

RP	Redundancy Priority

Indicates the priority of a redundancy connection defined in IA attribute. If one or more connections have RP value 1, 2 or 3, an automatic selection of redundancy connection functionality is taken into use. If redundancy priorities of all connection of a station are set to 0, automatic selection of redundancy connection functionality is not used. This the default functionality. The automatic selection of redundant connection changes the used connection automatically and STA objects in question does not change its status to 'SUSPENDED'. The connection is changed when the current connection becomes faulty or a higher priority connection becomes available. The connections with priority value 1 are prioritized over other connections. If there are no priority 1 connections, priority 2 connection is chosen. Priority 3 is chosen if priority 1 or 2 connections are not available. Connections with priority 0 are not included to the automatic connection selection. If the used connection is changed manually with the AC attribute, the connection is not changed even if it becomes faulty. By setting the AC attribute to 0 the automatic selection of redundant connection is enabled again. If configured connections are connected to two different IEDs acting, for example, as Hot-Stand-By, usage of values 101..103 can be considered. If active connection to, for example, IED B becomes faulty and backup connections to IED A and IED B has same priority, connection to IED B is preferred instead of connection to IED A.

Value:	0 = No priority (= connection not included to automatic selection) 1 = High Priority IED A 2 = Medium Priority IED A 3 = Low priority IED A 101 = High Priority IED B 102 = Medium Priority IED B 103 = Low Priority IED B
Index:	1..12 Defines the connection number
Access:	Read, conditional Write

Example:

```
; IED A and IED B are equal
#SET STA1:SRP1=1 ; High priority for first logical connection to IED A
#SET STA1:SRP2=1 ; High priority for second logical connection to IED A
#SET STA1:SRP3=101 ; High priority for first logical connection to IED B
#SET STA1:SRP4=101 ; High priority for second logical connection to IED B
; IED A is preferred if available
#SET STA1:SRP1=1 ; High priority for first logical connection to IED A
#SET STA1:SRP2=1 ; High priority for second logical connection to IED A
#SET STA1:SRP3=102 ; Medium priority for first logical connection to IED B
#SET STA1:SRP4=102 ; Medium priority for second logical connection to IED
B
```

If two IEDs is configured and they are operating as HOT-HOT and a single network failure may affect both IEDs, it is good to note that the disconnections are not necessarily detected at the same time. This may result an unexpected switch to another IED. Therefore, in HOT-HOT setups with connection count 4 or bigger, same priority for all connections is worth to consider.

LC **Locked redundancy Connection**

Indicates the state of the automatic selection of redundant connection. If a non-zero value is written to station attribute AC, active connection is locked to certain connection and value returned by LC indicates this. For more information, see attributes RP Redundancy Priority and AC Active Connection.

Value:	0 = Automatic selection of redundancy connection functionality is running 1 = Automatic selection of redundancy connection functionality is not running
Access:	Read only

UA **UAL Event Used**

Attribute UA defines whether the UAL (User activity logging) events are generated by the station object. Generation of the UAL events are recommended if the secure authentication is used, see attribute ZA. With ‘Standard logging’, all user status changes are logged. With ‘Special logging’, also all successful authentications, key change negotiations, authorization failures and error situations are logged. The event codes with 'Special logging' are supported by SYS600 but not necessarily, for example, with SDM600 product. In case the secure authentication is used and more detailed information from the system behaviour is needed, the usage of value 3 = 'Special logging' is recommended.

Data type:	Integer
Value:	0 = Disabled 1 = Standard logging 2 = Extended logging 3 = Special logging
Indexing:	No indexing
Default value:	1 (Enabled)
Access:	No limitations

UI **UAL Event Identification**

The UI attribute is used to define the name for the station object, and it is used to identify the source of the UAL (user activity logging) events. This string is added to the identification information of all UAL events from this station object. A unique value within the node is preferred. The node level module name (also in attribute UI) is added to form the full identification information for the user activity event. The default value of the string is based on the translated station number which is equal to B-attribute TN (Translated Object Number) in the base system. If a station identifier is not needed, an empty string should be assigned to this attribute.

Data type:	String
Value:	String containing a station level identifier with maximum length of 16 characters
Indexing:	No indexing
Default value:	”.STA(TN=x)”, where x = translated station number
Access:	No limitations

4.3.2.5 Authentication attributes

This chapter describes only the attribute interface related to secure authentication. See SYS600 System Configuration Manual, chapter 'Secure authentication using IEC/TS 62351-5' for detailed steps for configuring the system for secure authentication according to IEC/TS 62351-5.

ZA	Authentication Used

The ZA attribute defines whether secure authentication is used by the station object or not.

Value:	0 = Disabled 1 = Enabled, pre-shared update keys 2 = Enabled, update key negotiation
Indexing:	No indexing
Default value:	0 (Disabled)
Access:	Read/write

ZG	Aggressive Mode

The ZG attribute defines whether the aggressive mode of authentication is used by the station object. The aggressive mode uses less bandwidth and using it is recommended. The value of this attribute is meaningless if authentication is disabled (see attribute ZA). Modifying this attribute is possible only if it is enabled in the key storage using the setting 'Allow external modification of security attributes' (see attribute DZ, index 255).

Value:	0 = Aggressive mode disabled 1 = Aggressive mode enabled
Indexing:	No indexing
Default value:	1 (Enabled)
Access:	Read, write possible if the modification is enabled in the key storage

ZT	Key Storage Id

The ZT attribute is used to define the keys and user set of the STA object in the key storage. In case there is a need to change the station number and/or its translated number TN and the corresponding user set and key configuration is already configured, keeping the original value in the ZT attribute associates the existing user set with the new station object. The ZT value must be unique within the STA objects accessing the same key storage. Error is returned when setting to a reserved value is attempted. Value = 0 means that the station object is not attached to any user set and the enabling of the authentication using attribute ZA is not possible.

Value:	Identification of the STA object in the key storage, range 0..65535
Default value:	Same as the TN of the STA object
Indexing:	No Indexing
Access:	Read/write

ZU	Default User

The ZU attribute is used to define the user in case the user is not or cannot be received from the MicroSCADA application. This user is used in requests generated with station the attribute CO, SY or GI.

Value:	When read, the number of the active user is returned When written, number or the name of the wanted active user
Default value:	1 (Default user)
Indexing:	No indexing
Access:	Read/write

Example:

Issue an output command using user 2

```
@P_USER = STA1:SZU
#SET STA1:SZU=2
;close select command, double command, address 1000
#SET STA1:SCO=(46,1000,6,128+1)
#SET STA1:SZU=%P_USER
```

ZR **Authenticated Users**

The ZR attribute is used to read the user numbers and names defined in the key storage for the station. See also the ZU attribute for defining the default user. This attribute is indexed using the user number and it is not supported by the System Configuration tool.

Value:	String containing a user name with the maximum length of 32 characters.
Indexing:	1..65535 (User number) If index = 0 is given when read, a vector of configured user numbers for the STA object is returned. If only one user is configured, the returned value is a scalar of type integer. If ZA is 0 or no users is configured, no object is returned.
Access:	Read

ZI **Association Id**

The ZI attribute is used to define the association identification value of the user. This attribute is used to fully identify the user. The attribute is indexed using the user number and is not supported by the System Configuration tool.

Value:	The association id of the user defined by the index
Default value:	0
Indexing:	1..65535 (User number)

ZV	Authentication Vector

The ZV attribute defines the constants used by the specific user of the station object. Modifying these constants is possible but it may require some testing to be usable with the remote IED and its configuration. The given index defines the user, value 0 has a special meaning. The values of the vector cannot be modified one-by-one but when written, only a vector containing all values is accepted. If the third parameter is defined, at least one user with role 'Operator' (Value=2) need to be configured. Setting of third parameter for ZV0 is possible only when setting 'Allow external modification of security attributes' flag is set for the keystorage in use. This flag is defined in the 'System' level in the Authority Tool.
Fourth parameter of ZV0 is a bitmask which defines compatibility flags due to different interpretations of IEC62351-5 standard. Bit 0 affects MAC calculation of critical messages and bit 1 affects the handling of CSQ (Challenge sequence number) field. When bits 0 and 1 are set, the functionality is similar to DNP3 SAv5. In case the remote system or its software is North American originated, setting of bits 0 and 1 may be necessary. When bit 2 of the fourth parameter of ZV0 is set, a pre-defined update key for a user is used, instead of generating a random new key in every update key negotiation. This feature is useful if the IED in question uses this key, for example, as a user specific password in its HMI or remote access.

When index is >0, values of Key wrap algorithm of the session key in ZV(2), HMAC algorithm of the critical requests in ZV(4) and HMAC length of critical requests in ZV(5) are updated automatically as requested by the outstation.
If the count of the received authentication error messages reaches ZV(6), session keys are renegotiated.
ZV(11) is Maximum Session Key Status request count ZV(11), value is meaningless in master.
The attribute is indexed using the user number and is not supported by the System Configuration tool. Index 0 contains special compatibility flags applied for all users.

Value:

For index 0, vector of max 4 integers
ZV(1) User name null termination
(1 = User name transmitted without null termination (default))
(2 = User 'Common' with null termination, others without)
(3 = User names transmitted with null termination)
ZV(2) Authority certification key length with SHA-1 Update Key Change Method
(16= First 16 bytes used in MAC calculation)
(32 = All 32 bytes used in MAC calculation (default))
ZV(3) Mapping of user when command is originated from process object
(0 = Command sender is logged user (default))
(1 = Command sender is user defined with ZU)
(2 = Command sender is first user with role 'Operator')
ZV(4) Compatibility bitmask
(Bit 0 not set = European interpretation of IEC62351-5 MAC calculation (default))
(Bit 0 set = North American interpretation of IEC62351-5 MAC calculation, same as in DNP3)
(Bit 1 not set = European interpretation of IEC62351-5 CSQ handling (default))
(Bit 1 set = North American interpretation of IEC62351-5 CSQ handling, same as in DNP3)
(Bit 2 not set = Random update key is generated during negotiation (default))
(Bit 2 set = Update key is not generated during negotiation but taken as pre-defined from the keystorage)
For indices > 0, vector of 11 integers
ZV(1) Session key length
ZV(2) Key wrap algorithm of the session keys
(2=AES-256)
ZV(3) Challenge data length critical request
ZV(4) HMAC algorithm of the critical requests
(2 = SHA-256)
ZV(5) HMAC length
(8 = SHA-256 serial)
(16 = SHA-256 network)
ZV(6) Not used, see DZ(11) and ZH(11)
ZV(7) Session key change count
ZV(8) Key change interval in seconds
ZV(9) Challenge data length session key status
ZV(10) Challenge data length update key reply
ZV(11) Maximum Session Key Status Count (meaningful in slave only)

Table continues on next page

ZV	Authentication Vector
Default values:	Index 0: ZV(1) : 1 ZV(2) : 32 ZV(3) : 0 ZV(4) : 0 Indices >0: ZV(1) : 16 ZV(2) : 2 (AES-256) ZV(3) : 8 ZV(4) : 2 (SHA-256) ZV(5) : 16 (SHA-256 Network) ZV(6) : 2 ZV(7) : 1000 ZV(8) : 900 ZV(9) : 8 ZV(10) : 32 ZV(11) : 5
Indexing	1..65535 (User number), 0 (compatibility flags)
Access:	Read-only

Example 1:

```
@USERS = STA1:SZR
#LOOP_WITH I=1..LENGTH(%USERS)
     ; Change each user to use SHA-256 and AES-256 in TCP mode, session
key change interval 120 secs
    @USER=%USERS(%I)

    #SET STA1:SZV'USER'=(16,2,8,2,16,2,1000,120,8,32,5)

#LOOP_END
```

ZS	Authentication Status
The ZS attribute returns the current values of the authentication parameters and states of the specific user. This attribute is implemented only for debugging purposes and modifying these values directly is not possible. The attribute is indexed using the user number and is not supported by the System Configuration tool.	
Value:	Vector of 8 integers ZS(1) State of the authentication ZS(2) Not used at the moment ZS(3) Not used at the moment ZS(4) Challenge sequence number CSQ ZS(5) Key change sequence number KSQ ZS(6) Key status KST ZS(7) Last error in ZS(8) Last error out Values of Key Status in ZS(6) are : 1 = OK 2 = Not initialized 3 = Communication failure 4 = Authentication failure
Default value:	ZS(1) : 0 ZS(2) : 0 ZS(3) : 0 ZS(4) : 0 ZS(5) : 0 ZS(6) : 2 ZS(7) : 0 ZS(8) : 0

Table continues on next page

ZS	Authentication Status
Values of ZS(1)	0 : Initial State 10 : Wait for Key Status 11 : Wait for Key Change Confirmation 12 : Security Idle 13 : Wait for Reply 14 : Wait for User Change Response 15 : Wait for Update Key Reply 16 : Wait for Update Key Confirm
Indexing:	1..65535 (User number)
Access:	Read-only

ZO	User Roles

The ZO attribute is used to return user numbers and their roles for the authentication. The user set for the station is created using the authority tool and stored to the key storage file.

Value:	String containing a user role with maximum length of 32 characters. Standard roles are: 0 = 'Viewer' (has 'Monitor Data' permission) 1 = 'Operator' (has 'Monitor Data' and 'Operate Controls' permissions) 2 = 'Engineer' (has 'Monitor Data', 'Change Config', 'File access' and 'Local login' permissions) 3 = 'Installer' (has 'Monitor Data', 'Change Config', 'Change code', 'File Access' and 'Local login' permissions) 4 = 'SecAdm' (has 'Change Security Config', 'Change code' and 'Local login' permissions) 5 = 'SecAud' (has 'Monitor Data' and 'Local login' permissions) 6 = 'RBacMnt' (has 'Monitor Data', 'Change Config' and 'Change Security Config' (roles only) permissions See attribute CR for more information.
Default value:	Empty string
Indexing:	1..65535 (User number)
Access:	Read-only

ZN	Outstation Name

The ZN attribute is used to return the name of the outstation. This attribute is preconfigured using the Authority Tool and must match the value configured to master/slave.

Value:	String containing an outstation name with maximum length of 128 characters
Default value:	Empty string
Indexing:	No indexing
Access:	Read-only

ZD **Authentication Diagnostics**

The ZD attribute provides user specific counters for diagnostic purposes. These counters can be used to verify the activity of each user and to give information in problem situations. The same counters for all users can be read from the attribute DZ.

Value:	Vector of 17 integers (0..65535) ZD(1) Unexpected Messages ZD(2) Authorization Failures ZD(3) Authentication Failures ZD(4) Reply Timeouts ZD(5) Rekeys Due to Authentication Failure ZD(6) Total Messages Sent ZD(7) Total Messages Received ZD(8) Critical Messages Sent ZD(9) Critical Messages Received ZD(10) Discarded Messages ZD(11) Error Messages Sent ZD(12) Error Messages Received ZD(13) Successful Authentications ZD(14) Session Key Changes ZD(15) Failed Session Key Changes ZD(16) Update Key Changes ZD(17) Failed Update Key Changes
Default values:	ZD(1) ..ZD(17) : 0
Indexing:	1..65535 (User number)
Access:	Read/write (write only value 0)

ZP **Authentication Parameters**

The ZP attribute defines authentication parameters which has an effect on all users configured for the station object. The given index specifies the parameter.
ZP(1) defines the amount of critical or non-critical ASDUs received which will trigger the session key negotiation for all users, function 'Session Key change Count' in 62351-5 standard. Session key negotiation is triggered also because of the timer defined with ZV(8) (for each user), whichever reason occurs first. The default value for ZP(1) is 1000. In case the ASDU reception rate is high, bigger value is worth to be considered but the value should still be in line with the slave configuration. If ZP(1) value is 0, function is not used, that is, the session keys are negotiated only using a timer based triggering. Slave devices usually have corresponding configuration parameter to invalidate session keys after certain amount of transmitted ASDUs. If this parameter is smaller than ZP(1) in master, it is possible that the keys are invalidated unexpectedly and next critical request such as a control command is rejected. Slave device does not explicitly report when it has invalidated the session keys.
The attribute is not supported by the System Configuration tool. No other indices but 1 is used the moment.

Value:	ZP(1) Session Key change count
Default values:	ZP(1) : 1000 (range 0..2147483647, value=0 means disabled)
Indexing	1..1
Access:	Read/Write

DZ	Diagnostics of Authentication

The DZ attribute provides diagnostic counters of authentication related functions. These counters can be used to verify the activity of communication concerning data which requires authentication. The same counters can be read as user specific from the attribute ZD.
Index 255 has a special meaning. If DZ(255) returns 1, the editing of the attributes CR and ZG is allowed by a special setting in the key storage.
Special sets of the same counter are provided using indices 101..117 and 201..217. Indices 101..117 return the same diagnostic counters calculated from the beginning of the PC_NET start-up, without resetting.

Value:	Vector of 17 integers (0..2147483647) DZ(1) Unexpected Messages DZ(2) Authorization Failures DZ(3) Authentication Failures DZ(4) Reply Timeouts DZ(5) Rekeys Due to Authentication Failure DZ(6) Total Messages Sent DZ(7) Total Messages Received DZ(8) Critical Messages Sent DZ(9) Critical Messages Received DZ(10) Discarded Messages DZ(11) Error Messages Sent DZ(12) Error Messages Received DZ(13) Successful Authentications DZ(14) Session Key Changes DZ(15) Failed Session Key Changes DZ(16) Update Key Changes DZ(17) Failed Update Key Changes
Default values:	DZ(1) ..DZ(17) : 0 DZ(255) : 0 (attribute editing not allowed)
Indexing :	255 : editing of the attributes CR and ZG is allowed by a special setting in the key storage 1..17 : Diagnostic counters mentioned above, is reset 101..117 : Diagnostic counters mentioned above, is unreset 201..217 : Diagnostic counters mentioned above, next threshold value for special action
Access:	Read/write (write only value 0 for indices 1..17)

CR	Critical Requests

The CR attribute defines which requests are critical. The modification of this vector is possible but not recommended.
The default values follow the IEC TS 60870-5-7. Modifying this attribute is possible only it is enabled in the key storage using the setting 'Allow external modification of security attributes' (see attribute DZ, index 255). In IEC 60870-5-104, control commands are sent using ASDUs 45..51 (without time tag) or ASDUs 58..64 (with time tag) which are critical as default. The required permissions for a user are 'Operate Controls', see attribute ZO for more information. Index of the CR attribute defines the ASDU number in question.
This attribute is not supported by the System Configuration Tool.

Value:	Vector of 255 integers with values 0 = not critical 1 = critical 128 = not applicable
Default values:	CR(1..44) : 0 (Indication ASDUs) CR(45..51) : 1 (Non-timestamped command ASDUs) CR(52..57) : 0 (ASDUs not defined) CR(58..64) : 1 (timestamped command ASDUs) CR(65..69) : 0 (ASDUs not defined) CR(70) : 0 (End of initialization ASDU) CR(71..80) : 0 (ASDUs not defined) CR(81..95) : 128 (Authentication ASDUs) CR(96..99) : 0 (ASDUs not defined) CR(100..102) : 0 (Interrogation and read commands) CR(103) : 1 (Time synchronization command) CR(104) : 0 (Test command without time tag) CR(105) : 1 (Reset process command) CR(106) : 0 (Delay acquisition command) CR(107) : 1 (Test command with time tag) CR(108..109) : 0 (ASDUs not defined) CR(110..113) : 1 (Parameter setting and activation) CR(114..119) : 0 (ASDUs not defined) CR(120..126) : 1 (File Transfer) CR(127..255) : 0 (ASDUs not defined or private range)
Indexing :	Index 1..255 (defines the ASDU number)
Access:	Read, write if allowed by the key storage config

NU	New Keys

The NU attribute is used to renegotiate the update keys for specific user. When a user name is given, user status is set using 'ADD' operation and a new update key is negotiated. The role, role expiry interval and the used algorithm is read from the keystorage. In case the slave device has lost its user information, or the session key negotiation fails systematically, it may be necessary to use the special strings described below. "*DELETE" operation is allowed only when setting 'Allow external modification of security attributes' flag is set for the keystorage in use. This flag is defined in the 'System' level in the Authority tool. Special string "*ADD" makes an 'ADD' operation to all existing user users and their roles. If asymmetric mode is used and all necessary users are present in the slave device, the usage of "*UPDATE" may be considered since the recalculation of the private/public key pairs consumes a lot of CPU resources. Option "*UPDATE" renegotiates the update keys but does not change the user status.

Value:	When written, the name of the user to be negotiated again Special strings: "*ADD" : Add all users "*DELETE" Delete all users "*UPDATE" Negotiate update keys of all existing users
Indexing:	No indexing
Access:	Write

Example 1:

Renegotiate the update key for user "Mark"

```
#SET STA1:SNU="Mark" ; operation = add, role is read from keystorage
```

Example 2:

Delete and add all users. A new update key is negotiated when user is added.

```
#SET STA1:SNU="*DELETE" ; delete all users, takes few seconds per user
#PAUSE 30
#SET STA1:SNU="*ADD" ; add all users, takes few seconds per user
(symmetric mode)

#SET STA1:SNU="*UPDATE" ; renegotiate update key but do not change user
status
```

4.3.2.6 Security attributes

This chapter describes only the attribute interface related to encryption using TLS (IEC62351-3). These attributes should only be used together with the secure authentication, see Section 'Authentication attributes' and SYS600 System Configuration manual.

All TLS connections in one PC-NET instance must use same certificate and key and trusted certificate authority files, see attribute CI Certificate Information. Furthermore, all TLS connections in one PC-NET instance must use same min/max values of TLS version, see attribute CV Certificate Handling Vector

CI	Certificate Information

The CI attribute is used to define the certificate/key file and the trusted certificate authority file for the TLS communication. When set, it has an effect on all STA objects that have the same remote IP-address in attribute IA. Also, by setting both CI indices the TLS functionality is started. The certificate files location can be chosen freely, but it is recommended to place them in a folder with limited access rights to improve the security of the system. For example, use a folder where only the MicroSCADA user has access rights. Same certificate and trusted certificate authority file should be used in all STA objects configured to one PC-NET instance.

Value:	String containing the directory and the name of the certificate file. Only certificate file type .PEM is supported.
Indexing:	1 : Certificate and Key file 2 : Trusted certificate authority file

Table continues on next page

CI	Certificate Information
Default value:	Empty string
Access:	Read/conditional write

Example:

```
#SET STA1:SCI1="C:\Users\MicroSCADA\AppData\Roaming\ABB\MicroSCADA Pro
\Device_STA1.pem"
#SET STA1:SCI2="C:\Users\MicroSCADA\AppData\Roaming\ABB\MicroSCADA Pro
\CA_list.pem"
```

The TLS functionality is activated when both CI attribute indices are set.

CP	Certificate Passphrase

The CP attribute is used to define the passphrase to open the private key in the certificate file defined with attribute CI(1). If the certificate does not require passphrase, this attribute may be an empty string. If the creation of the self-signed certificates is enabled using attribute CV(2), the contents of this attribute is included to the passphrase of the private key of the created certificate. When set, it operates like attribute CI, that is, it has an effect on all STA objects that have the same remote IP-address in attribute IA.

Value:	String containing the passphrase with maximum length of 16 characters
Indexing:	No indexing
Default value:	Empty string
Access:	Read/conditional write

Example:

```
#SET STA1:SCP="96gd21"
```

CN	Common Name

The CN indices 1, 2 and 4 are used to define the Common Name, the Country Code and the Organization name of a self-signed certificate. All 3 values must be set when creating a self-signed certificate. The CN(1), the Common Name, should be the IP address of the station. In CN(2) the Country Code should be given with two capital letters. The CN(4), the Organization name, should be a single name without spaces. The name and location of the created certificate is defined using attribute CI(1). When self-signed certificate is used, the CN attribute operates like CI attribute, that is, it has an effect on all STA objects that have the same remote IP-address in attribute IA. CN indices 5 and 6 refer to Organization Unit and Domain Component and can be left empty. If set, corresponding OU and DC strings must be found from CN(3). For detailed instructions for creating a self-signed certificate, see SYS600 System Configuration manual.

If the certificate file contains multiple certificates, the CN index 3 is used for selecting a certain certificate that will be used. In CN(3), the CN(1), CN(2) and CN(4) needs to be listed and they must have the exact values that were set to the certain certificate. The format of CN(3) can be seen in the example below. If only one certificate exists in the certificate file, CN(3) can be left empty.

The CN attribute indices 1, 2 and 4 are needed only when a self-signed certificate is created. The creation of self-signed certificate is selected with CV attribute bit 2 values 1 or 2.

Value:	String
Indexing:	1 : Common name of the certificate with maximum length of 64 characters 2 : Country code with maximum length of 2 characters 3 : Certificate name with maximum length of 228 characters 4 : Organization name with maximum length of 64 characters 5 : Organization Unit name with maximum length of 64 characters 6 : Domain Component with maximum length of 64 characters

Table continues on next page

CN	Common Name
Default value:	Empty string
Access:	Read/conditional write

Example:

```
#SET STA1:SCN1="10.10.10.1"
#SET STA1:SCN2="FI"
#SET STA1:SCN4="ABB"

#SET STA1:SCN3="CN=10.10.10.1 O=ABB C=FI"
```

Example 2:

```
#SET STA1:SCN1="10.10.10.1"
#SET STA1:SCN2="FI"
#SET STA1:SCN4="ABB"
#SET STA1:SCN5="PSS1" ; optional
#SET STA1:SCN6="COM" ; optional

#SET STA1:SCN3="CN=10.10.10.1 O=ABB C=FI OU=PSS1 DC=COM"
```

CV	Certificate Handling Vector

The CV attribute defines a set of values which control error logging and certificate handling, creation and accepting. The modification of these attributes from the defaults may decrease the total security of the system. When set, it operates like attribute CI, that is, it has an effect on all STA objects that has the same remote IP-address in attribute IA.
CV(1) indicates if possible error messages are logged into the MicroSCADA Notify window. If given value is 2, all SCA printouts are directed to Notify Window. This mode should be used only temporarily.
CV(2) indicates if self-signed certificates are created when the communication is started. 0, 'Never', should be used when certificates already exist. This also applies to situations in which self-signed certificates are used. With option 1, 'If not found', a self-signed certificate is created in case the certificate set in CI(1) doesn't already exist. With setting 2, 'Always', a self-signed certificate is always created even if the certificate file set in CI(1) already exists. In this case the existing file is replaced with a new file.
CV(3) indicates the action that will occur when the remote certificate validation fails. With value 0, 'Ignore, continue communication', the communication is not terminated even though the remote certificate is found faulty or cannot be authenticated. This option should only be used in special situations, for example in testing. Value 1, 'Close connection', terminates the connection when the remote certificate validation fails. This is the default behavior and it is recommended to be used. Functionality with value 3 is similar to value 1 but the certificate from remote system does not require to have the IP-address in its 'Common Name' field.
CV(4) defines the accepted certificate file type. Currently only type .pem files are supported.
CV(5) defines the minimum TLS protocol version that is accepted from the remote certificate. In case the remote device uses TLS version lower than what is defined in CV(5) the communication is terminated (unless the CV(3) is set to 0). For highest security it is recommended to use the highest TLS version possible.
CV(6) defines the maximum TLS protocol version that is accepted from the remote certificate. In case the remote device uses TLS version higher than what is defined in CV(6) the communication is terminated (unless the CV(3) is set to 0). For highest security it is recommended to use the highest TLS version possible.
CV(7) and CV(8) defines the resumption mode and timeout. These values cannot be changed if the STA object using the TLS connection has been taken into use at least once.
CV(9) defines the CRL (certification revocation list) based revocation checking mechanism for remote certificates. Default mode is 0 = No CRL revocation check. When value 1 or 2 is used, regular CRL file update must be implemented to system. See SYS600 System Configuration manual for more information. CRL file is definition and activation should be made using station attribute RL (Revocation List).

Value:	Integer
Indexing:	CV(1) Error logging (0 = No error logging) (1 = Error logging to Notify window) (2 = All SCA printouts to Notify window) CV(2) Self-signed certificate generation (0 = Never) (1 = If not found) (2 = Always) CV(3) Operation when the remote certification validation fails (0 = Ignore, continue communication) (1 = Close connection) (2 = Not used) (3 = Close connection, no IP-address checking) CV(4) Type of the certificate store (0 = .pem file) CV(5) Minimum TLS version (31 = TLS 1.0/SSL 3.1) (32 = TLS 1.1/SSL 3.2) (33 = TLS 1.2/SSL 3.3) CV(6) Maximum TLS version (31 = TLS 1.0/SSL 3.1) (32 = TLS 1.1/SSL 3.2) (33 = TLS 1.2/SSL 3.3) CV(7) TLS Session Resumption Mode (0 = No Resumption) (1 = Ticket based resumption) (2 = Session ID based resumption) (3 = Both Ticket and Session ID based resumption) CV(8) TLS Session Resumption Timeout (in seconds) CV(9) CRL based certificate revocation Mode (0 = No CRL revocation check) (1 = CRL revocation check only for entity) (2 = CRL revocation check for entity and intermediate)

Table continues on next page

CV	Certificate Handling Vector
Default values:	CV(1) : 0 CV(2) : 0 CV(3) : 1 CV(4) : 0 CV(5) : 33 CV(6) : 33 CV(7) : 1 CV(8) : 300 CV(9) : 0
Access:	Read/conditional write

For the configured TLS versions to become valid, they must be set before the station and the line are taken into use for the first time. If the TLS versions are changed afterwards, the PC-NET must be restarted for the changes to become valid.

The minimum TLS version must be equal or lower than the maximum TLS version.

```
#SET STA1:SCV1=1 ; enable error logging to notify window
#SET STA1:SCV5=31 ; Set minimum TLS version to 1.0
Example:
#SET STA1:SCV6=33 ; Set maximum TLS version to 1.2
```

RL	Revocation List

Attribute RL defines the location of the certificate revocation list file for the TLS connection. When written, the previous file definition is overwritten and the contents of the new file loaded for the check of the remote certificate made in next full TLS handshake. Redefining the same file location only reactivates the certification check with the current contents of the file. See SYS600 System Configuration manual for information how CRL file is cyclically downloaded from certificate authority. CRL based certificate revocation checking is disabled by default and must be enabled using setting in attribute CV (Certificate handling Vector), index 9. Supported file types are .DER and .PEM. RL writing is possible not until the IA attribute is defined and station objects is taken into use at least once. All TLS connections in a same PC-NET instance are using the same CRL definition. CRL definition can be removed only by setting CV(9) to 0 in active configuration and restarting PC-NET.

Data Type:	String
Value:	File name and path
Indexing:	Always 1
Default value:	Empty string
Access:	No limitations

Example:

```
#SET STA1:SRL1="D:\sys600_certs\pcnet1_conns.der" ; define and activate
updated CRL file
```

EE	Encryption Error

The EE attribute is used to return the last error code occurred in encryption. The value is the same for all STA objects that have the same remote IP-address in attribute IA. See Status Codes manual for error descriptions, chapter CSA SCA error codes.

Value:	Integer
Indexing:	No indexing
Default value:	0
Access:	Read-only

4.3.2.7 File transfer attributes

The IEC file transfer feature transmits all types of files between the relay and the SYS600 computer. Only one transmission per one STA object can be active at any one time. If another file transfer request is made while the first file transfer is in progress, the status code is returned and the second file transfer progress does not start.

FI	File Information
The FI attribute initializes the file transfer system with the required base information.	
Value:	Vector of 5 integers 1 = internally used 2 = SEGMENTCOUNT 3 = internally used 4 = QUEUE (unbalanced slave) 5 = PRIORITY (slave) 6 = Section request delay IN (0.1 seconds) 7 = Section filling delay OUT (0.1 seconds)
Indexing:	1..7
Access:	Read/Write
Default value:	1 = 0 2 = 8 3 = 0 4 = 2 5 = 3 (1 is lowest value) 6 = 0 (0 milliseconds) 7 = 10 (1000 milliseconds)

Example:

The following example defines five segments in each file section.

```
#SET STA'sta':SFI(2)=5
```

FD	File Directory
The FD attribute defines to which directory the received files are stored. PC_NET interrupts file receiving if the directory does not exist or if it is write-protected.	
Value:	The string contains a valid directory name with the maximum length of 50 characters.
Access:	Read/Write
Default:	C:\TEMP

Example:

The following example defines C:\SC\DATA to the active directory.

```
#SET STA'sta':SFD="C:\SC\DATA"
```

FF **File Transmission Status**

The FF attribute indicates the status of file transmission.

Value: 0 = Free to start or the previous transmission is completed
1 = Transmit in progress
2 = Timeout in PC_NET
3 = Not used
4 = Invalid directory or file name
5 = File is not available in the remote end
6 = Service is not available, internal error
7 = Transfer aborted
8 = File reading or writing failed

Access: Read, Write is allowed when the value is not 6.

Default value: 0

If transmission is in progress when the FF attribute is written, the transmission is aborted, and the file is closed. It does not have any other effects, except the value is set to zero (0).

FT **File Timeout**

The FT attribute defines the maximum delay for incoming ack section or ack file request. If the time expires, PC_NET interrupts the file transmission.

Value: 0..255

Unit: Seconds

Access: Read/Write

Default value: 30 seconds

FB **File Bytes**

The FB attribute returns both counts of received or transmitted bytes from the beginning of the file transfer session (index 1) and the file size (index 2). At the beginning of the file reception, the value of index 1 is automatically set to zero (0). The value of index 2 is updated when the FB attribute is written, and the correct file index is given.

Value: 0..4294967295

Indexing: When read
1 = Number of bytes (DWORD), out
2 = File size in bytes (DWORD), out
3 = File name in relay (DWORD), out
4 = Number of bytes (DWORD), in
5 = File size in bytes (DWORD), in
6 = File name in relay (DWORD), in

Access: Read

Default: 0

FN	File Name

The FN attribute collects the information address of a certain file in the file system. When the remote end requests the directory, the information address is reported as a real file, not as a subdirectory (FOR = 0).

Value:	When written IOA NAMEOFFILE FILETYPE STATUSOFFILE NAMEINFILESYSTEM SIZEINFILESYSTEM DATEINFILESYSTEM MSECSINFILESYSTEM When read NAMEINFILESYSTEM When read
Indexing:	When read, (0..299) Queue out: index = 100+FILENUM Queue in: index = 200+FILENUM

If the FILENUM offset is bigger than the number of files in the list, status code 13887 ICCC_NO_SUCH_FILE is returned.

For more information about status codes, see Section 5.5.

Access:	Read/write

Where when writing

IOA

Information object address.

Type: DWORD

NAMEOFFILE

Defines the name of file field in the file transfer messages.

Type: WORD

FILETYPE

Type: WORD

Values: 1 = Transparent file

Other types are not supported at the moment.

STATUSOFFILE

Type: BYTE

Values: 0 = File waits for transfer

NAMEINFILESYSTEM

String contains a valid file name in the disk with maximum length of 100 characters. If the string is empty, the file is deleted from the list.

SIZEINFILESYSTEM (optional)

The file size.

Type: DWORD

DATEINFILESYSTEM (optional)

Creates file’s timestamp (seconds from 1.1.78).

Type: TIME

MSECSINFILESYSTEM (optional)

Creates file’s timestamp (milliseconds).

Type: WORD

Example of writing:

```
#SET STA'sta':SFN=(1000, 1,1,0, "error.log", 5000, clock)
```

Example of reading:

The second file is read from the outgoing file list and returns the error.log file.

```
STA'sta':SFN(102)
```

FV	File Values
The FV attribute checks the status of the defined file. During the reading process, the attribute's index defines where the file value is taken, either from the outgoing files list or from the incoming files list.	
Value:	Vector IOA NAMEOFFILE FILETYPE CTRLANDSTATUSOFFILE SIZEINFILESYSTEM DATEINFILESYSTEM MSECSINFILESYSTEM
Indexing:	When read, word (0..65535) Queue out: index = 100+FILENUM Queue in: index = 200+FILENUM If the FILENUM offset is bigger than the number of files in the list, the returned data type is "NONE"
Access:	Read For more information about status codes, see Section 5.5. IOA Information object address NAMEOFFILE Defines the name of file field in the file transfer messages. Type: WORD If value = 0 is given for both IOA and NAMEOFFILE, a unique value is assigned. FILETYPE Type: WORD Values: 1 = Transparent file Other types are not supported at the moment. CTRLANDSTATUSOFFILE Type: WORD. The upper byte is a control byte. Bit 0 : Internally used Bit 1=0: Not yet transmitted Bit 1=1: All sections transmitted Bit 2=0: Transmission not acknowledged by remote Bit 2=1: Transmission acknowledged by remote The lower byte is equal to status of file (SOF) Bit 7=0: File waits for transfer (FA) Bit 7=1 Transfer of this file is active (FA) SIZEINFILESYSTEM Type: DWORD The file size. DATEINFILESYSTEM Type: TIME Creates file’s timestamp.

Table continues on next page

FV	File Values

Example:

Reading the second file from the outgoing file list.

```
STA'sta':SFV(102)
3 ;Information object address
3 ;Name of file
1 ;Transparent file
1536 ;CTRL=(transmitted, acknowledged), SOF=0
10006 ;Filesize=10006 bytes
847636153 ;Timestamp
```

Example 2:

Initiating of the reception of the first file from remote device.

```
@STA=1
#IF STA'STA':SFF<>1 #THEN #BLOCK
  #SET STA'STA':SCO=(122,0,5,0,0,0,1) ; request directory
  #PAUSE 3
  @FV=STA'STA':SFV(201)
  #IF DATA_TYPE(%FV) == "VECTOR" #THEN #BLOCK
    ;at least one file available
    @NOF_L = %FV(2) mod 256
    @NOF_H = %FV(2) div 256
    #SET STA'STA':SCO=(122, %FV(1), 13, %NOF_L, %NOF_H,
0,1) ;request file
   #BLOCK_END
#BLOCK_END
```

Example 3:

Initiating of the reception without directory request. The IOA and NAMEOFFILE of the file in the remote device need to be known in advance.

```
@STA=1
#IF STA'STA':SFF<>1 #THEN #BLOCK
  ; no on-going file tranfer
  @NOF_L = %NAMEOFFILE mod 256
  @NOF_H = %NAMEOFFILE div 256
  #SET STA'STA':SCO=(122, %IOA, 13, %NOF_L, %NOF_H,
0,1) ;request file
#BLOCK_END
```

For more information about status codes, see Section 5.5.

For more examples on communication system configuration, see Appendix A.

4.4 After configuration

For each input signal received from the process device the process database should contain a process object whose value changes after process data is received. For each command there should be an output process object. The bit stream process object that receives unrecognized IEC messages from the slave should also be created.

Besides the configuration of the base system and the communication system, the IEC slave also needs to be configured.

4.5 How to test the configuration

When the slave and master stations have been physically tested and the configuration has been completed, the connection and configuration can be tested based on the following methods:

- Diagnostic counters. When the communication between the slave and master is running properly and data is moving on the line, the diagnostic counters indicating the number of received and transmitted data messages should be incrementing.
- Object status. The OS attribute of the IEC slave station should be 0.
- By connecting a protocol analyzer supporting the IEC 60870-5-104 standard to the line.

For MicroSCADA version 9.3 and newer, the protocol analyzer included in PC-NET can be used. See the NET line attributes AO and AU in the SYS600 System Objects manual.

One possible way to test the configuration is to use SYS600 as the IEC master/slave. In this case the base system and communication system configuration for the IEC 60870-5-104 Master line and station(s) have to be made. One IEC slave can be in the same computer.

Section 5 Technical description

5.1 IEC 60870-5-104 Protocol

The IEC Technical Committee 57 (Working Group 03) has developed a protocol standard for telecontrol, teleprotection and associated telecommunications for electric power systems. The result of this work is IEC 60870-5. The first five documents listed in Section 2.4 specify the base of IEC 60870-5.

The IEC Technical Committee 57 has also generated a companion standard IEC 60870-5-104 for telecontrol equipment and systems with coded bit serial data transmission TCP/IP based networks for monitoring and controlling geographically widespread processes.

The IEC 60870-5-104 protocol standard defines that transferred data entities in the station object are equal to the ones used in the IEC 60870-5-101 protocol. The implementation of the IEC 60870-5-104 protocol uses the same STA objects as the IEC 60870-5-101 implementation.

IEC 60870-5-104 is designed according to a selection of transport functions given in the TCP/IP Protocol Suite (RFC 2200). Various network types can be utilized within TCP/IP, including X.25, FR (Frame Relay), ATM (Asynchronous Transfer Mode), ISDN (Integrated Service Data Network), Ethernet and serial point-to-point (X.21). Figure 3 shows the protocols used in different layers.

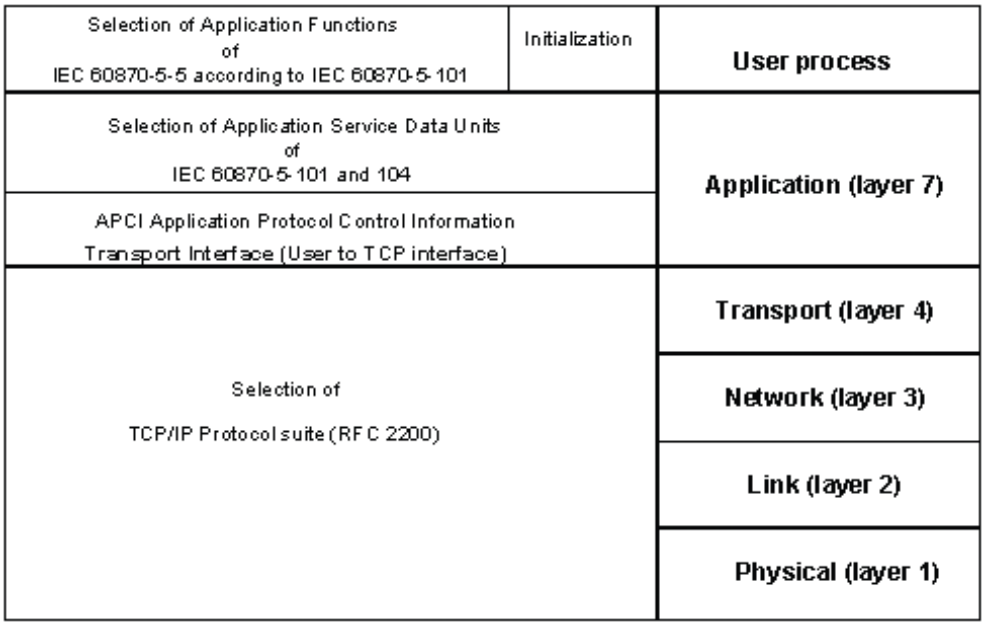


Figure 3: The protocols used in different layers

5.2 Level of implementation

In IEC 60870-5-104 the application level messages are called Application Service Data Units (ASDUs). Each ASDU consists of one or several information objects that contain the actual user data. SYS600 supports the ASDUs presented in Section 5.6

For more information, see Section 5.6.

5.3 Communication

This section gives a more detailed description of the implementation of the IEC 60870-5-104 Master protocol in SYS600, describing also the attributes that can be used for device communication. Examples of how to exchange data between the master and the slave are also given in this section along with information of the IEC 60870-5-104 Master status codes.

5.3.1 Protocol converter

Each IEC 60870-5-104 Master station configured on a line of a NET unit acts as a protocol converter between the IEC 60870-5-104 protocol and a base system. An internal protocol of SYS600 is used in communication between the SYS600 nodes, for example, between a base system and a NET unit.

5.3.2 Addressing

In IEC 60870-5-104, there are two kinds of addresses:

- **Station address**: A common address of an ASDU. There can be several common addresses of an ASDU with the same link address. This address is defined by the SA (Station Address) attribute of the IEC station.
- **Signal address**: An information object address. This address is unique for each signal with the same common address of an ASDU. The Information object address can be given in two ways:
    - As an unstructured address, which is basically just an integer within the range of the information object address.
    - As a structured address which is given byte-wise so that each byte usually represents a level in a hierarchical structure. For example, upper byte = unit number and lower byte = signal address.

SYS600 supports only unstructured addresses. However, this does not prevent communication with the IEC 60870 slaves using structured addresses, since the two types of addresses just demonstrate two different ways of presenting the same address. For example, a two-byte address can be represented as follows:

unstructured = 256*upper byte + lower byte

The station attributes SL, CL and IL define the lengths of station address, cause of transmission and information object address, and these values must match the configuration in the slave devices.

See attribute descriptions for more information.

In IEC 60870-5-104 protocol, the lengths of these fields have been defined in the standard and the values of SL, CL and IL should not be modified from their defaults.

In SYS600 both the input and output process objects share the same address range, which means that there cannot be two process objects with overlapping addresses. If the same address is needed for an input and output object, it can be achieved by using offsets that are outside the information address range limited by the IL attribute. The offset used must be large enough to set only the bits of the information object address that are more significant than the bits within the IL range. The recommended offset is 2000000 (hex) = 33554432 (decimal).

Example:

STAn:SIL = 3, 24 bit addresses

Overlapping information object address 2000 (decimal)

Offset = 33554432 (decimal) = 2000000 (hex)

Address for indication = 2000 (decimal)

Address for command = 2000 + 33554432 = 33556432 (decimal)

5.3.3 Device communication attributes

GI	General Interrogation
Data type:	Integer or vector
Value:	Vector (ENA,[QOI]) or integer 1
Access:	No limitations
Description of the vector parameters:	
ENA:	Activate (value 1) or deactivate (value 0) interrogation
QOI:	Qualifier of interrogation
Value 20:	General interrogation
Values 21…36:	Interrogation for groups 1…16

SY	Synchronize

The SY attribute is used to make an accurate time synchronization of the IEC 60870 stations. No time arguments are needed since the time sent in the synchronization message is taken from the internal clock of SYS600.
Clock synchronization may be used in configurations where the maximum network delay is less than the required accuracy of the clock in the receiving station. For example, if the network provider guarantees that the delay in the network is no more than 400 ms (a typical X.25 WAN value) and the required accuracy in the controlled station is 1 second, the clock synchronization procedure is useful.
The usage of time synchronization with secure authentication according to IEC/TS 62351-5 is not recommended because of significantly lower accuracy.

Data type:	Vector
Value:	Vector (COT, [BRO,[ADDR]])
Access:	Write only
Description of the vector parameters:	
COT:	Cause of transmission of the synchronization messages. Valid values: 6 = activate, 8 = deactivate.
BRO:	Value must be 0, broadcast is not supported in IEC 60870-5-104 Master.
ADDR:	Information object address of the synchronization message. In most cases value 0 is correct. If omitted, value 0 is assumed.

CO	Command Out

The CO attribute can be used for generating command messages, that is, requests, to IEC 60870 slave stations. All kinds of commands can be generated data commands, application commands and system commands. Parameters in the command direction are also sent by using the CO attribute.
The data content of the command is given as transparent data octet by octet. Note that the user is responsible for the validity of the data content. For more information, refer to the IEC 60870-5-104 standards listed in Section 2.1.

Data type: Vector

Value: Vector (TYPE, ADDR,COT,DATA)

Value range: 0...255, when IL attribute = 1
0...65535, when IL attribute = 2
0...16777215, when IL attribute = 3

Access: Write-only

Description of the vector parameters:

TYPE: Type identification of the ASDU, integer. This parameter can be a type identification given in the IEC 60870-5-104 companion standard or a private one. All ASDU types listed in the interoperability list are valid values for TYPE.

ADDR: Information object address of the command, integer.

COT: Cause of transmission of the message, integer. This parameter describes the reason why a message is sent. The causes of transmission shown in Table 1 are commonly used when using the CO attribute.

Table 1: The causes of transmission valid for the CO attribute

COT	Description
3	Spontaneous
5	Request
6	Activation
8	Deactivation

DATA: The set of information objects of the command as integers. Each integer corresponds to one octet in the IEC message.

Some examples of the use of the CO attribute are presented below. See also the examples of the data, application and system commands later in this document.

```
;general interrogation
#SET STA'STA_NR':SCO = (100,0,6,20)
;close select command, double command, address 1000
#SET STA'STA_NR':SCO = (46,1000,6,128+1)
;test command
#SET STA'STA_NR':SCO = (104,0,6,170,85)
```

TD	Transparent Data

The TD attribute is used for sending transparent data (for example SPA messages) to the IEC slave.

Data type: Vector
Value Vector (TYPE, ADDR, COT, TDT)

Value range: 0...255, for other parameters but ADDR

Table continues on next page

TD	Transparent Data
Access:	Write-only

Description of the vector parameters:

TYPE: Type identification of the ASDU, integer. The type identifications shown in Table 2 are allowed when transparent data is sent to the IEC master/slave by using the TD attribute.

Table 2: The type identifications allowed when using the TD attribute

Type id	ASDU	Description
131	C_SR_NA_1	Parameter, byte string
133	C_SB_NA_1	101 Encapsulated SPA bus message

ADDR: Information object address, integer

Value range: 0...255, when IL attribute = 1
0...65535, when IL attribute = 2
0...16777215, when IL attribute = 3

COT: Cause of transmission of the message, integer.

TDT: Transparent data (for example SPA message) as a text string

For more detailed information, see the examples and the interoperability list later in this document.

5.3.4 Data in monitoring direction

Data in the monitoring direction, that is, from the slave to the master, is received by IEC type process objects. Data in the monitoring direction includes, for example double indications and measured values. The relation between the IEC 60870-5-104 ASDUs and SYS600 process object types is presented in tables below.

The following table refers to ASDU types containing short time tags. These ASDU types are supported in order to provide compatibility with devices doing a direct conversion from IEC60870-5-101 to IEC60870-5-104.

Table 3: Relations between the SYS600 process object types and IEC 60870-5-104 ASDUs

Type id	Description	Process Object Type
1, 30	Single point information	Binary input
3, 31	Double point information	Double binary input
5, 32	Step position information	Analog input
9, 11, 13, 34, 35, 36	Measured value	Analog inputs
15, 37	Integrated totals	Pulse counter
7, 33	32-bit bitstring	Bit stream

Both static data (non-time-tagged data) and events (time-tagged data) with the same information object address are received by the same process object. When SYS600 receives an IEC 60870-5-104 message, the process object attributes in Table 4 are updated based on the information in the IEC 60870-5-104 message:

Table 4: Process object attributes updated from an IEC 60870-5-104 message

Attribute	Values	Description
TY	0…44	Type identification of the ASDU.
OV	-	Value of the information object. Data type depends on the ASDU.
OS	0…10	Object status, calculated from the qualifier descriptor bits of the information object.
QL	0…255	Qualifier byte of the information object.
IV (OS=1)	0, 1	Invalid bit of the qualifier.
NT(OS=2)	0, 1	Not topical bit of the qualifier.
BL	0, 1	Blocked bit of the qualifier.
SB	0, 1	Substituted bit of the qualifier.
OR	0, 1	Overflow bit of the qualifier. Only with analog input process objects.
OF	0, 1	Counter overflow bit of the qualifier. Only with pulse counter process objects.
CT	0…63	Cause of transmission of the message.
OG	0...255	Originator address of the message.
RT	Time	Time tag of the information object (time-tagged data), or system time (non-time-tagged data).
RM	0…999	Milliseconds of the information object (time-tagged data), or system time (non-time-tagged data).

For each information object in the received message, there is a qualifier octet that consists of a set of qualifier descriptor bits each of which indicates a property of the information object. Each qualifier descriptor bit updates a process object attribute as shown in Table 5. The whole qualifier octet is set to the QL attribute of the process object. The qualifier descriptor bits and their descriptions along with related process object types are given in the table below.

Table 5: Qualifier descriptor bits

Bit	Name	Description	Process Object Type
IV	Invalid	The value is valid, if it was acquired correctly. After the acquisition function recognizes abnormal conditions of the information source (missing or non-operating updating devices) the value is marked invalid. The value of the information object is not defined under this condition. The mark Invalid is used to indicate to the master that the value may be incorrect and cannot be used.	All
NT	Not topical	A value is topical if the most recent update was successful. It is not topical, if it was not successfully updated during a specified time interval or it is unavailable.	All
SB	Substituted	The value of the information object is provided by input of an operator (dispatcher) or by an automatic source.	All
BL	Blocked	The value of the information object is blocked for transmission; the value remains in the state that was acquired before it was blocked. Blocking and deblocking may be initiated, for example, by a local lock or a local automatic cause.	All

Table continues on next page

Bit	Name	Description	Process Object Type
CA	Counter adjusted	Counter was / was not adjusted since the last reading.	PC
OV	Overflow	The value of the information object is beyond a predefined range of value (mainly applicable to analogue values).	AI
CY	Carry	Counter overflow occurred / did not occur in the corresponding integration period	PC

A timestamp included in the timestamped data messages contains a status bit where the slave can mark the timestamp as invalid. Usually this means that the slave should be synchronized by the master. The value of the OS (Object Status) attribute of an input process object is calculated from the qualifier descriptor bits as in the following:

```
if IEC_IV then (*invalid bit set*)
OS := 1
elsif IEC_NT then (*not topical bit set*)
OS := 2
elsif IEC_Timetag_IV then (*time invalid bit set*)
OS := 3
end_if
```

The following sections give a brief description of each SYS600 input process object type and the corresponding IEC ASDUs.

5.3.4.1 Binary inputs and double binary inputs

Single indications (ASDUs 1 and 30) are received by binary input, and double indications (ASDUs 3 and 31) by double binary indication process objects. Note that in SYS600, the double indication values 1 and 2 are reversed compared to the ones in the IEC 60870 message, in order to make them equal to the double binary values of other master protocols implemented in SYS600.

5.3.4.2 Analog inputs and digital inputs

Measured values (ASDUs 9, 11, 13, 34, 35 and 36) and step position information (ASDUs 6 and 32) can be received by analog input process objects. The value ranges of the ASDUs are as shown in Table 6.

Table 6: Value ranges of measured value and step position ASDUs

Type id	Value type	Value range	Value in SYS600
5, 32	Step position	–64...63	Integer –128…127
9, 34	Normalized	-1…(1-2^-15)	Integer –32768…32767
11, 35	Scaled	–32768…32767	Integer –32768…32767
11, 35	Short floating point	32-bit float	Real

If the value of the measured value sent from the IEC 60870 slave is larger than the value range of the ASDU, the value is limited to the range and the overflow bit of the quality descriptor is set. This bit is sent to the OR attribute of the process object.

Step position information can also be received by digital input process objects. Note that the value range of the step position information is larger in SCIL, since it also contains the transient state bit, which is the second most significant bit of the octet.

5.3.4.3 Pulse counters

Integrated totals (ASDUs 15, 16 and 37) can be received by pulse counter process objects. In IEC 60870-5-104, the pulse counters are 32-bit counters, which have a 5-bit sequence number as the five least significant bits of their qualifier octet. The qualifier octet is set to the QL attribute of the process object.

5.3.4.4 Bit streams

32-bit strings (ASDUs 7 and 33) and transparent data (ASDUs 130 and 131) can be received by bit stream process objects. The message can be converted to an integer vector by using the UNPACK_STR function or to text by using the TYPE_CAST function, see the example below:

```
;convert an unrecognized IEC message to a vector of bytes and find ASDU id
@IEC_MSG = UNPACK_STR('LN':POV'IX',8)
@ASDU_ID = %IEC_MSG(3)
;convert a transparent SPA reply message to text
@SPA_MSG = TYPE_CAST('LN':POV'IX',"TEXT")
```

A special case of the IEC bit stream objects is the one receiving unrecognized messages from the IEC slave. The address of this process object is the same as the CA attribute of the IEC master station.

5.3.5 Data in control direction

Data that is sent from the IEC master to the IEC slave or slaves is called data in control direction. This data includes the data command, application command and system command messages. These messages are described in this section.

5.3.5.1 Command handling in IEC 60870-5-104 protocol

Command confirmation
The IEC 60870-5-104 protocol includes the concept of command confirmations. A confirmation is a message sent by the slave indicating that a command has been received, executed or rejected. Commands are confirmed in two steps as follows:

- A command is **confirmed** when it is received. An activation confirmation can be positive (command accepted) or negative (command rejected). The status ICCC_NEGATIVE_CONFIRMATION indicates of the latter.
- A command is **terminated** when its execution is finished. Activation termination can also be positive (command successfully completed) or negative (command failed).

The following exceptions apply:

- Select-type data commands, Reset process commands (ASDU 105) and Clock synchronization commands (ASDU 103) are only confirmed, not terminated.
- Read commands (ASDU 102) are not confirmed or terminated.

Confirmation and termination messages can be received by analog input or IEC command termination process objects with the UN attribute equal to the STA object number of the IEC master station and the OA attribute equal to command address + offset. Offset is 1000000 hexadecimal = 16777216 decimal. The updating of this process object can be used to indicate the completion of a sent command such as interrogation command, object command or an analog setpoint command. The OV attribute of the process object provides the following information presented in Table 7:

Table 7: Values of the process object receiving activation confirmations and terminations

Values	Description
0	Positive activation confirmation or termination
1	Negative activation confirmation
2	Activation confirmation timeout
3	Activation termination timeout
4	Negative activation termination

The ASDU identification number of the command is updated to the TY attribute of the command process object. This can be used to separate the result of a general interrogation command and the result of a counter interrogation command, both of which can have the same information object address. The length of the activation confirmation and termination timeouts is determined by the RT and CT attributes of the IEC master station, respectively.

Termination messages can be received by analog input or IEC command termination process objects with the UN attribute equal to the STA object number of the IEC 60870-5-103 master station and the OA attribute equal to command address + offset. Offset is 1000000 hexadecimal = 16777216 decimal. The OV attribute of the process object provides the following information presented in Table 8:

Table 8: Values of the process object receiving activation confirmations and terminations

Values	Description
0	Positive acknowledgement
1	Link layer negative acknowledgement received
2	No link layer acknowledgement
3	No command acknowledgement received
4	Negative acknowledgement

The lengths of the activation confirmation and termination timeouts are determined by the RT and CT attributes of the IEC 60870-5-103 master station, respectively.

Command transactions
In the SYS600 implementation of the IEC 60870-5-104 master protocol, one command transaction can be open at the same time. This means that while an IEC master station waits for a termination to a data, application or system command, a new command cannot be issued. The status

13867 ICCC_CONFIRMATION_OF_CMD_IS_NOT_READY

is returned in this situation.

If the RM attribute bit 6 is set, the user can execute parallel commands without having to wait for confirmation of the foregoing commands. The result of the executed command can be read from the process object with command confirmation offset.

5.3.5.2 Data commands

Object commands
Object commands (for example switching device open/close commands, tap changer raise/lower commands) include the ASDUs shown in Table 9. They are sent to the IEC slave by setting a binary output process object or by using the CO attribute of the IEC station. The unit number (UN attribute) of the output process object must be the same as the STA object number of the corresponding IEC master station. The address of the process object must also

equal the address of the command in the IEC slave. IEC object commands are usually select-before-execute commands. The usage of time-tagged command is preferred in IEC 60870-5-104. The corresponding ASDU numbers are 58...60

Table 9: Object command ASDUs

Type id	Description	Process Object Type
45, 58	Single command	Binary output
46, 59	Double command	Binary output
47, 60	Regulating step commands	Binary output

The value set to the process object is a list of attributes. The attributes included in the list are shown in Table 10. Optional attributes are indicated with an asterisk (*).

Table 10: Process object attributes included in an IEC object command

Attr.	Values	Default	Description
SE	-	-	If select command is sent, the parameter list is set to the SE attribute. Otherwise excluded.
TY	45...47 , 58...60	-	Type identification of the ASDU.
OV	0,1,2	-	Value of the command 0 = off, 1 = on (single command, double command), 0 = lower, 1 = higher (regulating step command).
QL*	0... 255	0	Qualifier of the command: 0 = do definition, 1 = short pulse, 2 = long pulse, 3 = persistent output.
CT	6, 8	-	Cause of transmission of the command: 6 = activate, 8 = deactivate.
OG*	0... 255	0	Originator address of the command.

Examples:

```
;time-tagged single command, select off, short pulse
#SET 'LN':PSE'IX' = LIST(OV=0,CT=6,OG=100,TY=58,QL=1)
;time-tagged double command, execute on, long pulse
#SET 'LN':POV'IX' = LIST(OV=1,CT=6,OG=100,TY=59,QL=2)

;single command, select off, short pulse
#SET 'LN':PSE'IX' = LIST(OV=0,CT=6,OG=100,TY=45,QL=1)
;single command, execute offn, short pulse
#SET 'LN':POV'IX' = LIST(OV=0,CT=6,OG=100,TY=45,QL=1)
;single command, cancel (deactivate) off, short pulse
#SET 'LN':POV'IX' = LIST(OV=0,CT=8,OG=100,TY=45,QL=1)
;double command, execute on, long pulse
#SET 'LN':POV'IX' = LIST(OV=1,CT=6,OG=100,TY=46,QL=2)
;regulating step command, execute lower, persistent output
#SET 'LN':POV'IX' = LIST(OV=0,CT=6,OG=100,TY=47,QL=3)
```

Analog setpoints

Analog setpoints (ASDUs 48, 49 and 50) can be sent by using the CO attribute or by setting an analog output process object. The unit number (UN attribute) of the process object must be the same as the STA object number of the corresponding IEC slave station. The address of the process object must also equal the address of the command in the IEC slave. IEC setpoint commands are usually direct (only execute sent) commands. The usage of time-tagged analog set-points is preferred in IEC60870-5-104. The corresponding ASDU numbers are 61...63.

There are three different types of analog setpoint values as presented in Table 11. Note that both the normalized and scaled values are handled as signed 16-bit integers in SYS600.

Table 11: Value ranges of setpoint ASDUs

Type id	Value type	Value range	Value in SYS600
48, 61	Normalized	-1…(1-2^-15)	Integer –32768…32767
49, 62	Scaled	–32768…32767	Integer –32768…32767
50, 63	Short floating point	32-bit float	Real

The value set to the process object is a list of attributes. The attributes included in the list are shown in Table 12. Optional attributes are indicated with an asterisk (*).

Table 12: Process object attributes included in an IEC 60870 setpoint command

Attr.	Values	Default	Description
TY	48... 50, 61... 63	-	Type identification of the ASDU
OV	0, 1, 2	-	Value of the command depending on the ASDU
QL*	0... 255	0	Qualifier of the command (no standard definitions yet)
CT	6, 8	-	Cause of transmission of the command: 6 = activate, 8 = deactivate
OG*	0... 255	0	Originator address of the command

Examples:

```
;time-tagged normalised setpoint command, execute
#SET 'LN':POV'IX' = LIST(OV=5000,CT=6,OG=100,TY=61,QL=0)
;time-tagged scaled command, cancel (deactivate)
#SET 'LN':POV'IX' = LIST(OV=100,CT=8,OG=100,TY=62,QL=0)

;normalised setpoint command, execute
#SET 'LN':POV'IX' = LIST(OV=5000,CT=6,OG=100,TY=48,QL=0)
;scaled command, cancel (deactivate)
#SET 'LN':POV'IX' = LIST(OV=100,CT=8,OG=100,TY=49,QL=0)
```

Bitstring commands

Bitstring command (ASDU 51) can be sent by setting a process object of type bitstream. The unit number (UN attribute) of the process object must be the same as the STA object number of the corresponding IEC slave station. The address of the process object must also equal the address of the command in the IEC slave. IEC bitstring commands are always direct (only execute sent) commands. The usage of time-tagged bitstring command (ASDU 64) is preferred with IEC60870-5-104.

Sending of the bitstring commands is possible using the CO-attribute, too.

The value set to the process object is a list of attributes. The attributes included in the list are shown in Table 13. Optional attributes are indicated with an asterisk (*).

Table 13: Process object attributes included in an IEC 60870 bitstring command

Attr.	Values	Default	Description
TY	51, 64	-	Type identification of the ASDU
BS	bitstring of max. 32 bits	-	Value of the command depending on the ASDU
CT	6	-	Cause of transmission of the command: 6 = activate
OG*	0... 255	0	Originator address of the command

Examples:

```
;time-tagged bitstring command
#SET 'LN':POV'IX' =
list(BS=pack_str((1,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,1,0,0,1,
1,0,1,1),
"BIT_STRING",1),TY=64,CT=6)

;non-timetagged bitstring command
#SET 'LN':POV'IX' =
list(BS=pack_str((1,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,1,0,0,1,
1,0,1,1),
"BIT_STRING",1),TY=51,CT=6)
```

5.3.5.3 Application commands

Application commands include the ASDUs shown in Table 14. All application commands are sent with address zero.

Table 14: IEC 60870-5-104 application commands

Type id	ASDU	Description
100	C_IC_NA_1	Interrogation command
101	C_CI_NA_1	Counter interrogation command
102	C_RD_NA_1	Read command
105	C_RP_NA_1	Reset process command

General interrogation command
When the IEC slave station receives a general interrogation command (ASDU 100) from the master, it must send all the input signals except the pulse counters to the master without a time tag. The cause of transmission is set to 20. IEC 60870-5-104 also includes a group interrogation function. When this function is used, the signals to be sent to the IEC master are divided into groups which can be interrogated one at the time. The cause of transmission is set to 20 + group number. Interrogation commands can be sent by using the GI or CO attributes of the IEC master station as shown in the examples below.

```
;activate general interrogation
#SET STA'STA_NR':SGI = 1
;activate group interrogation
@GROUP = 1 ; 1..16
#SET STA'STA_NR':SCO = (100,0,6,20+%GROUP)
```

Counter interrogation command
The counter interrogation command is like a general interrogation but only for integrated totals (pulse counters). A counter interrogation can also be a group interrogation. In this case, the number of the groups is four. The cause of transmission of the interrogated pulse

counters are 37 in the case of a counter interrogation, or 37 + group number in the case of a group counter interrogation. A counter interrogation command can be sent by using the CO attribute as shown below:

```
;activate counter interrogation
#SET STA'STA_NR':SCO = (101,0,6,5)
;activate group counter interrogation
@GROUP = 1 ; 1..4
#SET STA'STA_NR':SCO = (101,0,6,%GROUP)
```

The meaning of the fourth byte comes directly from the standard:

Bits 0...5:

0 = no counter requested

1 = request counter group 1

2 = request counter group 2

3 = request counter group 3

4 = request counter group 4

5 = general request counter

Bits 6...7:

0 = no freeze or reset

1 = counter freeze without reset

2 = counter freeze with reset

3 = counter reset

Read command
By using the read command (ASDU 102), the user can request the value of an individual signal from the IEC master. The requested signal is sent with the cause of transmission value 5. Note that pulse counters are not included in the read command.

A read command can be sent by using the CO attribute as shown below:

```
;read of user data command
@ADDR = 255 ; information object address
#SET STA'STA_NR':SCO = (102,%ADDR,5)
```

Reset process command
The purpose of the reset process command (ASDU 105) is to re-initialize the application level of the IEC slave station. It can be sent by using the CO attribute as shown below:

```
;activate reset process command
#SET STA'STA_NR':SCO = (105,0,6,1)
```

5.3.5.4 System commands

System commands include the ASDUs presented in Table 15. All the application commands are sent with address zero by default. The address of the clock synchronization command can be changed by using the ADDR parameter of the SY (Synchronize) attribute.

Table 15: IEC 60870-5-104 system command ASDUs

Type id	ASDU	Description
103	C_CS_NA_1	Clock synchronization command

Clock synchronization command
The clock synchronization commands (ASDU 103) are used for synchronizing IEC slave stations. This command can be sent by using the SY attribute of the IEC master station as shown below:

```
;activate synchronization for one station
#SET STA'STA_NR':SSY = 6
;deactivate synch to one station
#SET STA'STA_NR':SSY = (8,0)
```

Test command
By sending a test command (ASDU 107) to the IEC slave, the IEC master can check that the connection to the application level of the slave is working properly. A test command can be sent by using the CO attribute as shown below. The command is time-tagged and it is worth it to check that master and slave are synchronized.

```
@CMD = 107
@FULLTIME = TIMEMS
@CMD_STA = 1
@IOA = 0
@SU=0 ; summertime

@YEAR = DEC_SCAN(SUBSTR(%FULLTIME, 1,2))
@MONTH = DEC_SCAN(SUBSTR(%FULLTIME, 4,2))
@DAY = DEC_SCAN(SUBSTR(%FULLTIME, 7,2))
@HOUR = DEC_SCAN(SUBSTR(%FULLTIME, 10,2))
@MINUTE = DEC_SCAN(SUBSTR(%FULLTIME, 13,2))
@MSECS = DEC_SCAN(SUBSTR(%FULLTIME,
16,2))*1000+DEC_SCAN(SUBSTR(%FULLTIME, 19,3))
@MSECSL = %MSECS mod 256
@MSECSH = %MSECS div 256
#IF STA'CMD_STA':SOS==0 #THEN #BLOCK
  #SET STA'CMD_STA':SCO=(%CMD,%IOA, 6, 170,85,%MSECSL,
%MSECSH,%MINUTE,%HOUR+128*%SU,%DAY,%MONTH,%YEAR)
#BLOCK_END
```

5.3.6 Transparent data commands

It is possible to exchange transparent messages between a SYS600 IEC slave and an IEC master. SPA messages are an example of these kinds of messages. Transparent SPA messages are sent as commands to the slave by using the TD attribute of the IEC master station and received in bit stream process objects.

The example shown in Figure 4 has two SYS600 base systems, one as the network control system (IEC master) and one as the substation control system (IEC slave). The latter also acts as the master for several SPA devices. In this example a transparent SPA command is sent from the IEC master to the SPA unit via the SYS600 IEC slave and the answer from the SPA unit is sent back to the IEC master. The following steps are taken according to Figure 4.

Step **1**: The SPA command "RF:" is sent from the IEC master to the IEC slave as an encapsulated SPA message (ASDU 133) to address 12345 by using the TD attribute as in the following:

```
#SET STA1:STD = (133,12345,6,”RF:”)
```

Step **2** and **3**: The SPA reply message is received by the IEC slave in a bit stream process object with the UN attribute equal to the STA object number of the IEC slave station and the OA attribute value equal to the address of the command, which is 12345 in this case. Attached to this process object is an event channel, which activates a command procedure. The SPA message is parsed by the command procedure as in the following:

```
@SPA_MSG = TYPE_CAST(%BS,"TEXT")
```

The SPA message is sent to the SPA unit and the corresponding answer is read by using the SM attribute of the SPA station as in the following:

```
#SET STA2:SSM = %SPA_MSG
@SPA_ANSW = STA2:SSM
```

Step **4**: The answer is sent back to the IEC master as an activation confirmation of the command, that is, the encapsulated SPA reply message, as in the following:

```
@IEC_STA_NR = 'LN':PUN'IX'
@ORIG = 'LN':POG'IX'
@CMD_ADDR = 'LN':POA'IX'
@CMD_TYPE = 'LN':PTY'IX'
#SET STA'IEC_STA_NR':SCF = -
(256*%ORIG+7,%CMD_ADDR,%CMD_TYPE,%SPA_ASW)
```

The message is received by the IEC master in a bit stream process object with the UN attribute equal to the STA object number of the IEC slave station and the OA equal to the address of the command. In this case, the message can also be interpreted using the TYPE_CAST function to convert the message into text.

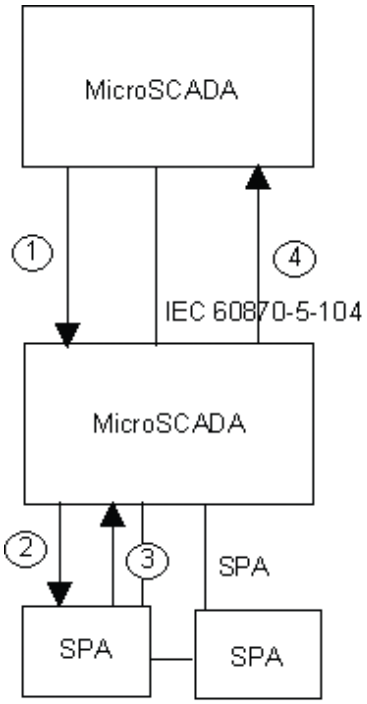


Figure 4: Flow of the transparent SPA messages

By using a mechanism like the one described above, it is possible to read and write the parameters of SPA units over an IEC 60870-5-104 line. The same kind of mechanism can also be used for other purposes, for example exchanging free-format text messages between the master and the slave.

5.3.7 Parameter in control direction

In the IEC 60870-5-104 protocol it is possible for the master to set and activate parameters of information objects of the IEC slave. This kind of action is, for example, setting the limits of a measured value. The following ASDUs presented in Table 16 are provided by the protocol:

Table 16: ASDUs for parameters in the control direction

Type id	ASDU	Description
110	P_ME_NA_1	Parameter of measured values, normalized value.
111	P_ME_NB_1	Parameter of measured values, scaled value.
112	P_ME_NC_1	Parameter of measured values, short floating point number.
113	P_AC_NA_1	Parameter activation.

All of these ASDUs can be sent using the CO attribute of the IEC master station. See the description of the CO attribute in Section 5.3.3 for more details.

ASDUs 110…112 are for setting the parameters of measured values. The syntax is as in the following:

```
#SET STAn:SCO = (TYPE, ADDR,COT,VALUE,QUAL)
```

The elements of the argument vector set to the CO attribute are shown in Table 17.

Table 17: The arguments used when sending parameters of the measured value ASDUs

Argument	Description
TYPE	Type identification of the ASDU, integer 110…112.
ADDR	Information object address of the target measured value object.
COT	Cause of transmission, integer 6.
VALUE	Value of the parameter as normalized value (ASDU 110), scaled value (ASDU 111) or short floating point number (ASDU 113).
QUAL	Qualifier of the ASDU as follows: 1 = threshold value, 2 = smoothing factor, 3 = low limit, 4 = high limit.

When sending a parameter activation message (ASDU 113), the syntax of the CO attribute is in the following. Table 18 describes the values of the elements in the argument vector.

```
#SET STAn:SCO = (TYPE, ADDR,COT,QUAL)
```

Table 18: The arguments used when sending the parameter activation ASDUs

Argument	Description
TYPE	Type identification of the ASDU, integer 113.
ADDR	Information object address of the target object.
COT	Cause of transmission, integer 6 = activate, 8 = deactivate.
QUAL	Qualifier of the ASDU as follows: 1 = act/deact of the previously loaded parameters (addr 0), 2 = act/deact of the parameter of the addressed object, 3 = act/deact of persistent cyclic or perodic transmission of the addressed object.

Examples:

```
;send the low limit 100 of the object with address 1500 as scaled value
#SET STA1:SCO = (111,1500,6,100,3)
;deactivate the previous parameter setting
#SET STA1:SCO = (113,1500,8,2)
```

5.4 Signal engineering

The term signal engineering here means the engineering needed to establish communication to the IEDs using the IEC protocol. In order to create the process object database, the data types and the addresses of the data points used by each remote device need to be identified. When system configuration is completed, communication to the IEDs is possible but the utilization of the functions of the IEDs is not possible until the process object database is created. The principal sequence for the signal engineering is:

1. Make a list of all signals that are to be transferred between the master and the slave. Create the corresponding process objects. No data poll definitions are needed since IEC60870-5-104 uses spontaneous data transmission.
2. Determine the need for the general interrogations and time synchronizations and make the necessary application changes.
3. Test each signal.

5.5 Status codes

The status codes for the IEC 60870-5-104 Master protocol are defined in the SYS600 Status Codes manual. Some typical reasons for some of the status codes are also given.

Status codes are sent as system messages which can be received by analog input project objects with a unit number (UN) 0 and an object address (OA) as determined by the MI attribute of the line or station, or alternatively, they are returned as a response to a SCIL command accessing a IEC station object.

5.6 Interoperability list

5.6.1 Interoperability

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of "structured" or "unstructured" fields of the INFORMATION OBJECT 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 both command and 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 interoperability list is defined as in IEC 60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters which are not applicable to this companion standard are strike-through (corresponding check box is marked black).

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

5.6.1.1 Application layer telegram formats

The selected parameters should be marked in the white boxes as follows:

- ☐ 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
- ☒ A Function or ASDU may need some additional application level work

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

A black check box indicates that the option cannot be selected in this companion standard.

5.6.1.2 System or device

(system-specific parameter)

- ☐ System definition
- ☒ Controlling station definition (Master)
- ☐ Controlled station definition (Slave)

5.6.1.3 Network configuration

(network-specific parameter)

- ■ ~~Point-to-point~~
- ■ ~~Multiple point-to-point~~
- ■ ~~Multipoint-partyline~~
- ■ ~~Multipoint-star~~

5.6.1.4 Physical layer

(network-specific parameter)

Transmission speed (control direction)

Unbalanced interchange Circuit V.24/V.28 Standard		Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s		Balanced interchange Circuit X.24/X.27			
■	~~100 bit/s~~	■	~~2400 bit/s~~	■	~~2400 bit/s~~	■	~~56000 bit/s~~
■	~~200 bit/s~~	■	~~4800 bit/s~~	■	~~4800 bit/s~~	■	~~64000 bit/s~~
■	~~300 bit/s~~	■	~~9600 bit/s~~	■	~~9600 bit/s~~		
■	~~600 bit/s~~			■	~~19200 bit/s~~		
■	~~1200 bit/s~~			■	~~38400 bit/s~~		

Transmission speed (monitor direction)

Unbalanced interchange Circuit V.24/V.28 Standard		Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s		Balanced interchange Circuit X.24/X.27			
■	~~100 bit/s~~	■	~~2400 bit/s~~	■	~~2400 bit/s~~	■	~~56000 bit/s~~
■	~~200 bit/s~~	■	~~4800 bit/s~~	■	~~4800 bit/s~~	■	~~64000 bit/s~~
■	~~300 bit/s~~	■	~~9600 bit/s~~	■	~~9600 bit/s~~		
■	~~600 bit/s~~			■	~~19200 bit/s~~		
■	~~1200 bit/s~~			■	~~38400 bit/s~~		

5.6.1.5 Link layer

(network-specific parameter)

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

Link transmission

■	~~Balanced transmission~~
■	~~Unbalanced transmission~~

Address field of the link

■	~~Not present (balanced transmission only)~~
■	~~One octet~~
■	~~Two octets~~
■	~~Structured~~
■	~~Unstructured~~

Frame length

■	~~Maximum length L (number of octets)~~

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
9, 11, 13, 21	<1>

■ ~~A special assignment of ASDUs to class2 is used as follows:~~

Type identification	Cause of transmission

5.6.1.6 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)

■ ~~One octet~~ ☒ Two octets

Information object address
(system-specific parameter)

■ ~~One octet~~ ☐ Structured

■ ~~Two octets~~ ☒ Unstructured

☒ Three octets

Cause of transmission
(system-specific parameter)

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

Length of APDU
(system-specific parameter)

The maximum length of APDU for both directions is 253. It is a fixed system parameter.

■ Maximum length of APDU per system in control direction

■ Maximum length of APDU per system in monitor direction

Selection of standard ASDUs
Process information in monitor direction

(station-specific parameter)

☒	<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~~
☒	<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_PS_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

Table continues on next page

☒	<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
☒	<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

Although ASDUs <2>, <4>, <6>, <8>, <10>, <12>, <14> and <16> are not part of the IEC 60870-5-104 companion standard, they are also supported to provide compatibility with gateway devices using IEC 60870-5-101.

Process information in control direction
(station-specific parameter)

☒	<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 time tag CP56Time2a	C_SC_TA_1
☒	<59> := Double command with time tag CP56Time2a	C_DC_TA_1
☒	<60> := Regulating step command with time tag CP56Time2a	C_RC_TA_1
☒	<61> := Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
☒	<62> := Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☒	<63> := Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
☒	<64> := Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

System information in monitor direction
(station-specific parameter)

☒	<70> := End of initialization	M_EI_NA_1

System information in control direction
(station-specific parameter)

X	<100>:= Interrogation command	C_IC_NA_1
X	<101>:= Counter interrogation command	C_CI_NA_1
X	<102>:= Read command	C_RD_NA_1
X	<103>:= Clock synchronization command	C_CS_NA_1
■	~~<104>:= Test command~~	~~C_TS_NA_1~~
X	<105>:= Reset process command	C_RP_NA_1
■	~~<106>:= Delay acquisition command~~	~~C_CD_NA_1~~
A	<107>:= Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in control direction
(station-specific parameter)

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

File transfer
(station-specific parameter)

B	<120>:= File ready	F_FR_NA_1
B	<121>:= Section ready	F_SR_NA_1
B	<122>:= Call directory, select file, call file, call section	F_SC_NA_1
B	<123>:= Last section, last segment	F_LS_NA_1
B	<124>:= Ack file, ack section	F_AF_NA_1
B	<125>:= Segment	F_SG_NA_1
X	<126>:= Directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1
☐	<127>:= Query Log – Request archive file	F_SC_NB_1

Type identifier and cause of transmission assignments
(station-specific parameters)

Shaded boxes are not required.

Blank = function or ASDU is not used.

Mark type identification/cause of transmission combinations:

"**X**" if used only in the standard direction

"**R**" if used only in the reverse direction

"**B**" if used in both directions

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X						X	X		X					
~~<2>~~	~~M_SP_TA_1~~			■		■						■	■							
<3>	M_DP_NA_1		X	X		X						X	X		X					
~~<4>~~	~~M_DP_TA_1~~			■		■						■	■							
<5>	M_ST_NA_1		X	X		X						X	X		X					
~~<6>~~	~~M_ST_TA_1~~			■		■						■	■							
<7>	M_BO_NA_1		X	X		X									X					
~~<8>~~	~~M_BO_TA_1~~			■		■														
<9>	M_ME_NA_1	X	X	X		X									X					
~~<10>~~	~~M_ME_TA_1~~			■		■														
<11>	M_ME_NB_1	X	X	X		X									X					
~~<12>~~	~~M_ME_TB_1~~			■		■														
<13>	M_ME_NC_1	X	X	X		X									X					
~~<14>~~	~~M_ME_TC_1~~			■		■														
<15>	M_IT_NA_1			X												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																			

Table continues on next page

Type identification		Cause of transmission																		
<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						X	X							
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<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																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X						X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X

Table continues on next page

Type identification		Cause of transmission																		
<63>	C_SE _TC_1						X	X	X	X	X						X	X	X	X
<64>	C_BO _TA_1						X	X			X						X	X	X	X
<70>	M_EI_ NA_1				X															
<100 >	C_IC_ NA_1						X	X	X	X	X						X	X	X	X
<101>	C_CI_ NA_1						X	X	X	X	X						X	X	X	X
<102>	C_RD _NA_1					X											X	X	X	X
<103>	C_CS _NA_1			■			X	X									X	X	X	X
~~<104 >~~	~~C_TS _NA_1~~						■	■									■	■	■	■
<105>	C_RP _NA_1						X	X									X	X	X	X
~~<106 >~~	~~C_CD _NA_1~~			■			■	■									■	■	■	■
<107>	C_TS _TA_1						A	A									A	A	A	A
<110>	P_ME _NA_1						A	A							A		A	A	A	A
<111>	P_ME _NB_1						A	A							A		A	A	A	A
<112>	P_ME _NC_ 1						A	A							A		A	A	A	A
<113>	P_AC _NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_ NA_1													B			X	X	X	X
<121>	F_SR_ NA_1													B			X	X	X	X
<122>	F_SC_ NA_1					X								B			X	X	X	X
<123>	F_LS_ NA_1													B			X	X	X	X
<124>	F_AF_ NA_1													B			X	X	X	X
<125>	F_SG _NA_1													B			X	X	X	X
<126>	F_DR _TA_1 *			X		X														
<127>	F_SC_ NB_1*																			
	* Blank or X only.																			

5.6.1.7 Basic application functions

Station initialization
(station-specific parameter)

- [X] Remote initialization

Cyclic data transmission
(station-specific parameter)

- [X] Cyclic data transmission

Read procedure
(station-specific parameter)

- [X] Read procedure

Spontaneous transmission
(station-specific parameter)

- [X] Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous
(station-specific parameter)

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.

- [ ] Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
- [ ] 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
- [ ] 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 or object-specific parameter)

[X]	global				
[X]	group 1	[X]	group 7	[X]	group 13
[X]	group 2	[X]	group 8	[X]	group 14

Table continues on next page

X	group 3	X	group 9	X	group 15
X	group 4	X	group 10	X	group 16
X	group 5	X	group 11		
X	group 6	X	group 12		

Clock synchronization
(station-specific parameter)

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

Command transmission
(station-specific parameter)

X	Direct command transmission
X	Direct set-point command transmission
X	Select and execute command
X	Select and execute set-point command
X	C_SE ACTTERM used
X	No additional definition
X	Short-pulse duration (duration determined by a system parameter in the controlled station)
X	Long-pulse duration (duration determined by a system parameter in the controlled station)
X	Persistent output
X	Supervision of maximum delay in command direction of commands and set point commands

255 sec	Maximum allowable delay of commands and set point commands

Transmission of integrated totals
(station-specific parameter or object-specific parameter)

- [X] Mode A: local freeze with spontaneous transmission
- [X] Mode B: local freeze with counter interrogation
- [X] Mode C: freeze and transmit by counter interrogation commands
- [X] Mode D: freeze by counter interrogation command, frozen values reported spontaneously

- [X] Counter read
- [X] Counter freeze without reset
- [X] Counter freeze with reset
- [X] Counter reset

- [X] General request counter
- [X] Request counter group 1
- [X] Request counter group 2
- [X] Request counter group 3
- [X] Request counter group 4

Parameter loading
(object-specific parameter)

- [A] Threshold value
- [A] Smoothing factor
- [A] Low limit for transmission of measured value
- [A] High limit for transmission of measured value

Parameter activation
(object-specific parameter)

- [X] Act/deact of persistent cyclic or periodic transmission of the addressed object

Test procedure
(object-specific parameter)

- [A] Test procedure

File transfer
(object-specific parameter)

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)

☒ Background scan

Acquisition of transmission delay
(station-specific parameter)

■ ~~Acquisition of transmission delay~~

5.6.1.8 Definition of time-outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	1-255 s
t_1	15 s	Time-out of send or test APDUs	1-255 s
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	1-255 s
t_3	20 s	Time-out for sending test frames in case of a long idle state	1-255 s

Maximum range for timeouts t0 to t2: 1 s to 255 s, accuracy 1 s.

5.6.1.9 Maximum number of outstanding I format APDUs *k* and latest acknowledge APDUs (*w*)

Parameter	Default value	Remarks	Selected value
k	12 APDUs	Maximum difference receive sequence number to send state variable	1-32767
w	8 APDUs	Latest acknowledge after receiving w I format APDUs	1-32767

Maximum range of values *k*: 1 to 32767 (2^15–1) APDUs, accuracy 1 APDU

Maximum range of values *w*: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: *w* should not exceed two-thirds of *k*).

5.6.1.10 Portnumber

Parameter	Value	Remarks
Portnumber	2404	Configurable with an optional definition to the station attribute IA.

5.6.1.11 Redundant connections

1...12 Number N of redundancy group connections used

5.6.1.12 RFC 2200 suite

RFC 2200 is an official Internet Standard which describes the state of standardization of protocols used on the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used on the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

☒ Ethernet 802.3

☐ Serial X.21 interface

☐ Other selection from RFC 2200:

List of valid documents from RFC 2200

1.
2.
3.
4.
5.
6.
7. etc.

5.7 Description of the SPA bus messages

In distribution automation systems, the SPA-bus protocol may be required to access device information that is not mapped to the IEC 60870-5-101 protocol. This information includes several device specific parameters and recorded disturbance data. Two ASDU types from the private range have been selected to enable transparent transfer of the SPA-bus messages.

ASDU 133 - SPA-bus message

TYPE IDENT 133: C_SB_NA_1

SPA-bus message

Single information object (SQ = 1)

Table 19: ASDU C_SB_NA_1 – SPA-bus message

1	0	0	0	0	1	0	1	TYPE IDENTIFICATION	
1				N*				VARIABLE STRUCTURE QUALIFIER	DATA UNIT
								CAUSE OF TRANSMISSION	IDENTIFIER
								COMMON ADDRESS OF ASDU	
								INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
								SPA-bus command message (in control direction) or SPA-bus reply message (in monitor direction)	

* N defines, in binary format, the number of information elements (characters) in the ASDU. N is a value between 0 and 127.

CAUSES OF TRANSMISSION used with TYPE IDENT 133: = C_SB_NA_1

CAUSE OF TRANSMISSION

In control direction: <6>:=activation

In monitor direction: <7>:=activation confirmation

ASDU 130 - SPA-bus reply message

TYPE IDENT 130: M_SB_NA_1

SPA-bus reply message

Single information object (SQ = 0)

Table 20: ASDU M_SB_NA_1 – SPA-bus reply message

1	0	0	0	0	0	1	0	TYPE IDENTIFICATION	
0	0	0	0	0	0	0	1	VARIABLE STRUCTURE QUALIFIER	DATA UNIT
								CAUSE OF TRANSMISSION	IDENTIFIER
								COMMON ADDRESS OF ASDU	
								INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
								SPA-bus reply message	

CAUSES OF TRANSMISSION used with TYPE IDENT 130: = M_SB_NA_1

CAUSE OF TRANSMISSION

In monitor direction: <5>:= requested

Transfer procedure

Transparent transfer of the SPA-bus messages can be initiated by the controlling station by sending a SPA command message to the controlled station using C_SB_NA_1 ASDU with the

"activation" cause of transmission. The controlled station returns a corresponding SPA reply message using C_SB_NA_1 ASDU with the "activation confirmation" cause of transmission.

The last SPA reply message can also be requested by the controlling station using the Read application function. The controlled station returns the latest SPA reply message using M_SB_NA_1 ASDU with the "requested" cause of transmission. The transfer procedure is presented in Figure 5.

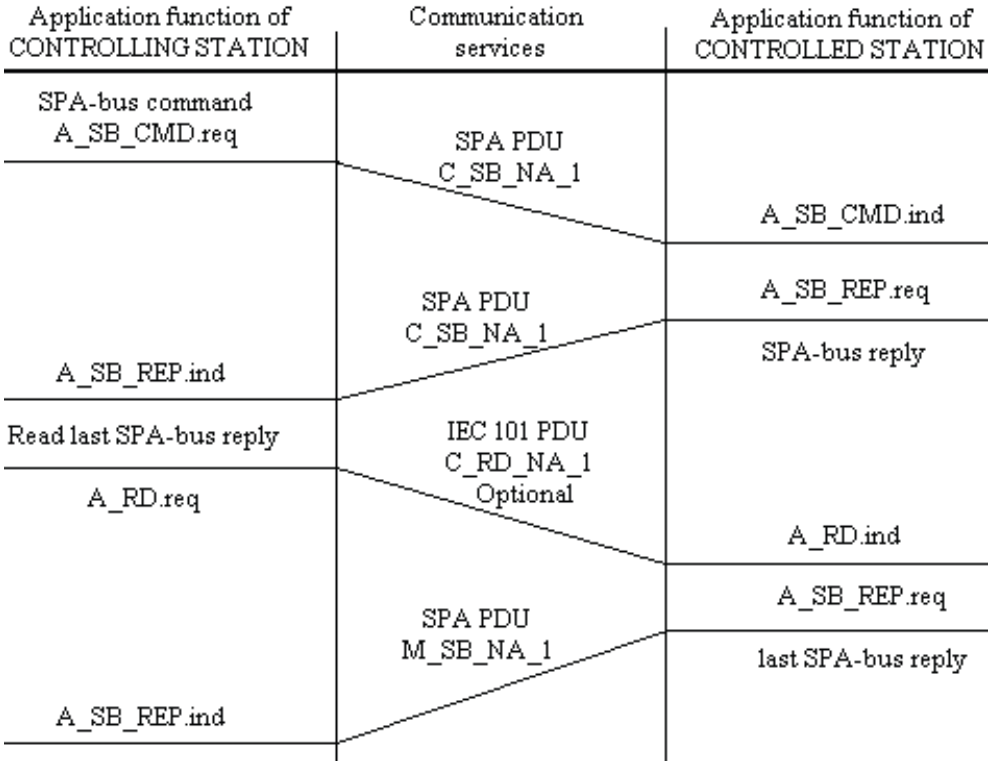


Figure 5: The transfer procedure of transparent SPA-bus protocol

5.8 Description of parameter/byte string messages

In distribution automation systems, several outstation parameters may be accessed as unstructured byte strings (for example, configuration data, device description texts, modem control strings). Two ASDU types from the private range have been selected to enable the parameter setting and parameter reading operations.

ASDU 131 – Parameter, byte string

TYPE IDENT 131: C_SR_NA_1

Parameter, byte string

Single information object (SQ = 0)

Table 21: ASDU C_SR_NA_1 – Parameter, byte string

1	0	0	0	0	0	1	1	TYPE IDENTIFICATION	
0	0	0	0	0	0	0	1	VARIABLE STRUCTURE QUALIFIER	DATA UNIT
								CAUSE OF TRANSMISSION	IDENTIFIER
								COMMON ADDRESS OF ASDU	
								INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
								Character string or byte array	

CAUSES OF TRANSMISSION used with TYPE IDENT 131: = C_SR_NA_1

CAUSE OF TRANSMISSION

In control direction: <6>:=activation

In monitor direction: <7>:=activation confirmation

ASDU 128 – Parameter data, byte string

TYPE IDENT 128: M_SR_NA_1

Parameter, byte string

Single information object (SQ = 0)

Table 22: ASDU M_SR_NA_1 – Parameter data, byte string

1	0	0	0	0	0	1	1	TYPE IDENTIFICATION	
0	0	0	0	0	0	0	1	VARIABLE STRUCTURE QUALIFIER	DATA UNIT
								CAUSE OF TRANSMISSION	IDENTIFIER
								COMMON ADDRESS OF ASDU	INFORMATION OBJECT
								INFORMATION OBJECT ADDRESS	
								Character string or byte array	

CAUSES OF TRANSMISSION used with TYPE IDENT 128: = M_SR_NA_1

CAUSE OF TRANSMISSION

In control direction: <6>:=activation

In monitor direction: <7>:=activation confirmation

Parameter setting and reading procedure

String parameter setting is initiated by the controlling station by sending a parameter value to the controlled station using C_SR_NA_1 ASDU with the "activation" cause of transmission. The controlled station returns an acknowledgement using C_SB_NA_1 ASDU with the "activation confirmation" cause of transmission.

The string parameter value can also be requested by the controlling station by using the Read (ASDU 102, C_RD_NA_1) application function. The controlled station returns the addressed parameter value using M_SR_NA_1 ASDU with the "requested" cause of transmission.

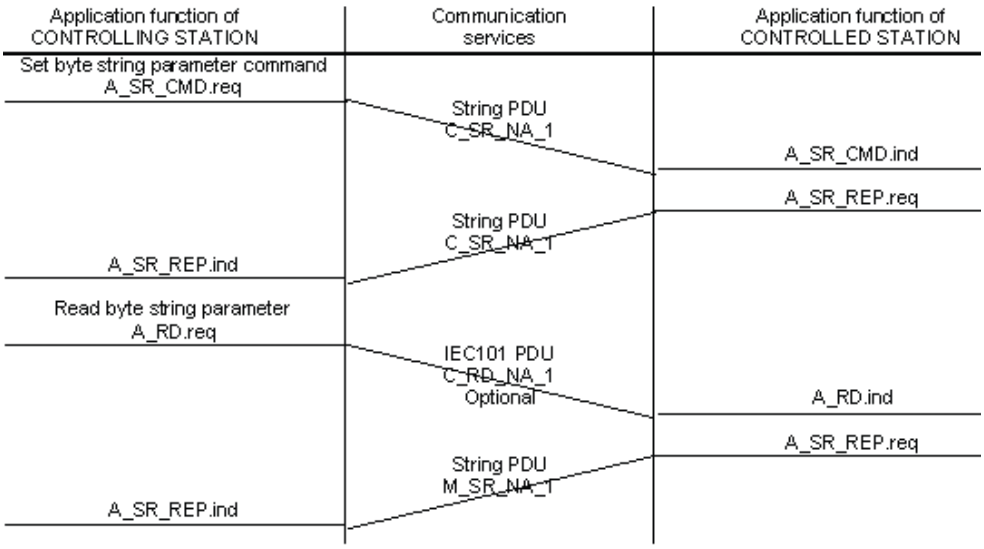


Figure 6: The parameter setting and reading procedure

Appendix A Examples of communication system configuration

The following SCIL procedures make the communication system configuration which is related to the base system configuration example presented earlier in this document. The first procedure creates an IEC 60870-5-104 Master line and two stations on this line.

```
;*************************************************************************
; INPUT PARAMETERS
@NET = 3 ; NODE NUMBER OF THE PC-NET
@LINE = 1 ; LINE NUMBER
@STATIONS = (1,2) ; MASTER STATION NUMBERS
There may be only one connection from the same IP-address in slave to
same IP-address in master. This means that it is not possible to have
 #SET STA1:SIA1="192.168.1.11:1"
 #SET STA1:SIA2="192.168.1.11:1"
but it is possible to have
 #SET STA1:SIA1="192.168.1.11:1"
 #SET STA1:SIA2="192.168.1.11:2"
and (as mentioned before)
 #SET STA1:SIA1="192.168.1.11:1"
 #SET STA1:SIA2="192.168.1.12:1"
@APPLIC = 1 ; APPLICATION NUMBER
;*************************************************************************
; CREATE A IEC 60870-5-104 MSTER LINE TO NET
#IF NET'NET':SPO'LINE'==0 #THEN #BLOCK
 #SET NET'NET':SPO'LINE' = 44 ;IEC 60870-5-104 master
 #SET NET'NET':SPD'LINE' = 20 ;polling delay (s)
 #SET NET'NET':SMS'LINE' = %APPLIC ;message application
 #SET NET'NET':SMI'LINE' = %LINE+(6000+(%NET*100)) ;message identifier
 #SET NET'NET':SPS'LINE' = 50 ;buffer pool size
 #SET NET'NET':SHT'LINE' = 1000 ;connect timeout(ms)
 #SET NET'NET':STI'LINE' = 15 ;timeout interval (s)
 #SET NET'NET':SIU'LINE' = 1 ;Set line in use
#BLOCK_END
;*************************************************************************
; CREATE IEC 60870-5-104 MASTER STATIONS TO NET
#LOOP_WITH I = 1..LENGTH(%STATIONS)
@STA=%STATIONS(%I)
 #SET NET'NET':SDV(29) = (%STA,%LINE) ;create station to line
 #SET STA'STA':SAL = 1 ;allocated
 #SET STA'STA':SAS = %APPLIC ;allocating application
 #SET STA'STA':SMI = 29000+%STA ;message identification
 #SET STA'STA':SMS = %APPLIC ;message application
 #SET STA'STA':SSE = 1 ;system messages enabled
 #SET STA'STA':SSA = %STA ;station address
 #SET STA'STA':SSL = 2 ;station address length (bytes)
 #SET STA'STA':SIL = 3 ;info addr. length (bytes)
 #SET STA'STA':SCL = 2 ;COT length (bytes)
 #SET STA'STA':SCA = 32000 ;command address
 #SET STA'STA':SST = 5000 ;SYS waiting time (ms)
 #SET STA'STA':SRT = 10 ;application reply timeout (s)
 #SET STA'STA':SCT = 60 ;application termin. timeout (s)
 #SET STA'STA':SSU = 0 ;summer time (0=no, 1=yes)
 #SET STA'STA':SML = 230 ;max. message length
 #SET STA'STA':SRM = 0 ;running mode
 #SET STA'STA':SIA = ”host” ;hostname or IP address of
;the remote host
 #SET STA'STA':SUS = 12 ;unocknowledge send
 #SET STA'STA':SUR = 8 ;unacknowledge receive
 #SET STA'STA':SAT = 10 ;akcnowledge timeout (s)
```

```
 #SET STA'STA':SET = 30 ;reconnecting timeout (s)
 #SET STA'STA':SIU = 1 ;set station in use
#LOOP_END
```

Index

W

Z

Hitachi ABB Power Grids
Grid Automation Products
PL 688
65101 Vaasa, Finland

https://hitachiabb-powergrids.com/microscadax

Scan this QR code to visit our website

1MRK 511 492-UEN