IEC 60870-5-104 Protocol RTU IED Server Simulator User Manual

Stack Version: 21.05.006

IEC 60870-5-104 Protocol

FreyrSCADA Embedded Solution

No.5, BommaiyaSamy Kovil Street, Annanji, Theni, TamilNadu, India

www.freyrscada.com

CIN: U72900TN2018PTC120601

Table of Contents

1. Introduction 3
2. Features 4
3. Add and Delete Server 5
4. Server Configuration 6
5. Server Data Configuration 9
6. Map controling point to Monitoring Point 12
7. Update Monitoring Information 14
8. Traffic window 15
9. Log Window 15
10. IEC 60870-5-104 Server Simulator Interoperability 16
11. Discussions 32

1. Introduction

IEC 60870-5 part 104 enables communication between IED, RTU control station and substation via a standard TCP/IP network. The TCP protocol is used for connection-oriented secure data transmission. IEC 60870 5104 protocol (IEC 104) is a part of IEC Telecontrol Equipment and Systems Standard IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation. IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for telecontrol (supervisory control and data acquisition SCADA) in electrical engineering and power system automation applications. Part 5 provides a communication profile for sending basic telecontrol messages between two systems, which uses permanent directly connected data circuits between the systems. The IEC Technical Committee 57 (Working Group 03) have developed a protocol standard for telecontrol, teleprotection, and associated telecommunications for electric power systems. The result of this work is IEC 60870-5. Five documents specify the base IEC 60870-5:

- 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

FreyrSCADA IEC 60870-5-104 Server Simulator was originally developed to test the IEC 60870-5-104 stack.

We developed the stack to run multiple hardware platform (windows, Linux, RTLinux, QNX..). So, we had to test multiple platform. At that time, our engineers, developed the test simulation application.

We tested this simulator with multiple test software available in the market.

The interoperability list focused only for our Stack. If you have any specific requirement to implement new Type id ASDU, please contact to us.

Our support team has young, dynamic and professional team of engineers. And they will provide the quick and accurate solution as per customer requirement.

tech.support@freyrscada.com

Thanks

Management- FreyrSCADA Embedded Solution

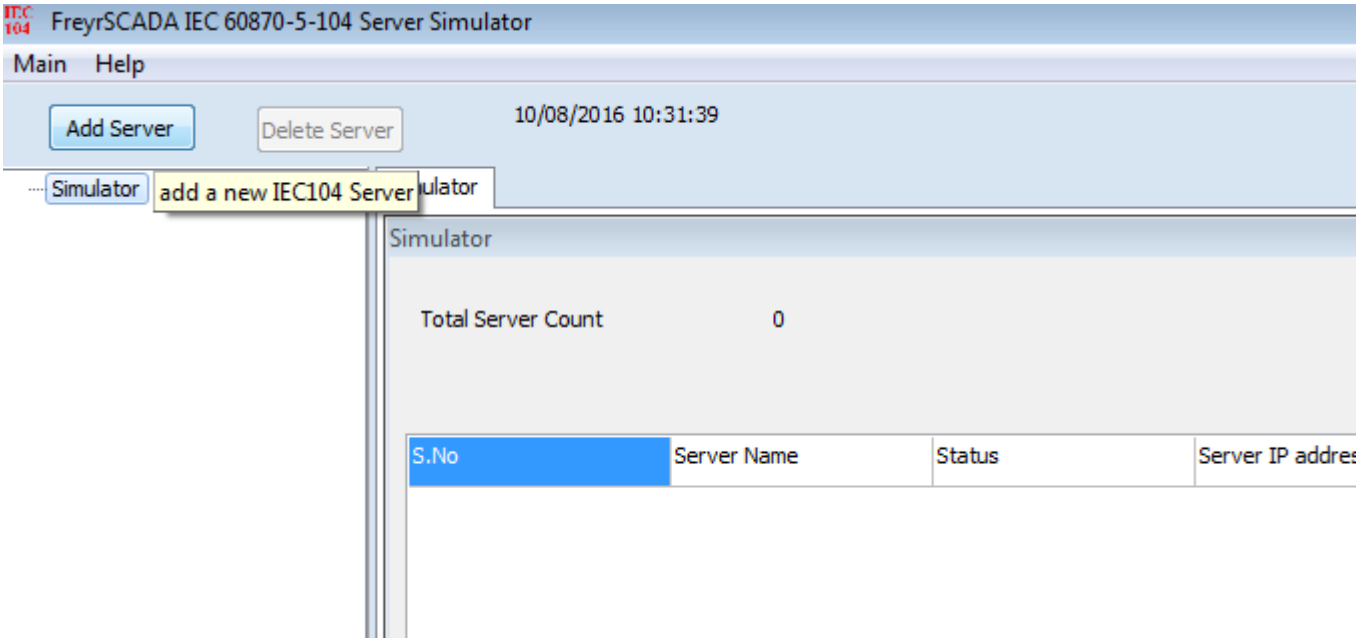
2. Features

- ✓ Multiple Server Simulation
- ✓ In a Single Server(link) simulate Multiple Stations (Common Address)
- ✓ Redundancy Enabled
- ✓ Mapping of Control Point to monitor Information point, consider C_SC point can map to M_SP point
- ✓ Communication with redundant control systems and interruption-free switchover between redundant systems
- ✓ Supports "select-before-operate" or "direct-execute" command execution modes
- ✓ Supports File Transfer (Monitor Direction and Control Direction), Directory commands
- ✓ On-demand transmission (e. g. single indications, Analog...)
- ✓ Spontaneous transmission (e. g. single indications with time tag ...)
- ✓ Clock synchronization

3. Add and Delete Server

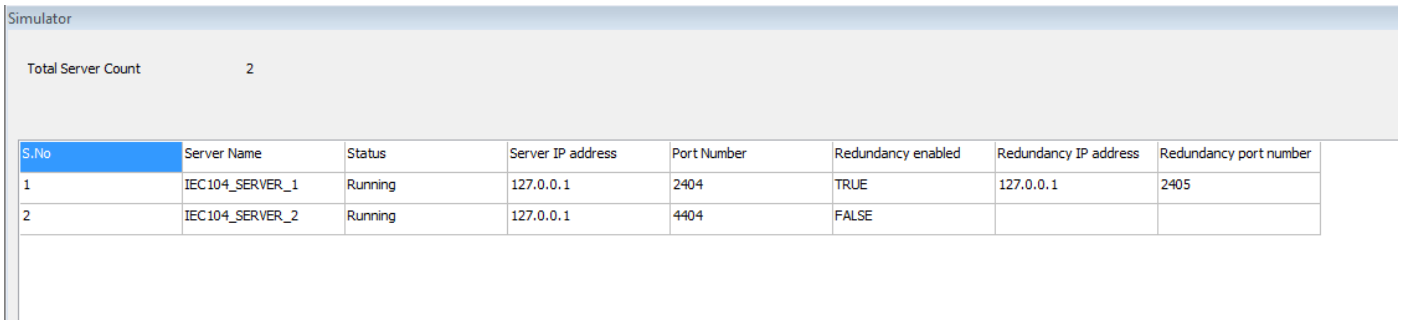
We can add up to 50 server nodes in the simulator. Every server node will work independently.

And also we can delete the server.



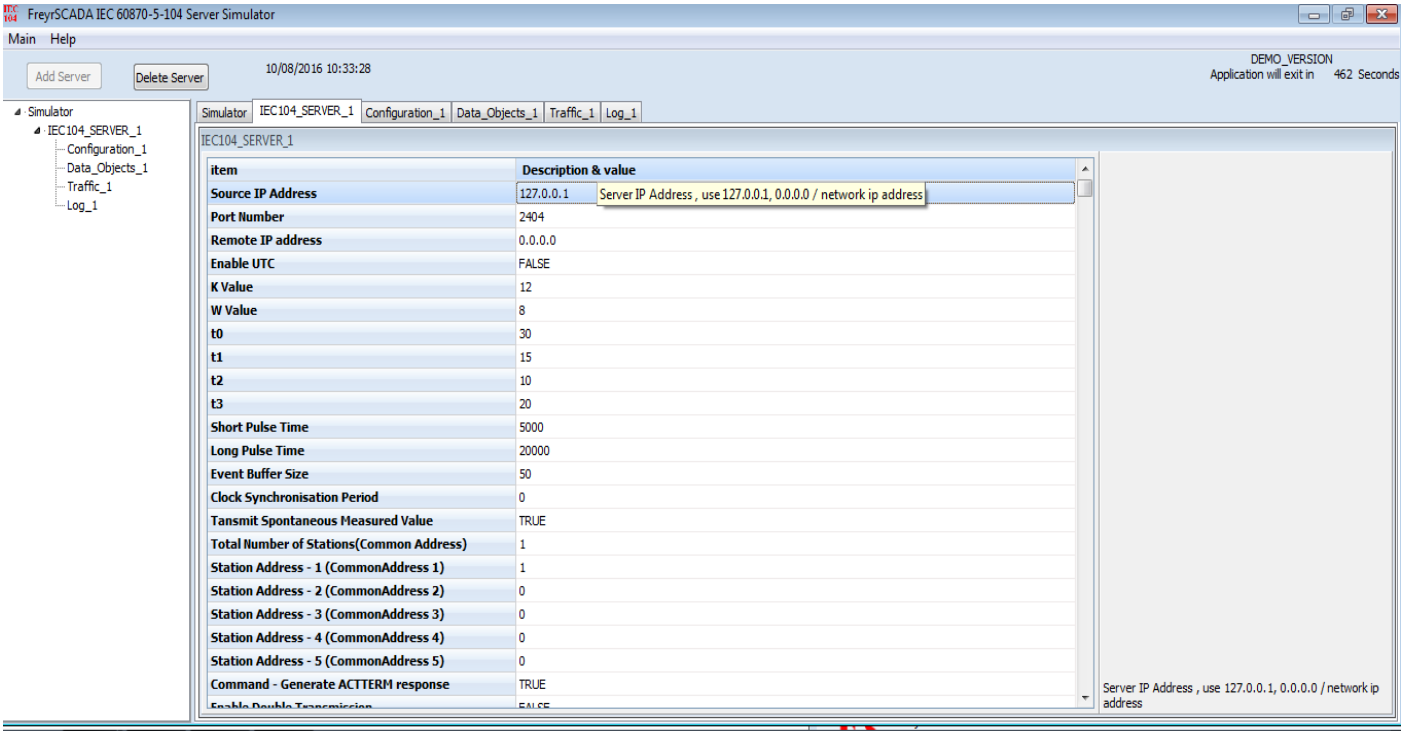
Simulator window shows the status & connection ip address, port number, reduandancy enabled or not,

If reduancy enabled it shows, the reduanct source ip address, port .



4. Server Configuration

Server Protocol Configuration window shows the actual protocol settings.



Configuration Parameters as follows:

1) **Source IP Address -** IEC104 server to bind ip address , use 127.0.0.1 loopback, 0.0.0.0 / network ip address.
2) **Port Number** - IEC104 server to bind port number, - server listen on incoming client connection, default 2404.
3) **Remote IP Address** – Expected IEC104 Client ip address, use 0,0.0.0 to accept all remote station ip.
4) **Enable UTC** - Enable UTC time / local time for update the monitoring information & initial database time initilization.
5) **K Value** - Maximum difference receive sequence number to send state variable (k: 1 to 32767) default – 12.
6) **W Value** - Latest acknowledge after receiving w I format APDUs

(w: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of k) default :8).

7) **t0** - Time out of connection establishment in seconds (1-255s).

8) **t1** - Time out of send or test APDUs in seconds (1-255s).

9) **t2** - Time out for acknowledges in case of no data message t2 M t1 in seconds (1-172800 sec).

10) **t3** - Time out for sending test frames in case of long idle state in seconds (1 to 48h(172800sec)).

11) **Long Pulse Time** –in milliseconds 10000, For Certain Command points have Pulse Duration, so after actconform, the actterm signal will be trigged according to this pulse time.

12) **Short Pulse Time** - in milliseconds default 5000. For Certain Command points have Pulse Duration, so after actconform, the actterm signal will be trigged according to this pulse time

13) **Event Buffer Size** - SOE Sequence of Event Buffer Size (100-65,535).

14) **Clock Synchronisation Period** - in milliseconds. If 0 than Clock Synchronisation command is not expected from Master. If the time elapsed, and did not receive the time sync command , in the events, cp56time21 time stamp, the invalid bit will set.

15) **Transmit spontanous Measured Value** - transmit M_ME measured values as COT – spont ,spontanous message.

16) **Total number of stations** - In a single physical device/ server, we can run many stations – Total nmuber of stations in iec104 server ,according to common address (1-5).

17) **Station Address - 1 (CommonAddress 1) -** station address 1- Common Address 1 , 1-65534 , 65535 = global address (only master can use this).

18) **Station Address - 2(CommonAddress 2) - station address 2**- Common Address 2 , 1-65534 , 65535 = global address (only master can use this).

19) **Station Address - 3 (CommonAddress 3) -** station address 3- Common Address 3 , 1-65534 , 65535 = global address (only master can use this).

20) **Station Address - 4 (CommonAddress 4) -** station address 4- Common Address 4 , 1-65534 , 65535 = global address (only master can use this).

21) **Station Address - 5(CommonAddress 5) -** station address 5- Common Address 5 , 1-65534 , 65535 = global address (only master can use this).

22) **Command - Generate ACTTERM response** - if Yes , Generate ACTTERM responses for operate commands.

23) **Enable Double Transmission** - enable double transmission.

24) **Enable File Transfer** - Enable FILE transmission.- in demo version, file transfer disabled

25) **File Transfer Directory Path** - File Transfer Directory Path – location of file to list in directory command & transfer to iec104 master.

26) **Max Files In Directory** - Maximum Number of Files in Directory (default 25).

27) **Enable Redundancy** - enable redundancy for the connection.

28) **Redundancy Server IP Address** , use 127.0.0.1- loopback, 0.0.0.0 / network ip address.

29) **Redundancy Port Number**.- IEC104 server to bind port number, - server listen on incoming client connection,

30) **Redundancy Remote IP Address** , use 0,0.0.0 to accept all remote station ip.

31) **Transmit Interrogation Measured Value** - Transmit M_ME measured values in General interrogation.

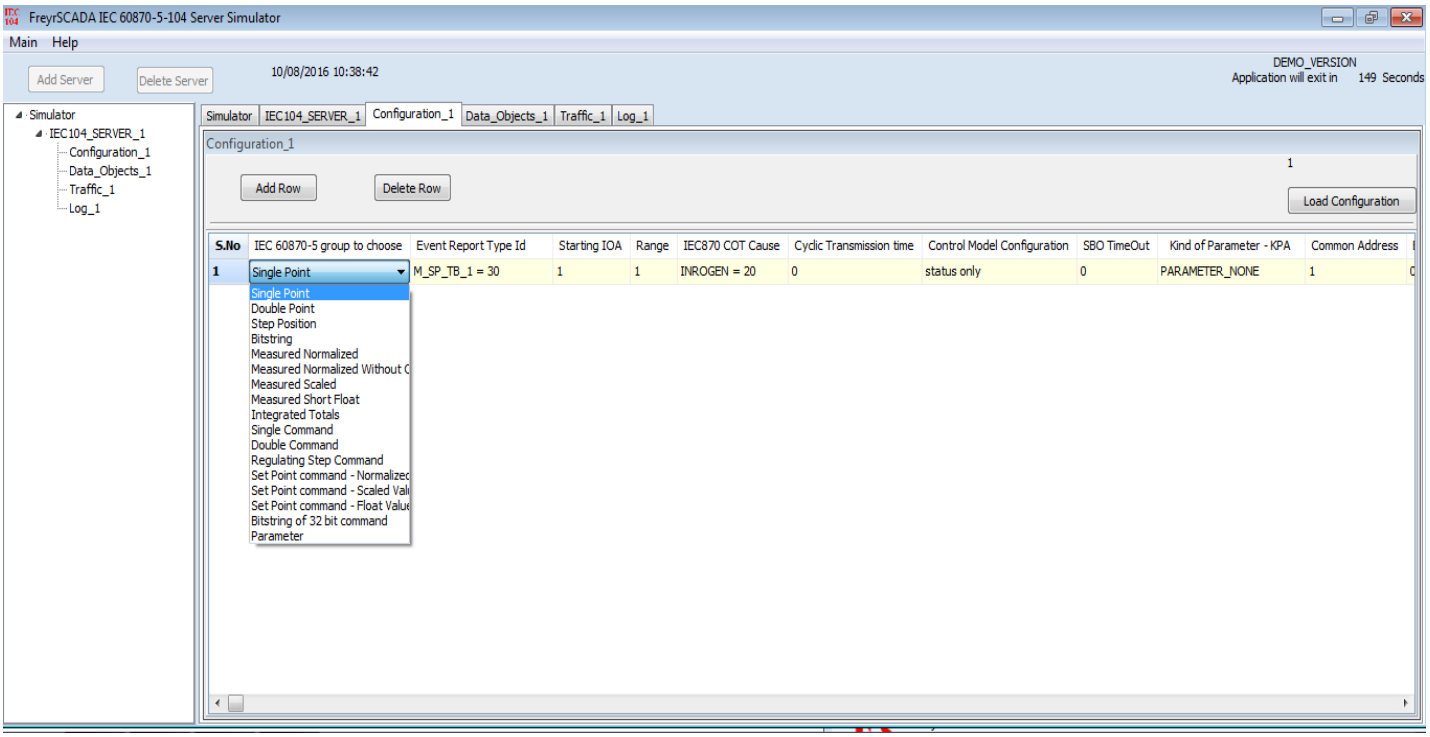
32) **Transmit Background Scan Measured Value** - transmit M_ME measured values in background Scan message.

33) **Update Check Timestamp** - if it is true ,the timestamp change also generate event during the iec104update for Monitoring information.

34) COT Size - Cause of Transmission(COT) Size

5. Server Data Configuration

Server Data Configuration window shows the point list configuration.



IEC 60870-5 Group & Typeid to choose

1) Single Point - Single-point information

M_SP_NA_1 = 1 Single-point information

M_SP_TB_1 = 30 Single-point information with time tag CP56Time2a

2) Double Point - Double-point information

M_DP_NA_1 = 3 Double-point information

M_DP_TB_1 = 31 Double-point information with time tag CP56Time2a

3) Step Position - Step position information

M_ST_NA_1 = 5 Step position information

M_ST_TB_1 = 32 Step position information with time tag CP56Time2a

4) Bitstring - Bit string of 32 bit

M_BO_NA_1 = 7 Bitstring of 32 bit

M_BO_TB_1 = 33 Bitstring of 32 bit with time tag CP56Time2a

5) Measured Normalized - Measured normalized value

M_ME_NA_1 = 9 Measured value, normalized value

M_ME_TD_1 = 34 Measured value, normalized value with time tag CP56Time2a

6) Measured Normalized Without Quality - Measured normalized value without quality descriptor

M_ME_ND_1 = 21 Measured value, normalized value without quality descriptor

7) Measured Scaled - Measured scaled value

M_ME_NB_1 = 11 Measured value, scaled value

M_ME_TE_1 = 35 Measured value, scaled value with time tag CP56Time2a

8) Measured Short Float - Measured value, short float value

M_ME_NC_1 = 13 Measured value, short floating point value

M_ME_TF_1 = 36 Measured value, short floating point value with time tag CP56Time2a

9) Integrated Totals - Integrated totals

M_IT_NA_1 = 15 Integrated totals

M_IT_TB_1 = 37 Integrated totals with time tag CP56Time2a

10) Event of Protection Equipment - Event of protection equipment with time tag CP56Time2a

M_EP_TD_1 = 38, Event of protection equipment with time tag CP56Time2a

11) Packed Start Events of Protection Equipment - Packed start events of protection equipment with time tag CP56Time2a

M_EP_TE_1 = 39, Packed start events of protection equipment with time tag CP56Time2a

12) Packed Output Circuit Information of Protection Equipment - Packed output circuit information of protection equipment with time tag CP56Time2a

M_EP_TF_1 = 40, Packed output circuit information of protection equipment with time tag CP56Time2a

13) Single Command - Single command

C_SC_NA_1 = 45 Single command

C_SC_TA_1 = 58 Single command with time tag CP56Time2a

14) Double Command - Double command

C_DC_NA_1 = 46 Double command

C_DC_TA_1 = 59 Double command with time tag CP56Time2a

15) Regulating Step Command - Regulating step command

C_RC_NA_1 = 47 Regulating step command

C_RC_TA_1 = 60 Regulating step command with time tag CP56Time2a

16) Set Point command - Normalized Value - Set point command, normalized value

C_SE_NA_1 = 48 Set point command, normalized value

C_SE_TA_1 = 61 Set point command, normalized value with time tag CP56Time2a

17) Set Point command - Scaled Value - Set point command, scaled value

C_SE_NB_1 = 49 Set point command, scaled value

C_SE_TB_1 = 62 Set point command, scaled value with time tag CP56Time2a

18) Set Point command - Float Value - Set point command, short floating point value

C_SE_NC_1 = 50 Set point command, short floating point value

C_SE_TC_1 = 63 Set point command, short floating point value with time tag CP56Time2a

19) Bitstring of 32 bit command - Bitstring of 32 bit command

C_BO_NA_1 = 51 Bitstring of 32 bit command

C_BO_TA_1 = 64 Bitstring of 32 bit command with time tag CP56Time2a

20) Parameter - Parameter

P_ME_NA_1 = 110 Parameter of measured value, normalized value

P_ME_NB_1 = 111 Parameter of measured value, scaled value

P_ME_NC_1 = 112 Parameter of measured value, short floating point value

The selection of following parameters based on the typeid selection.

Consider for the following items

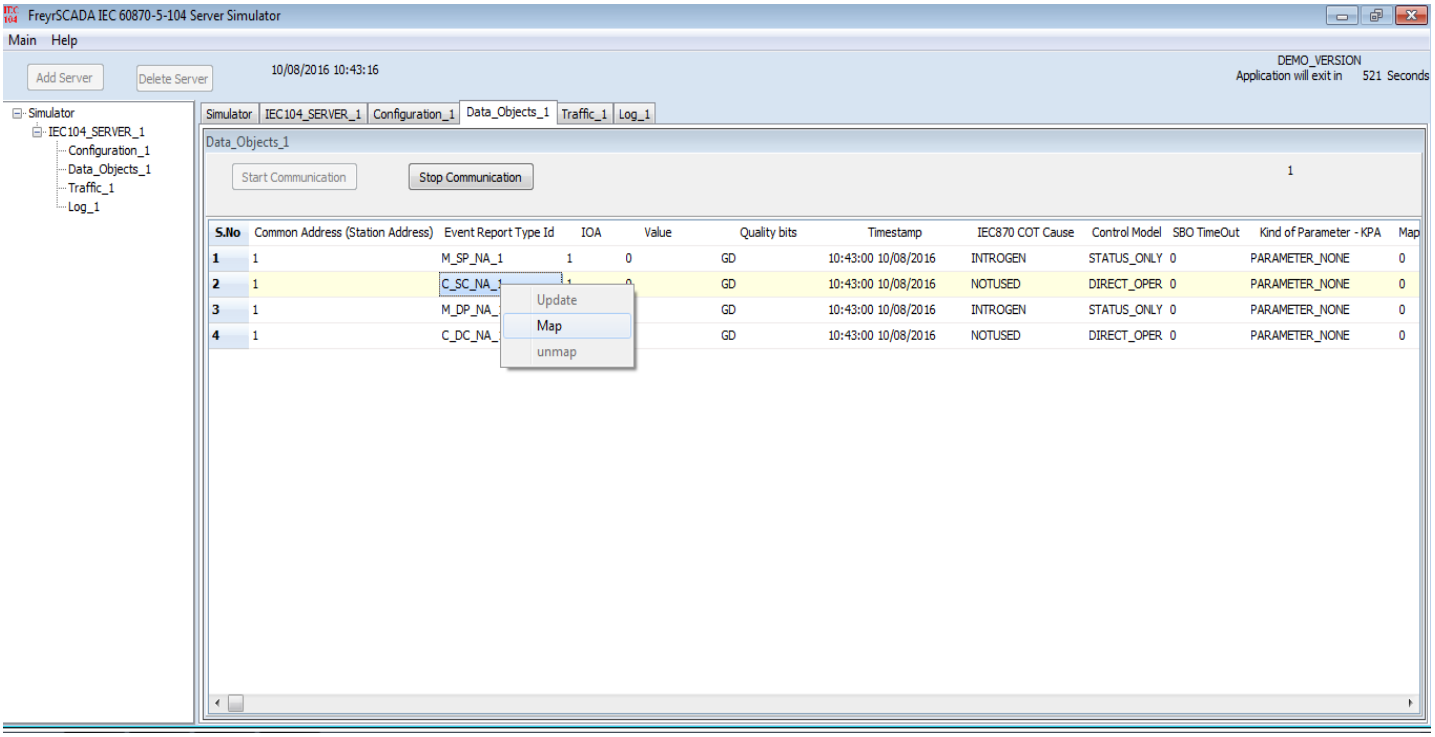
	Monitoring information	**Control / Command Point**	**Parameter Value**
IEC 60870-5 Group to Choose	Single Point	Single Command	Parameter
Event Report Type Id	M_SP_NA_1 = 1	C_SC_NA_1 = 45	P_ME_NA_1 = 110
Starting IOA	**10**	**100**	**2000**
Range	**5**	**5**	**5**
IEC870 COT Cause	INROGEN = 20	NOTUSED	INROGEN = 20
Cyclic Transmission time	**0**	**0**	**0**
Control Model Configuration	status only	direct operate	status only
SBO TimeOut	**0**	**0**	**0**
Kind of Parameter - KPA	PARAMETER_NONE	PARAMETER_NONE	PARAMETER_THRESHOLDVALUE
Common Address	**1**	**1**	**1**
Background Scan time	**0**	**0**	**0**

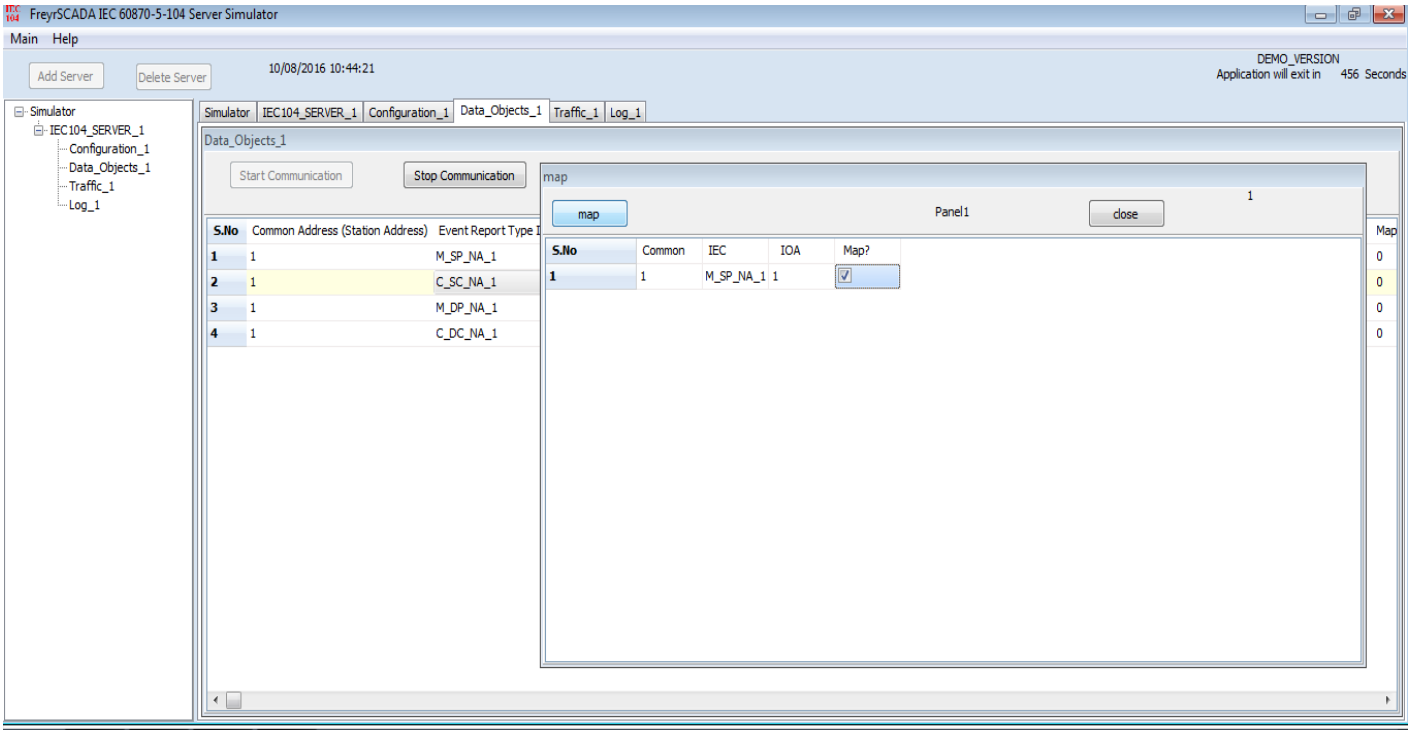
6. Map controling point to Monitoring Point

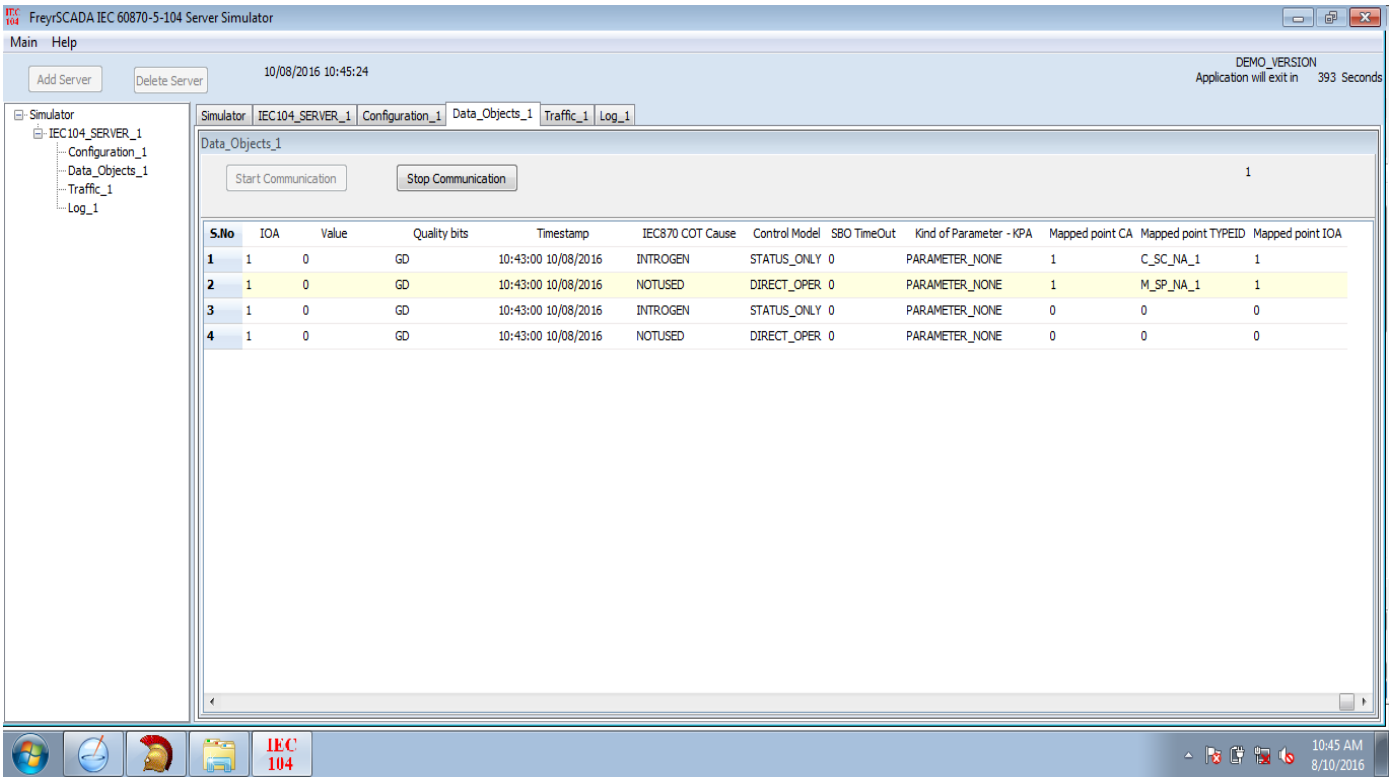
In the simulator, Data object window, We can map the controlling point to a monitoring point individually,

Consider a point (C_SC, IOA 1), can map to a monitoring information point (M_SP, IOA 1),

Right click the command point-> map, a new window will show the available monitoring point, and select the point and map it. If a control point receive the command, the command value will reflect in the monitoring point




FreyrSCADA IEC 60870-5-104 Server Simulator
Main Help
Add Server
Delete Server
10/08/2016 10:44:21
DEMO_VERSION
Application will exit in 456 Seconds
Simulator
IEC104_SERVER_1
Configuration_1
Data_Objects_1
Traffic_1
Log_1
Start Communication
Stop Communication
map
Panel1
close
S.No
Common Address (Station Address)
Event Report Type
Common
IEC
IOA
Map?
M_SP_NA_1
C_SC_NA_1
M_DP_NA_1
C_DC_NA_1

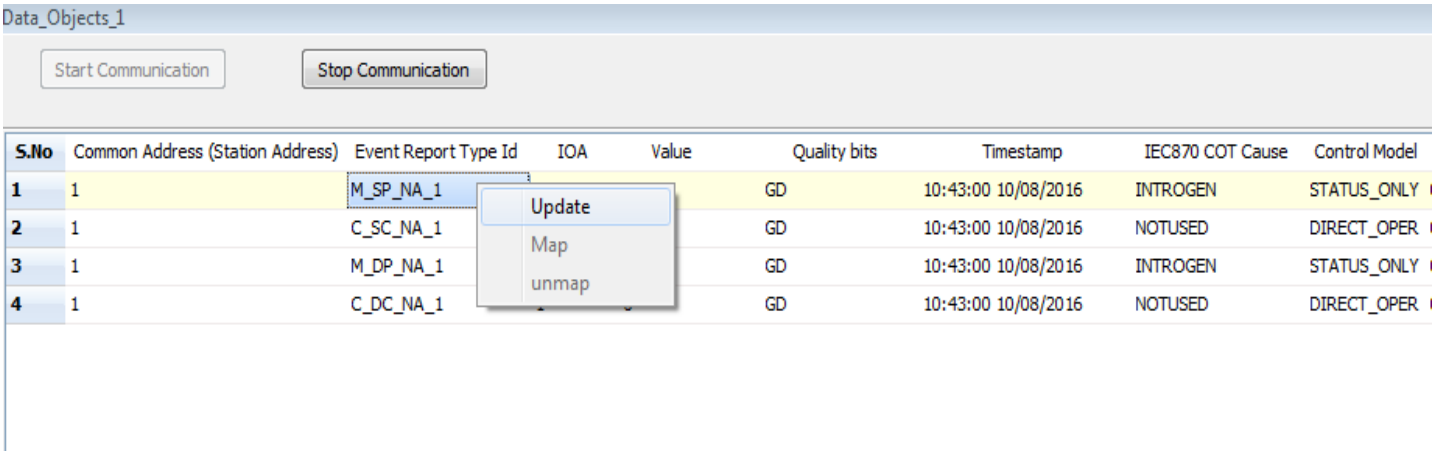

FreyrSCADA IEC 60870-5-104 Server Simulator
Main Help
Add Server
Delete Server
10/08/2016 10:45:24
DEMO_VERSION
Application will exit in 393 Seconds
Simulator
IEC104_SERVER_1
Configuration_1
Data_Objects_1
Traffic_1
Log_1
Start Communication
Stop Communication
S.No
IOA
Value
Quality bits
Timestamp
IEC870 COT Cause
Control Model
SBO TimeOut
Kind of Parameter - KPA
Mapped point CA
Mapped point TYPEID
Mapped point IOA
10:45 AM
8/10/2016

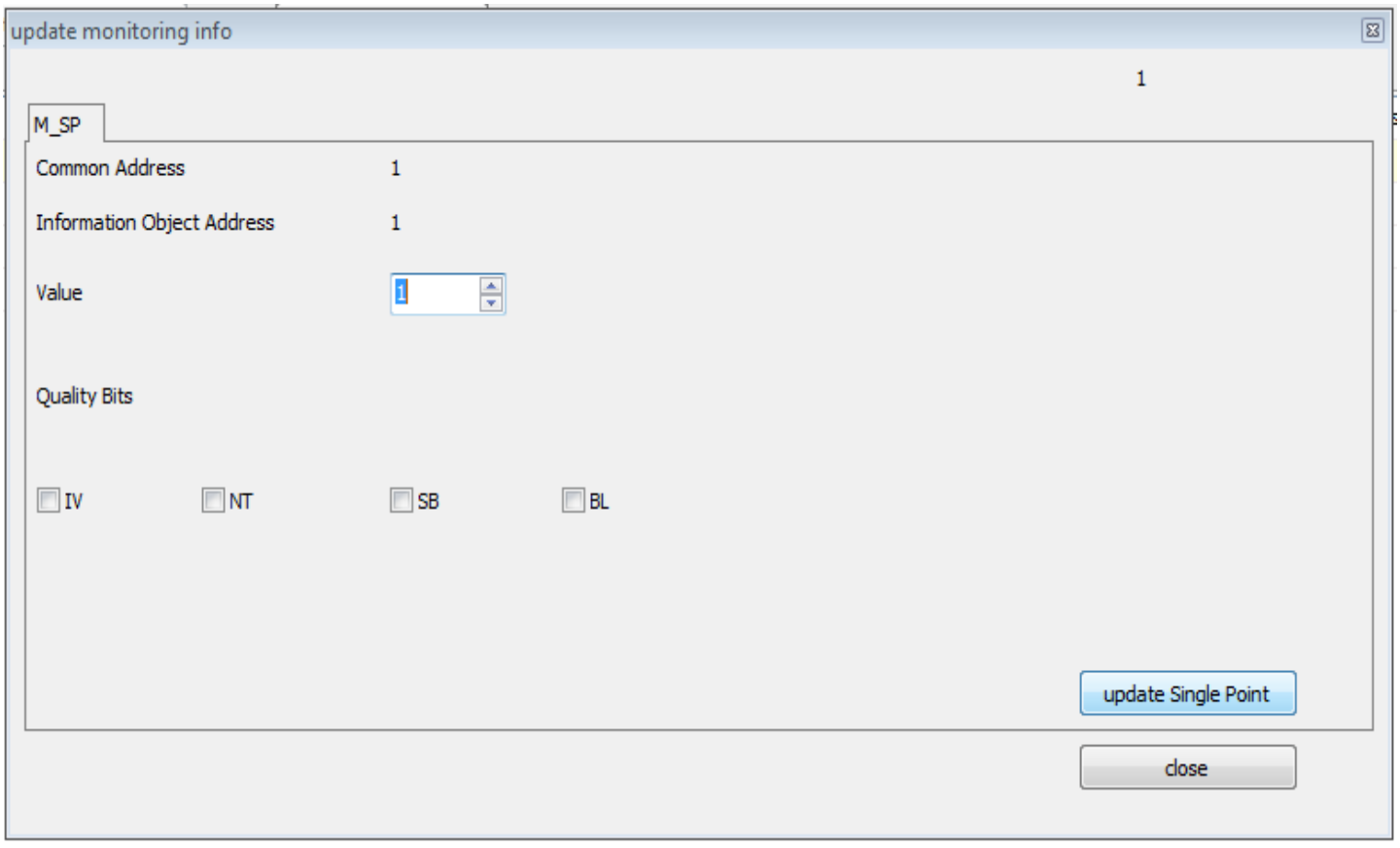
7. Update Monitoring Information

The user can update the monitoring Point information .The following parameters can change

Value, quality bits

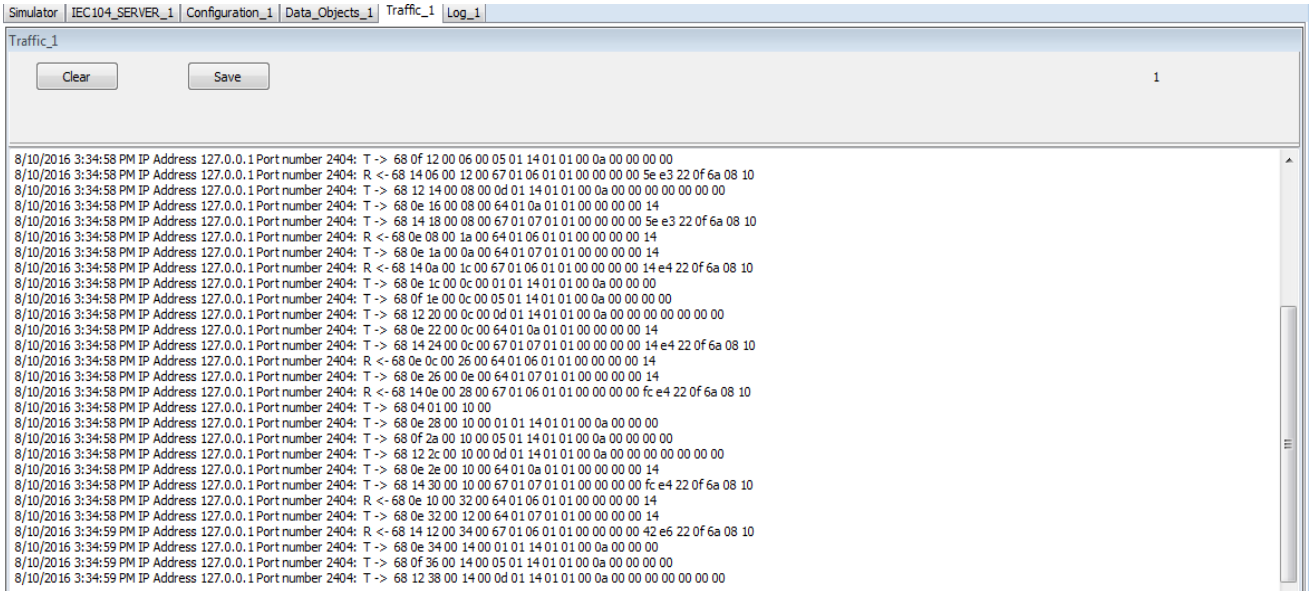
and according to event report typeid , the change reported to end client system by spontaneous.





8. Traffic window

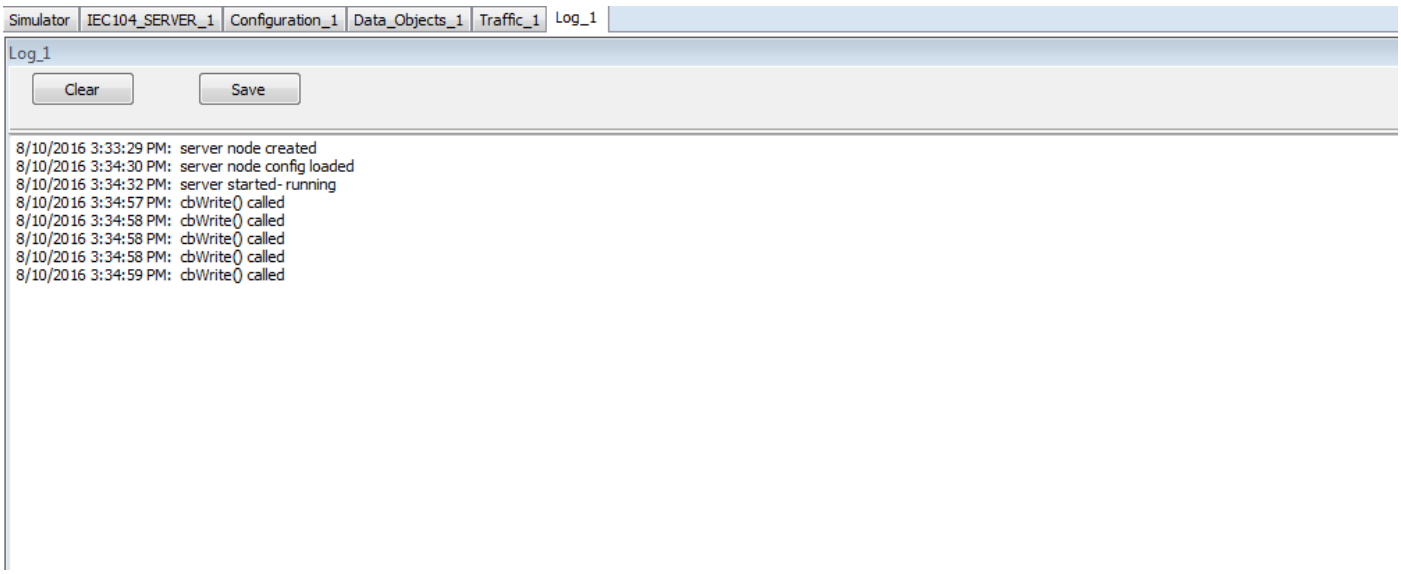
In this we can monitor the traffic of iec104 communication.



In this we can save the traffic, and clear the traffic

9. Log Window

Log window for internal reference



In the log, we can monitor the command exchange between server & master, and there is an option to save the log & clear log.

For more information, just drop a mail to support@freyrscada.com

10. IEC 60870-5-104 Server Simulator Interoperability

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 command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

The 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).

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

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

☐	Function or ASDU is not used
X	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 s

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.

1.1 System or device

(System-specific parameter, indicate the definition of a system or a device by marking
One of the following with an "**X**")

☐	System definition
☐	Controlling station definition (master)
X	Controlled station definition (slave)

1.2 Network configuration

(Network-specific parameter, all configurations that are used are to be marked with an "**X**")

- ~~Point-to-point~~
- ~~Multiple point-to-point~~
- ~~Multipoint-party line~~
- ~~Multipoint-star~~

1.3 Physical layer

(Network-specific parameter, all interfaces and data rates that are used are to be marked with an "**X**")

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~~	~~2 400 bit/s~~	~~2 400 bit/s~~	~~56 000 bit/s~~
~~200 bit/s~~	~~4 800 bit/s~~	~~4 800 bit/s~~	~~64 000 bit/s~~
~~300 bit/s~~	~~9 600 bit/s~~	~~9 600 bit/s~~	
~~600 bit/s~~		~~19 200 bit/s~~	
~~1 200 bit/s~~		~~38 400 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~~	~~2 400 bit/s~~	~~2 400 bit/s~~	~~56 000 bit/s~~
~~200 bit/s~~	~~4 800 bit/s~~	~~4 800 bit/s~~	~~64 000 bit/s~~
~~300 bit/s~~	~~9 600 bit/s~~	~~9 600 bit/s~~	
~~600 bit/s~~		~~19 200 bit/s~~	
~~1 200 bit/s~~		~~38 400 bit/s~~	

Link layer

(Network-specific parameter, all options that are used are to be marked with an "**X**".
Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the type ID and COT of all messages assigned to class 2.)

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

Link transmission procedure

- ~~Balanced transmission~~
- ~~Unbalanced transmission~~

Frame length

- Maximum length L (number of octets)

Address field of the link

- ~~not present (balanced transmission only)~~
- ~~one octet~~
- ~~two octets~~
- ~~Structured~~
- ~~Unstructured~~

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 class 2 messages is used as follows:~~

Type identification	Cause of Transmission

~~NOTE (In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available).~~

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, all configurations that are used are to be marked with an "**X**")

■ ~~One octet~~	[X] two octets

Information object address

(System-specific parameter, all configurations that are used are to be marked with an "**X**")

■ ~~One octet~~	[X] Structured
■ ~~Two octets~~	[X] Unstructured
[X] Three octets	

Cause of transmission

(System-specific parameter, all configurations that are used are to be marked with an "**X**")

■ ~~One octet~~	[X] two octets (with originator address)
	Originator address is set to zero if not used

Length of APDU

(System-specific parameter, specify the maximum length of the APDU per system)

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, mark each type ID with an "**X**" if it is only used in the standard Direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

X	<1>:= Single-point information	M_SP_NA_1
	~~<2>:= Single-point information with time tag~~	~~M_SP_TA_1~~
X	<3>:= Double-point information	M_DP_NA_1
	~~<4>:= Double-point information with time tag~~	~~M_DP_TA_1~~
X	<5>:= Step position information	M_ST_NA_1
	~~<6>:= Step position information with time tag~~	~~M_ST_TA_1~~
X	<7>:= Bitstring of 32 bit	M_BO_NA_1
	~~<8>:= Bitstring of 32 bit with time tag~~	~~M_BO_TA_1~~
X	<9>:= Measured value, normalized value	M_ME_NA_1
	~~<10>:= Measured value, normalized value with time tag~~	~~M_ME_TA_1~~
X	<11>:= Measured value, scaled value	M_ME_NB_1
	~~<12>:= Measured value, scaled value with time tag~~	~~M_ME_TB_1~~
X	<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~~
X	<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
X	<21>:= Measured value, normalized value without quality descriptor	M_ME_ND_1
X	<30>:= Single-point information with time tag CP56Time2a	M_SP_TB_1
X	<31>:= Double-point information with time tag CP56Time2a	M DP TB 1
X	<32>:= Step position information with time tag CP56Time2a	M_ST_TB_1
X	<33>:= Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
X	<34>:= Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
X	<35>:= Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
X	<36>:= Measured value, short floating point value with time tag CP56Time2a	M ME TF 1
X	<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

In this companion standard only the use of the set <30> – <40> for ASDUs with time tag is permitted.

Process information in control direction

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

X	<45>:= Single command	C_SC_NA_1
X	<46>:= Double command	C_DC_NA_1
X	<47>:= Regulating step command	C_RC_NA_1
X	<48>:= Set point command, normalized value	C_SE_NA_1
X	<49>:= Set point command, scaled value	C_SE_NB_1
X	<50>:= Set point command, short floating point value	C_SE_NC_1
X	<51>:= Bitstring of 32 bit	C_BO_NA_1
X	<58>= Single command with time tag CP56Time2a	C_SC_TA_1
X	<59>= Double command with time tag CP56Time2a	C_DC_TA_1
X	<60>= Regulating step command with time tag CP56Time2a	C_RC_TA_1
X	<61>= Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
X	<62>= Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
X	<63>= Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
X	<64>= Bitstring of 32 bit command 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, mark with an "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

X	<70>:= End of initialisation	M_EI_NA_!

System information in control direction

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

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~~
X	<107>:= Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in control direction

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

X	<110>:= Parameter of measured value, normalized value	P_ME_NA_1
X	<111>:= Parameter of measured value, scaled value	P_ME_NB_1
X	<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, mark each type ID with an "**X**" if it is only used in the standard Direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

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

Type identification and cause of transmission assignments
(Station-specific parameters)

Shaded boxes: option not required.
Black boxes: option not permitted in this companion standard
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**																		
		periodic, cyclic	**background scan**	**spontaneous**	**initialized**	**request or requested**	**activation**	**activation confirmation**	**deactivation**	**deactivation confirmation**	**activation termination**	**return info caused by a remote cmd**	**return info caused by a local cmd**	**file transfer**	**interrogated by group <number>**	**request by group <n> counter request**	**unknown type identification**	**unknown cause of transmission**	**unknown common address of ASDU**	**unknown information object address**
		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		X	X		X									X					
<21>	M_ME_ND_1	X	X	X		X									X					

Type identification		Cause of transmission																		
		periodic, cyclic	background scan	spontaneous	initialized	request or requested	activation	activation confirmation	deactivation	deactivation confirmation	activation termination	return info caused by a remote cmd	return info caused by a local cmd	file transfer	interrogated by group <number>	request by group <n> counter request	unknown type identification	unknown cause of transmission	unknown common address of ASDU	unknown information object address
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<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
<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
<102>	C_RD_NA_1					X											X	X	X	X
<103>	C_CS_NA_1			X			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						X	X									X	X	X	X

Type identification		Cause of transmission																		
		periodic, cyclic	background scan	spontaneous	initialized	request or requested	activation	activation confirmation	deactivation	deactivation confirmation	activation termination	return info caused by a remote cmd	return info caused by a local cmd	file transfer	interrogated by group <number>	request by group <n> counter request	unknown type identification	unknown cause of transmission	unknown common address of ASDU	unknown information object address
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<110>	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112>	P_ME_NC_1						X	X							X		X	X	X	X
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_NA_1													X			X	X	X	
<121>	F_SR_NA_1													X			X	X	X	
<122>	F_SC_NA_1					X								X			X	X	X	
<123>	F_LS_NA_1													X			X	X	X	
<124>	F_AF_NA_1													X			X	X	X	
<125>	F_SG_NA_1													X			X	X	X	
<126>	F_DR_TA_1*			X		X														
<127>	F_SC_NB_1*					X								X			X	X	X	

*** Blank or X only**

Basic application functions

Station initialization

(Station-specific parameter, mark with an "**X**" if function is used)

[X] Remote initialization

Cyclic data transmission

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

[X] Cyclic data Transmission

Read Procedure

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

[X] Read procedure

Spontaneous transmission

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

[X] Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

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

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

[X] Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1

[X] Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1

[X] Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1

[X] Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project, see 7.2.1.1)

[X] Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1

[X] Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1

[X] Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station interrogation

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

- [X] global
- [X] group 1
- [X] group 2
- [X] group 3
- [X] group 4
- [X] group 5
- [X] group 6
- [X] group 7
- [X] group 8
- [X] group 9
- [X] group 10
- [X] group 11
- [X] group 12
- [X] group 13
- [X] group 14
- [X] group 15
- [X] group 16

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

Clock synchronization

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

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

Command transmission

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

- [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 of command direction of commands and set point commands

Configurable Maximum allowable delay of commands and set point commands

Transmission of integrated totals

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

- [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, mark with an "**X**" if function is used only in the standard direction, "**R**" if used only in the reverse direction, and "**B**" if used in both directions)

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

Parameter activation

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

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

Test procedure

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

- [X] Test procedure

File transfer

(Station-specific parameter, mark with an "**X**" if function is used)

File transfer in monitor direction

- [X] 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

- [X] Transparent file

Background scan

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

- [X] Background scan

Acquisition of transmission delay

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

- [■] ~~Acquisition of transmission delay~~

Definition of time outs

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

Maximum range for time-outs t_0 to t_1: 1 s to 255 s, accuracy 1 s.

Recommended range for timeout t_3:1 s to 48h, resolution 1s.

Long timeouts for t_3 may be needed in special cases where satellite links or dialup connections are used (for instance to establish connection and collect values only once per day or week).

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	Configurable
w	8 APDUs	Maximum difference receive sequence number to send state	Configurable

Maximum range of values k: 1 to 32767 (215–1) 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).

Port number

Parameter	Default value	Remarks
Portnumber	2404	In all cases(Configurable)

Redundant connections

[1] Number N of redundancy group connections used

RFC 2200 suite

RFC 2200 is an official Internet Standard which describes the state of standardization of
Protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in 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.

[X] 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.

11. Discussions

- Multiple Common Address / Station Address in a single link

How are logical devices identified within a physical device?

Both -101 and -104 have the concept of a logical device which is identified by the "Common Address of ASDU" (CAA). Each different logical device is identified by a different value of CAA. There is absolutely no requirement in the protocol definition that there is any relationship between the value of the device's data link address (101) or IP address (104) and the value(s) of the Common Address of ASDU for the logical device(s) in that physical device. The data link address or IP address has no part in identifying the data: the combination of CAA and Information Object Address (IOA) uniquely identifies each and every database object in the system.

When a -101 message is sent to a device, the data link address is used by the link layer to identify if it should accept the message or not. If it does accept the message, the CAA contained within the message identifies which logical device within the physical device should process the message. In -104 the mechanism is a little different due to the way that TCP/IP handles connections, but essentially the messages are addressed to the physical device identified by the IP address and then the CAA is used to pass the message to the correct logical device for processing in the same way as for -101.

- **Information Object Address & type id**

The information object address may be specified independently from the ASDU (type identification) which transmits the particular information object. Information objects may be transmitted with the same information object addresses using different ASDUs, for example, as a single-point information with or without time tag.

Table 15 – ASDUs in the monitor direction which may transmit objects with equal information object addresses

Type identification	Type identification with time tag	Alternative format type identification
1	2 or 30	20
3	4 or 31	17 or 38
5	6 or 32	
7	8 or 33	
9	10 or 34	21
11	12 or 35	
13	14 or 36	
15	16 or 37	

There are no other combinations of ASDUs of specific common addresses per line which may carry the same information object addresses in the monitor or (and) in the control direction.