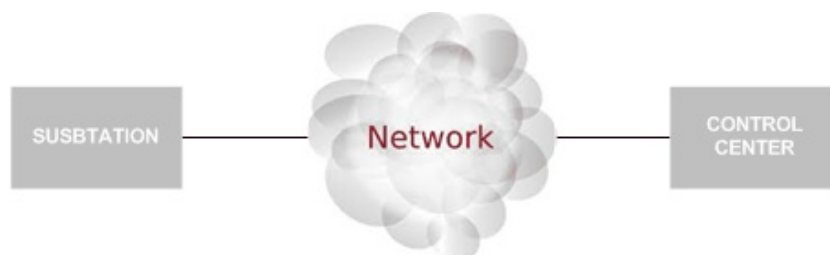


IEC 60870-5-104

IEC 60870-5-104 is a protocol for power system monitoring and controlling. Mostly used to communication between substations and control centers over Ethernet (Fiber optics, 2/3/4G, ...). IEC 60870-5-104 protocol is an extension of IEC 60870-5-101 protocol with the changes in transport, network, link and physical layer services to suit the complete network access.



Info about protocol

Telegram Structure

Teleram format with fixed length

	7	6	5	4	3	2	1	0
0	Start byte							
1	Length of APDU							
2	Control field 1							
3	Control field 2							
4	Control field 3							
5	Control field 4							

Telegram format with variable length

	7	6	5	4	3	2	1	0
0	Start byte							
1	Length of APDU							
2	Control field 1							
3	Control field 2							
4	Control field 3							
5	Control field 4							
6...	ASDU							

- **APCI** - Application Protocol Control Information (First 6 bytes)
- **APDU** - Application Protocol Data Unit (All variable length telegram)
- **ASDU** - Application Service Data Unit

Type identification

Standard IEC 60870-5-104 data types[1-255]

- [1-127] - standard definition
- [128-135] - reserved for routing of messages
- [136-255] - for special use

Dec	Type	Description	Direction	Support
Process information				
1	M_SP_NA_1	Single-point information	Monitor	Yes
2	M_SP_TA_1	Single-point information with time tag	Monitor	Yes
3	M_DP_NA_1	Double-point information	Monitor	Yes
4	M_DP_TA_1	Double-point information with time tag	Monitor	Yes
5	M_ST_NA_1	Step position information	Monitor	Yes
6	M_ST_TA_1	Step position information with time tag	Monitor	Yes
7	M_BO_NA_1	Bit string of 32 bit	Monitor	Yes
8	M_BO_TA_1	Bit string of 32 bit with time tag	Monitor	Yes
9	M_ME_NA_1	Measured value, normalized value	Monitor	Yes
10	M_ME_TA_1	Measured value, normalized value with time tag	Monitor	Yes
11	M_ME_NB_1	Measured value, scaled value	Monitor	Yes
12	M_ME_TB_1	Measured value, scaled value with time tag	Monitor	Yes
13	M_ME_NC_1	Measured value, short floating point number	Monitor	Yes
14	M_ME_TC_1	Measured value, short floating point number with time tag	Monitor	Yes
15	M_IT_NA_1	Integrated totals	Monitor	Yes
16	M_IT_TA_1	Integrated totals with time tag	Monitor	Yes
17	M_EP_TA_1	Event of protection equipment with time tag	Monitor	Yes
18	M_EP_TB_1	Packed start events of protection equipment with time tag	Monitor	Yes
19	M_EP_TC_1	Packed output circuit information of protection equipment with time tag	Monitor	Yes
20	M_PS_NA_1	Packed single point information with status change detection	Monitor	Yes
21	M_ME_ND_1	Measured value, normalized value without quality descriptor	Monitor	Yes
30	M_SP_TB_1	Single-point information with time tag CP56Time2a	Monitor	Yes

31	M_DP_TB_1	Double-point information with time tag CP56Time2a	Monitor	Yes
32	M_ST_TB_1	Step position information with time tag CP56Time2a	Monitor	Yes
33	M_BO_TB_1	Bit string of 32 bit with time tag CP56Time2a	Monitor	Yes
34	M_ME_TD_1	Measured value, normalized value with time tag CP56Time2a	Monitor	Yes
35	M_ME_TE_1	Measured value, scaled value with time tag CP56Time2a	Monitor	Yes
36	M_ME_TF_1	Measured value, short floating point number with time tag CP56Time2a	Monitor	Yes
37	M_IT_TB_1	Integrated totals with time tag CP56Time2a	Monitor	Yes
38	M_EP_TD_1	Event of protection equipment with time tag CP56Time2a	Monitor	Yes
39	M_EP_TE_1	Packed start events of protection equipment with time tag CP56Time2a	Monitor	Yes
40	M_EP_TF_1	Packed output circuit information of protection equipment with time tag CP56Time2a	Monitor	Yes
45	C_SC_NA_1	Single command	Control	Yes
46	C_DC_NA_1	Double command	Control	Yes
47	C_RC_NA_1	Regulating step command	Control	Yes
48	C_SE_NA_1	Set-point Command, normalized value	Control	Yes
49	C_SE_NB_1	Set-point Command, scaled value	Control	Yes
50	C_SE_NC_1	Set-point Command, short floating point number	Control	Yes
51	C_BO_NA_1	Bit string 32 bit command	Control	Yes
58	C_SC_TA_1	Single command with time tag CP56Time2a	Control	Yes
59	C_DC_TA_1	Double command with time tag CP56Time2a	Control	Yes
60	C_RC_TA_1	Regulating step command with time tag CP56Time2a	Control	Yes
61	C_SE_TA_1	Measured value, normalized value command with time tag CP56Time2a	Control	Yes
62	C_SE_TB_1	Measured value, scaled value command with time tag CP56Time2a	Control	Yes
63	C_SE_TC_1	Measured value, short floating point number command with time tag CP56Time2a	Control	Yes
64	C_BO_TA_1	Bit string of 32 bit command with time tag CP56Time2a	Control	Yes

System information				
70	M_EI_NA_1	End of Initialization	Monitor	Yes
100	C_IC_NA_1	Interrogation command	Control	Yes
101	C_CI_NA_1	Counter interrogation command	Control	Yes
102	C_RD_NA_1	Read command	Control	Yes
103	C_CS_NA_1	Clock synchronization command	Control	Yes
104	C_TS_NA_1	Test command	Control	Yes
105	C_RP_NA_1	Reset process command	Control	Yes
106	C_CD_NA_1	Delay acquisition command	Control	No
107	C_TS_TA_1	Test command with time tag CP56Time2a	Control	No
Parameter				
110	P_ME_NA_1	Parameter of measured values, normalized value	Control	No
111	P_ME_NB_1	Parameter of measured values, scaled value	Control	No
112	P_ME_NC_1	Parameter of measured values, short floating point number	Control	No
113	P_AC_NA_1	Parameter activation	Control	No
File transfer				
120	F_FR_NA_1	File ready	File transfer	No
121	F_SR_NA_1	Section ready	File transfer	No
122	F_SC_NA_1	Call directory, select file, call file, call section	File transfer	No
123	F_LS_NA_1	Last section, last segment	File transfer	No
124	F_FA_NA_1	ACK file, ACK section	File transfer	No
125	F_SG_NA_1	Segment	File transfer	No
126	F_DR_TA_1	Directory	File transfer	No

127	F_SC_NB_1	Request archive file	File transfer	No
-----	-----------	----------------------	---------------	----

Cause of transmission

Standard IEC 60870-5-101 cause of transmission [0-63]

Dec	Description
1	Periodic, cyclic
2	Background interrogation
3	Spontaneous
4	Initialized
5	Interrogation or interrogated
6	Activation
7	Confirmation activation
8	Deactivation
9	Confirmation deactivation
10	Termination activation
11	Return information caused by a remote command
12	Return information caused by a local command
13	File transfer
20	Interrogated by general interrogation
21	Interrogated by interrogation group 1
22	Interrogated by interrogation group 2
23	Interrogated by interrogation group 3
24	Interrogated by interrogation group 4
25	Interrogated by interrogation group 5
26	Interrogated by interrogation group 6
27	Interrogated by interrogation group 7
28	Interrogated by interrogation group 8

29	Interrogated by interrogation group 9
30	Interrogated by interrogation group 10
31	Interrogated by interrogation group 11
32	Interrogated by interrogation group 12
33	Interrogated by interrogation group 13
34	Interrogated by interrogation group 14
35	Interrogated by interrogation group 15
36	Interrogated by interrogation group 16
37	Interrogated by counter general interrogation
38	Interrogated by interrogation counter group 1
39	Interrogated by interrogation counter group 2
40	Interrogated by interrogation counter group 3
41	Interrogated by interrogation counter group 4
44	Type Identification unknown
45	Cause unknown
46	ASDU address unknown
47	Information object address unknown

Settings

Structure			
<div>Structure</div> <div>COT size in bytes: 2</div> <div>ASDU size in bytes: 2</div> <div>IOA size in bytes: 3</div>		Master, Slave, Monitor	
	COT size in bytes	COT size in bytes	
	ASDU size in bytes	ASDU size in bytes	
	IOA size in bytes	IOA size in bytes	
Timeouts (ms)			
<div>Timeouts</div>		Master	Slave
	t0 in seconds	Timeout for the establishment of the connection with the server.	Not used

<div> <div>t0 in seconds: <input type="text" value="30"/></div> <div>t1 in seconds: <input type="text" value="15"/></div> <div>t2 in seconds: <input type="text" value="10"/></div> <div>t3 in seconds: <input type="text" value="20"/></div> </div>	t1 in seconds	This parameter defines the time in seconds that Master waits maximum for an acknowledge from the slave.	This parameter defines the time in seconds that slave waits maximum for an acknowledge from the master.
	t2 in seconds	A S-format frame will be sent at the latest after this time starting from the last received telegram from the slave.	A S-format frame will be sent at the latest after this time starting from the last received telegram from the master.
	t3 in seconds	A Test frame will be sent at the latest after this time starting from the last received telegram from the slave.	A Test frame will be sent at the latest after this time starting from the last received telegram from the master.

Windows			
<div>Windows</div> <div> <div>RWT (w) size: <input type="text" value="8"/></div> <div>SWT (k) size: <input type="text" value="12"/></div> </div>		Master	Slave
	w size	This parameter indicates the number of received I frames after the S-Frame will be send.	This parameter indicates the number of received I frames after the S-Frame will be send
	k size	Maximum I-frames send until acknowledgment.	Not used

SLAVE Parameters		
<div>Parameters</div> <div> <input checked="" type="checkbox"/> Send End of ini. on start up <input checked="" type="checkbox"/> Auto ack. U-Frame <input checked="" type="checkbox"/> Auto ack. control commands <input checked="" type="checkbox"/> Auto ack. system commands </div>		Slave
	Send End of ini. on start up	Send end of initialization TI 70 (M_EI_NA_1)
	Auto ack. U-Frame	Auto ack. U-Frame.
	Auto ack. control commands	Auto acknowledge commands
	Auto ack. system commands	Auto acknowledge system commands (TI: 100, 103)

MASTER Parameters		
<div>Parameters</div> <div> <input checked="" type="checkbox"/> Send Start DT on start up <input checked="" type="checkbox"/> Auto ack. Test Frame </div>		Master
	Send Start DT on start up	Send Start DT on startup
	Auto ack. Test Frame	Auto ack. Test frame

System

For all system functions user can set custom address:

APDU

ASDU:

☐ Test

Originator:

General Interrogation

This function will send telegram Type-identification = 100 (C_IC_NA_1)

General interrogation

Send

QOI:

QOI - qualifier of interrogation [0...255]

- 20 - Station interrogation
- 21 - Interrogation of group 1

- 22 - Interrogation of group 2
- 23 - Interrogation of group 3
- 24 - Interrogation of group 4
- 25 - Interrogation of group 5
- 26 - Interrogation of group 6
- 27 - Interrogation of group 7
- 28 - Interrogation of group 8
- 29 - Interrogation of group 9
- 30 - Interrogation of group 10
- 31 - Interrogation of group 11
- 32 - Interrogation of group 12
- 33 - Interrogation of group 13
- 34 - Interrogation of group 14
- 35 - Interrogation of group 15
- 36 - Interrogation of group 16

Counter Interrogation

This function will send telegram Type-identification = 101 (C_CI_NA_1)

Counter interrogation

FRZ:
RQT:

FRZ - freeze[0..3]

- 0 - Station interrogation
- 1 - Interrogation of group 1
- 2 - Interrogation of group 2
- 3 - Interrogation of group 3

RQT - request[0..63]

- 1 - Counter group 1
- 2 - Counter group 2
- 3 - Counter group 3
- 4 - Counter group 3
- 5 - General request

Commands

Read command will send telegram Type-identification = 102 (C_RD_NA_1)

Test command will send telegram Type-identification = 104 (C_TS_NB_1)

Commands

Clock synchronization

This function will send telegram Type-identification = 103 (C_CS_NA_1)

Clock synchronization

☐ IV
☐ SM
☐ SB

☒ PC time

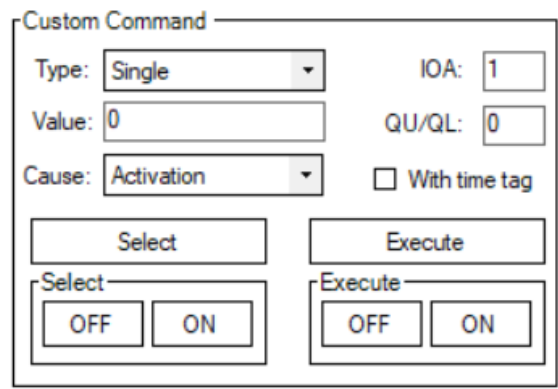
If "PC time" checkbox is checked, then the PC time will be sent. If it's not checked user can set time manually.

Time tag status bits:

- **IV** - invalid time
- **SM** - Summer/Winter
- **SB** - Substitute

Custom Commands

This function allows user to send commands to the slave device.



Custom Command

Type: IOA:

Value: QU/QL:

Cause: ☐ With time tag

Select

Select

Execute

Channel

With these functions a user has the ability to send any U or S frame telegram.



U-frame

- **Start DT act** - Send *Start Data terminal* activation
- **Start DT cnf** - Send *Start Data terminal* confirmation
- **Stop DT act** - Send *Stop Data terminal* activation
- **Stop DT cnf** - Send *Stop Data terminal* confirmation
- **Test Frm act** - Send *Test Frame* activation
- **Test Frm cnf** - Send *Test Frame* confirmation



S-frame

S-Frame ack - Send S-Frame. User can specify acknowledgment telegram count in text box.

Tags

This function allows user to created named points. After points created user can send it manually or set reply checkbox to automatic reply.

- To export Tags to csv file: **Tags -> Export -> Save file dialog appear**
- To import Tags from csv file: **Tags -> Import -> Open file dialog appear**

There are two ways of creating tags:

1. Create tag button.
2. Double click a signal with the left mouse button in the statistic tab.

Main parameters:

- **Name** - user-friendly tag name
- **Asdu** - Identifier of the device
- **loa** - Identifier of values from the device.
- **Type** - the type of value.

Here is an example image of the tag window with the **M_SP_TB_1 (30)** type selected. Each type has different options that can be configured when sending data. For example this type depicted in the picture below can send a value **Off** or **On** and it also is time-tagged. The user in this case can either select a specific time that they have in mind or just mark the PC checkbox and The Vinci software will automatically send the current PC time. As you can see the Value box in this example is greyed out that is because this tag is created on a **master** simulation, and this type doesn't support writing to slave.

Tag

Name:

Type:

Asdu: Ioa: Value:

Quality: ☐ BL ☐ SB ☐ NT ☐ IV ☐ OV

Time: ☐ PC

Setup

To setup an IEC 60870-5-104 simulation it is fairly straightforward.

1. Select IEC 60870-5-104 and the mode.

Protocol:

Mode:

2. Select Ethernet settings to connect to device. Set the **IP** and the **Port**. (Default port: 2404)

IP:

Port:

3. Select settings in the settings tab according to your device and preference.

Structure

COT size in bytes:

ASDU size in bytes:

IOA size in bytes:

Parameters

☒ Send Start DT on start up

☒ Auto ack. Test Frame

Timeouts

t0 in seconds:

t1 in seconds:

t2 in seconds:

t3 in seconds:

Windows

RWT (w) size:

SWT (k) size:

4. Press the green **START** button and the simulation should start. If everything was done correctly The Vinci software should establish communication with the IEC 60870-5-104 device which you can monitor in the console tab.

Protocol:	<input type="text" value="IEC 60870-5-104"/>	<div>START</div>
Mode:	<input type="text" value="Master (Client)"/>	

🕒Revision #10
★Created 24 January 2022 09:32:12
✎Updated 23 June 2022 15:21:10