Operating instructions

WinPP104 test program

Receive, check, filter, store, display, print, transmit and
simulate IEC 60870-5-104 messages.
The program creates a process image and a TCP 104 connection table.

Contents

1 Installation

Note: For the driver installation you must log on as Administrator.

System Requirements: Windows 10, 8, 7, Vista or XP, Pentium, 100 MB RAM, 100 MB Disc, VGA or better, Network interface (LAN Ethernet, TCP/IP) and USB port for dongle.

The setup program of WinPP104 is delivers on CD. On the CD the program is in the folder “Programme”.
The file name is SetupWinPP104vnnnn.exe, nnnn stands for program version.
Par example: SetupWinPP104v2300.exe = Setup program for WinPP104 Version 2.3.0.0.

Insert the CD into the drive and start the program "SetupWinPP104vnnnn.exe”, then follow the instructions on the screen.

You can uninstall WinPP104 via the dialogue field "Properties of Software” (Menu: *Start | Settings | System Control | Software*).

After installation the following files are in the chosen directory:

WinPP104.exe	Test program
W104Text.ger	Program texts in German
W104Text.usa	Program texts in English
W104Ger.chm	German Online Help
W104Usa.chm	English Online Help
Bed104Ger.pdf	German operating instructions
Bed104Usa.pdf	English operating instructions
CbSetup.exe	Auxiliary program, installs the dongle driver.
ExText4.csv	Example file for text of objects.
Typ4Ger.csv	Example file for short texts of message types, German.
Typ4Usa.csv	Example file for short texts of message types, English.
4Version.txt	Versions log of WinPP104.
Log.lg4	Standard Log file for online messages
SeTel.st4	Standard file for transmission messages and lists.

You can also save Log files, and the files for transmission messages and lists, under your own choice of name for reloading later. Do not add the file extensions ("lg4” or "st4”) as the program automatically append them.

On exiting the program it saves the configuration specific to your PC in the file W104.cfg.

2 Overview

2.1 Function

WinPP104 is a test and simulation program for the telecontrol protocol IEC 60870-5-104. You can monitor the messages of an existing connection or simulate the client (master) or the server (substation). The program creates a process image and a TCP 104-connection table, see Menu: "View > Process image or Connections". You can display the process image and the connections online or use them for filtering.
You can start the program several times and simulate several Masters or Stations.

The program can be used without administrator rights.
Upon the first start, the program creates the "Data Directory" under "C:\MyDocuments\ Users\ User Data\ PPFink\ WinPP104\ and copies the "Log.lg4" and "SeTel.st4" files into the directory. The "Data Directory" is used for saving the log, send and configuration data.
You can change the directory with the menu „Parameterize | General | Data directory".

Settable parameters (among others):

- Program function (Master, Station, Monitoring)
- Send messages
- Send lists
- Text of the objects, substations and IP addresses (Text file)
- Simulation of command responses
- Check delay time (transmission time) of the commands (Type: 58-64)
- Simulation answer of general interrogation
- Messages into csv files send, see help text: message parameterize > type.
- Cyclic transmission of an extern telegram, loading lists, command responses, see help text: options parameterize.
- Color of the objects
- Structure of station address and of object address
- The parameters t_0, t_1, t_2, t_3, k and w
- IP address of partner station
- IP address of the master

When storing or displaying messages you can filter them with respect to:

- Message type, Cause of transmission, Quality descriptor
- IP address
- Port number
- Data type
- Common address
- Object address, Originator address
- Time, Message number (and others)

The program reads the texts from a text file (csv format), see also file "ExText4.csv" in the program directory. Select a CSV file in the "File | Objecttexts Load" menu. The currently used file is indicated in the status bar. Format of the text file:
Function: Lines assigning a text to a Common (substation) Address.
Format: CA; Common Address;text;
Example: CA; 244;Berlin;
Function: Lines assigning a text to a IP Address.
Format: IP; IP Address;text;
Example: IP; 192.168.0.10; Master east;

Function: Lines assigning a color and a text to a Object Address.
Format: Object Address;color; text;
Example: 315432; 0;110kV AF F101 Trafo 11 LS;

You find the color code and additional example in the file “ExText4.csv” in the program folder. Don't use the file names "BspText4.csv" and "ExText4.csv". These files are overwritten during each installation.

The program checks the received messages for transmission errors, link faults and ASDU faults. Faulty messages are marked as such. Every transmitted and received message is allocated a time stamp and is stored in a Log file.
You may also import files (pcap-Format) which are created by “libpcap” or “winpcap” programs, menu “File | Log open”. The maximum size and the log file directory can be defined via the related parameters. As a rule, the program uses the ”Log.lg4“ log file. If the user activates the ”Use new log file every day ...“ option (see Parameterize | Options), a new log file will be created for each day of the month. The number of the day (01 - 31) is indicated in the file name.

During reception, the user can page up and down the messages saved in the log file and shown on screen. A message of 20 bytes takes up 50 bytes of Log file space.
The log file can be printed or saved as a text file or log file.

Start options
With startup options you can modify the program start see online Help > Overview > Start Options.

The parameters used last (function, t_0, t_1, t_2, t_3, k…) are also saved in the transmit message file and in the log file.

The Log file is organised as a circular buffer. When the file is full then the newest message overwrites the oldest message. You can prevent this by deleting (Ctrl+D) the old messages, before you start testing or increase the maximum size of the Log file or limit the time for message storage or the number of stored messages via Filter.

If you start the program several times the following log files are used: Log.lg4, Log2.lg4, Log3.lg4, etc.

The message colors may be modified in one of the following ways:

- Color of the receiver/transmitter (lowest priority)
- Color of the transmission cause (dialog or file ExText4.csv)
- Color of the ASDU type
- Color of the object address, refer to the ExText4.csv object text file.
- Color for messages with qualifier greater than zero (highest priority).

When storing or displaying messages you can filter them with respect to: time, message number, type, station address, object address, etc. With the time filter you can specify, for example, that only messages from 02:00 till 08:00 should be stored.

The transmitted messages are parameterized logically. There are 12 messages and 12 lists available, see **Parameterize message** or **Parameterize list**. In a list you can parameterize 3000 objects. For the simulation of command responses 1000 objects are available. The transmission instigation for the messages and lists takes place via the operation **Transmit** or via an event. An event can be: reception of a particular type of message or successful establishment of a link. You can then send an interrogation command, answer an interrogation command automatically, send commands, simulate responses, transmit cyclic measured values or simulate an avalanche of messages.

For test purposes you can send illogical messages. For example: send private ASDU, increment the Send Sequence Number by 2, or do not send ACKs, see online help Simulate faults.

2.2 Initial start

Place the Dongle onto the parallel (LPT) or USB interface and start the program. You choose the English or German user interface with the menu “Parametrieren | Sprache”. Connect the PC with the network. On starting the first time you should parameterize in the dialogue field Parameterize Rec/Trans 1 (Menu: Parameterize | Receiver/Transmitter 1) the following parameters:

“Function: ...” and
“IP Address of Partner station: ...”.

Save the parameters by clicking "OK".
Choose the display "On-line message” (Menu: View).
Go On-line (Menu: Mode).
Please note the table, the LEDs and the status bar at the bottom of the window.

If you receive the message "e.n.n.n Dongle missing/wrong" after entering the online mode then check please:

- Was the program installed with administrators’ right?
- Is the dongle on USB present?

The error code e.n.n.n has the following meaning:

2, 1011 or 1034.n.n.n	Dongle not found.
1004, 1005 or 1006.n.n.n	Device driver not installed.

With the Menu View or the keypad shortcut ”1 to 7” you can change the output format of the messages. The current output format is displayed in the heading.

WinPP104 saves the current parameters, Log file and messages when you exit from the program.

For test purposes you can carry out a loop test. Parameterize: "Function” from Receiver/Transmitter 1 to "Station” and "Function” of Receiver/Transmitter 2 to "Master”. Enter your own IP address for the "IP Address of Partner station”.

If no network card is installed in the PC, enter the IP address 127.0.0.1.

2.3 Operating Instructions

The usual Windows operations apply for program start, maximising, minimising and closing the program window.

The program WinPP104 uses menus for setting values and operation.

You call the on-line Help for any main menu and for the dialogue fields via the key "F1" (e.g. select the menu and press F1).

You can select menus and input fields with the mouse or keypad. Keypad selection takes place via the "Alt" key and a "**Hotkey**". "Hotkey" is the underlined character in the menu text (e.g. "F" in File Menu) or in the label of an input field. Some operating systems display the Hotkey in the menu text only after menu selection (Press the Alt key).

For commonly used commands (On-line, Off-line, Transmit Message) you can enable a "**keypad shortcut**”, see Menu “Parameterize | Options” . A "keypad shortcut” is a key combination with which you execute a command directly. For example the key combination “Alt+F1” transmits the first message or “Ctrl+D” deletes the messages in the log file.

Please note that the key Alt activates the Menu selection (a Menu is optically highlighted/raised). If the Menu selection is activated then the shortcuts are **deactivated**. By pressing the Alt key once more you can deactivate the Menu selection again.

If you have selected a table then you are in Navigation mode. Select the desired field with the cursor keys. By a mouse click or by using the key F2 or by pressing "any key" you change to the edit mode. If the "any key" is a valid input then the character entered replaces the previous value. If the input is an invalid key then the current value is retained.

In dialogue windows you can select the next field with the keys "Tab" or "Enter" (Return) or select the previous field with "Shift+Tab". In a drop-down field you can make the list drop down via the key F4 or make a selection with the arrow keys Up/Down or the Spacebar.

In the dialogue windows usually the buttons "OK", "Cancel" and "Help" are displayed. "OK" saves the entered values and ends the input, "Cancel" ends the input **without** saving the values, "Help" calls the on-line Help for the current dialogue field.

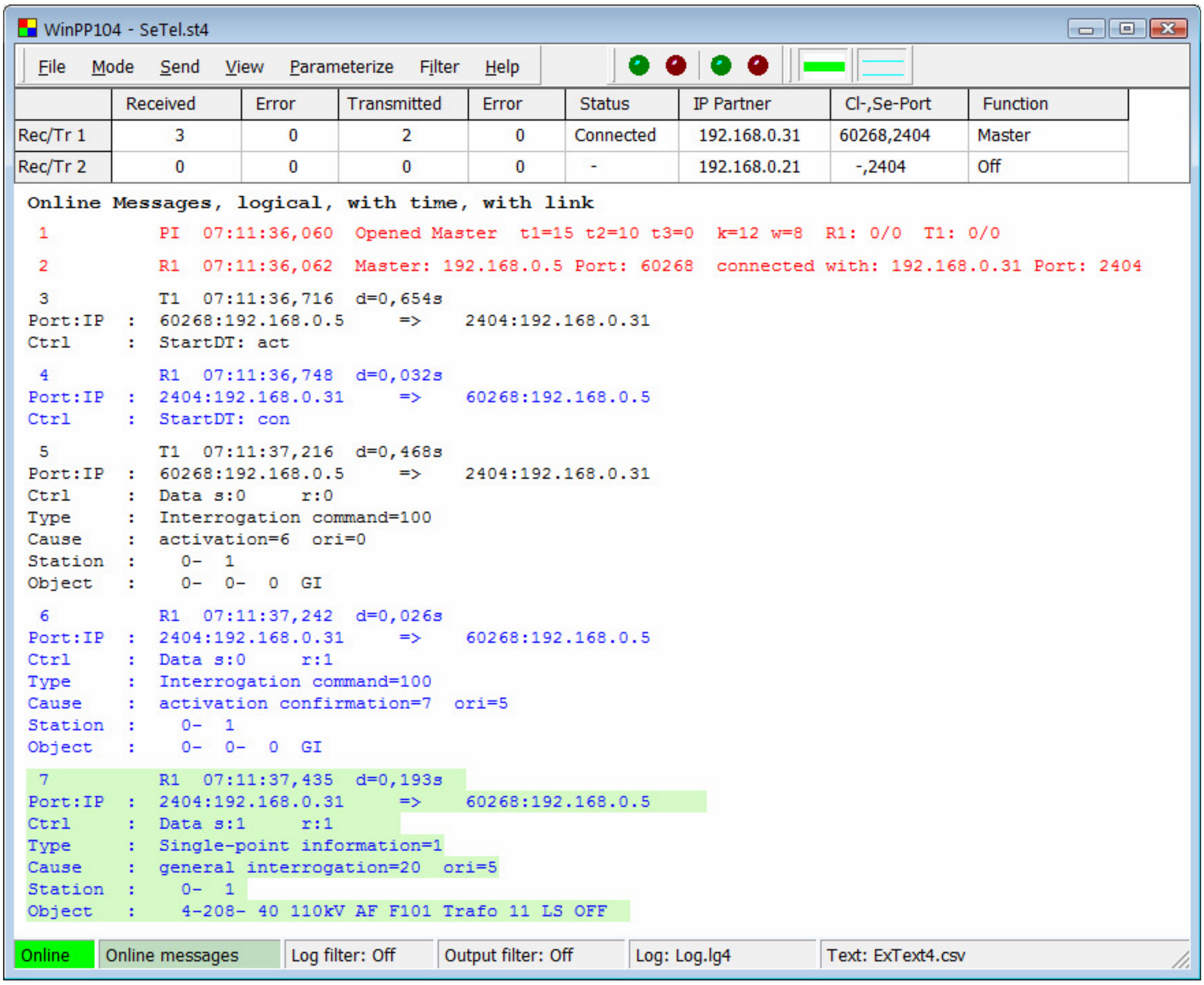
You can enter numbers as decimal or hexadecimal numbers, example: 100 or $64;

2.4 Display Messages

The program displays either the "On-line messages” or the "Log messages”. The title bar displays the program name, the name of the send telegram file and the data directory. If the send telegram file is not in the data directory, the path of the send telegram file is also displayed. With the Menu **View** you select the messages and the output format. The status bar (lowest line) displays the program status, the kind of displayed message, the status of the filters and the name of the Log file. The kind of message will also be displayed in the message header. With the **Output filter**you can filter the On-line messages and the Log messages. The meanings of abbreviations can be found in the online help. Faulty messages are marked with an Error text. For the message time a millisecond timer is used which is always synchronised with the PC time at a change from offline to online. For a received message the message time gives the time of reception of the last byte of the message, for a transmitted message the time of starting transmission. With a right click you call the pop up menu.
After the time, the time difference to the previous telegram is displayed, eg: d = 0.035 s means: The current telegram was saved 35 ms after the previous telegram. If the time difference is zero, the current and the previous telegram was transferred in the same packet (frame). The time difference of zero is not displayed.

Display On-line messages

In the window of the "On-line Message Display” you can see the Status Table, the Header and the received and transmitted messages. The messages will be issued one below the other. The lower most is the newest message.



	Received	Error	Transmitted	Error	Status	IP Partner	Cl-,Se-Port	Function
Rec/Tr 1	3	0	2	0	Connected	192.168.0.31	60268,2404	Master
Rec/Tr 2	0	0	0	0	-	192.168.0.21	-,2404	Off

```
Online Messages, logical, with time, with link
 1          PI  07:11:36,060  Opened Master  t1=15 t2=10 t3=0  k=12 w=8  R1: 0/0  T1: 0/0
 2          R1  07:11:36,062  Master: 192.168.0.5 Port: 60268  connected with: 192.168.0.31 Port: 2404
 3          T1  07:11:36,716  d=0,654s
Port:IP   :  60268:192.168.0.5      =>    2404:192.168.0.31
Ctrl      :  StartDT: act
 4          R1  07:11:36,748  d=0,032s
Port:IP   :  2404:192.168.0.31      =>    60268:192.168.0.5
Ctrl      :  StartDT: con
 5          T1  07:11:37,216  d=0,468s
Port:IP   :  60268:192.168.0.5      =>    2404:192.168.0.31
Ctrl      :  Data s:0      r:0
Type      :  Interrogation command=100
Cause     :  activation=6   ori=0
Station   :    0-  1
Object    :    0-  0-   0  GI
 6          R1  07:11:37,242  d=0,026s
Port:IP   :  2404:192.168.0.31      =>    60268:192.168.0.5
Ctrl      :  Data s:0      r:1
Type      :  Interrogation command=100
Cause     :  activation confirmation=7   ori=5
Station   :    0-  1
Object    :    0-  0-   0  GI
 7          R1  07:11:37,435  d=0,193s
Port:IP   :  2404:192.168.0.31      =>    60268:192.168.0.5
Ctrl      :  Data s:1      r:1
Type      :  Single-point information=1
Cause     :  general interrogation=20   ori=5
Station   :    0-  1
Object    :    4-208- 40 110kV AF F101 Trafo 11 LS OFF
```

Online | Online messages | Log filter: Off | Output filter: Off | Log: Log.lg4 | Text: ExText4.csv

Online message display

The output format can be selected via Menu View.
The Status Table displays the most important parameters from receiver/transmitter 1 and 2, see also **Parameterize Rec/Trans**. The columns have the following meaning:

Text **Description**

Received Displays the number of received and saved messages since selection of on-line status.

Errors Displays the number of received and saved messages with errors since selection of on-line status.

Transmitted Displays the number of messages transmitted since selection of on-line status.

Errors Displays the number of repeatedly transmitted messages since selection of on-line status.

Status Displays the state of the port.

-	Port is off-line
Opened	Port is waiting for connection.
Connected	Port is connected.

IP Partner Displays the IP address of the partner station.

Cl., Se. Port Displays the port number of the client and server after a connection is established.

Function Displays the parameterized function.

The **Header** displays the kind of message, the filter function and the output format. The messages are displayed continuous (scroll mode). If you wish to look at the messages received at your own speed, select “Display Log messages” via F9. The program continues to send/transmit in the background.

Display Log messages
In the “Log Message Display” window will be displayed: the Header, the date and the number of the first message and the number of messages. The output format can be selected via menu View.

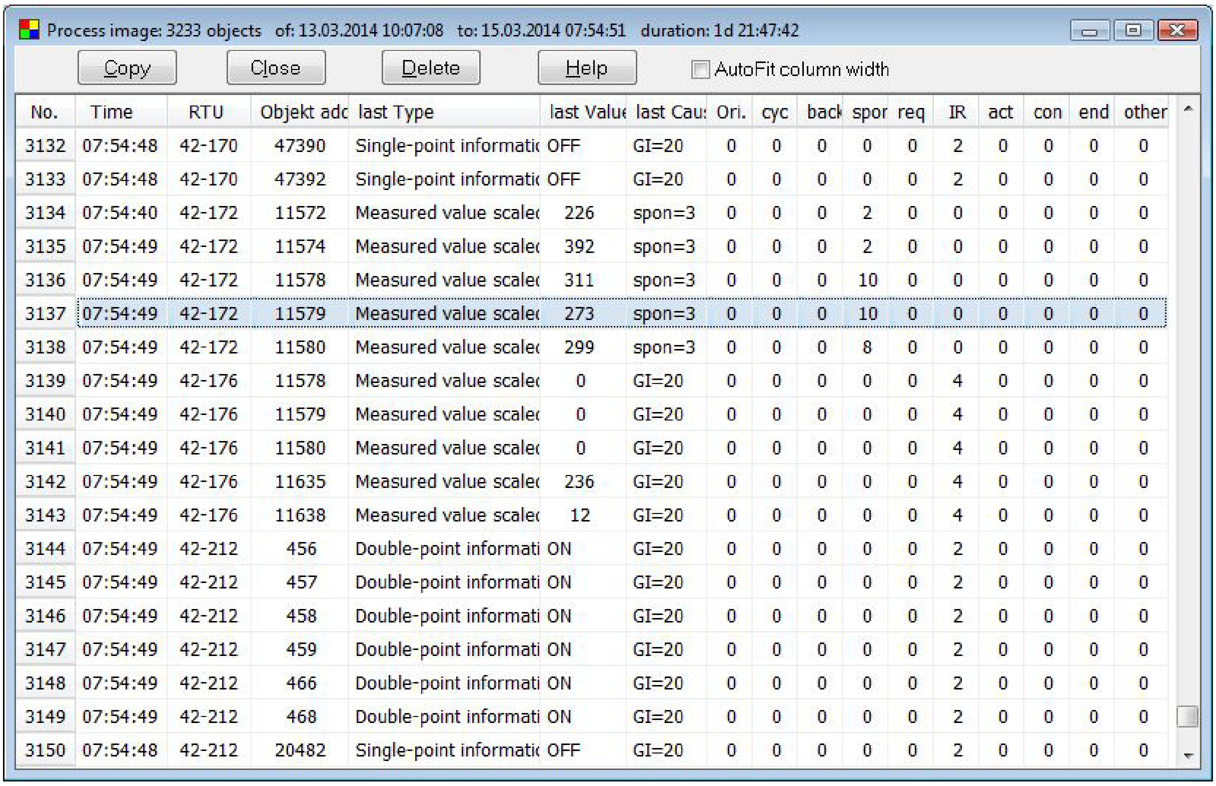
With the cursor keys and the scroll bar you can page forwards and backwards. The cursor key Up/Down leafs one message back or forwards. The Page Up/Down keys move five messages backwards or forwards. If you press simultaneously the key Page up/down and the Key Shift, Control or Shift and Control then you move 50, 500 or 5000 messages backwards or forwards. The Home key displays the first (oldest) message. The End key displays the latest (newest) message. If the on-line reception overwrites the messages just being displayed, then the last message received will be displayed the next time that you leaf through the pages.

2.5 Process image

When you are monitoring or simulating the program builds a process image. The output is via the menu "View > Process Image" or via the context menu. The process image is useful for a quick overview of the state of the objects and to filter for an object in the log file. To filter for an object by clicking in the "No" column of the row.

Each table row corresponds to an object. The objects are grouped by RTU address, Object address and type.

The number in the "No." column is a sequential number, "time" is the last reception time, "RTU" is the RTU address, "last type" is the last object type, "last value" is the last value of the object, "last cause" is the cause of transmission, “Ori.” is the originator address, "cyc, back, spon, req, IR, act, con, end, other" are counters of the causes of transmission: cyclic, background, spontan, requested, interrogated or requested counter, activation, confirmation or return information command, end of activation and all other causes.


Process image: 3233 objects of: 13.03.2014 10:07:08 to: 15.03.2014 07:54:51 duration: 1d 21:47:42

No.	Time	RTU	Objekt adc	last Type	last Valu	last Cau	Ori.	cyc	back	spor	req	IR	act	con	end	other
3132	07:54:48	42-170	47390	Single-point informatic	OFF	GI=20	0	0	0	0	0	2	0	0	0	0
3133	07:54:48	42-170	47392	Single-point informatic	OFF	GI=20	0	0	0	0	0	2	0	0	0	0
3134	07:54:40	42-172	11572	Measured value scalec	226	spon=3	0	0	0	2	0	0	0	0	0	0
3135	07:54:49	42-172	11574	Measured value scalec	392	spon=3	0	0	0	2	0	0	0	0	0	0
3136	07:54:49	42-172	11578	Measured value scalec	311	spon=3	0	0	0	10	0	0	0	0	0	0
3137	07:54:49	42-172	11579	Measured value scalec	273	spon=3	0	0	0	10	0	0	0	0	0	0
3138	07:54:49	42-172	11580	Measured value scalec	299	spon=3	0	0	0	8	0	0	0	0	0	0
3139	07:54:49	42-176	11578	Measured value scalec	0	GI=20	0	0	0	0	0	4	0	0	0	0
3140	07:54:49	42-176	11579	Measured value scalec	0	GI=20	0	0	0	0	0	4	0	0	0	0
3141	07:54:49	42-176	11580	Measured value scalec	0	GI=20	0	0	0	0	0	4	0	0	0	0
3142	07:54:49	42-176	11635	Measured value scalec	236	GI=20	0	0	0	0	0	4	0	0	0	0
3143	07:54:49	42-176	11638	Measured value scalec	12	GI=20	0	0	0	0	0	4	0	0	0	0
3144	07:54:49	42-212	456	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3145	07:54:49	42-212	457	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3146	07:54:49	42-212	458	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3147	07:54:49	42-212	459	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3148	07:54:49	42-212	466	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3149	07:54:49	42-212	468	Double-point informati	ON	GI=20	0	0	0	0	0	2	0	0	0	0
3150	07:54:48	42-212	20482	Single-point informatic	OFF	GI=20	0	0	0	0	0	2	0	0	0	0

The above example is an excerpt from a process image with 3233 objects.

"Copy" copies the objects in CSV format to the clipboard.
"Delete" will delete the objects data.
"AutoFit Column Width" If selected, the columns will change when outputting for the longest text.

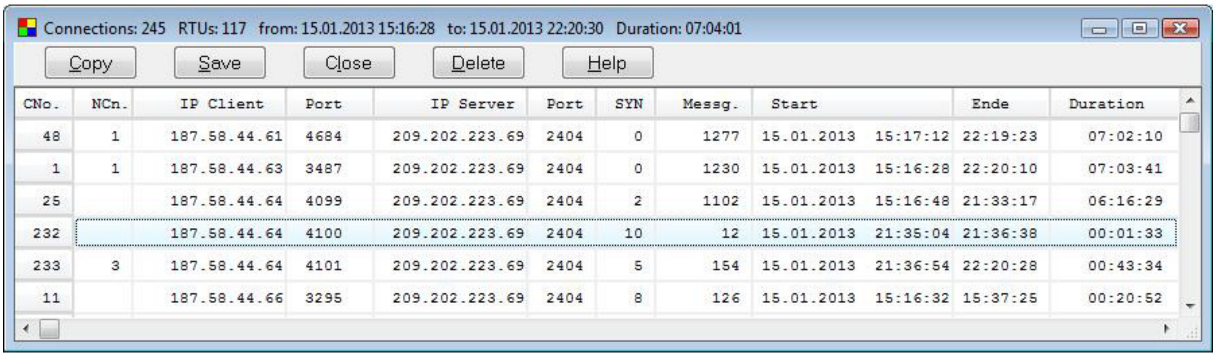
2.6 TCP 104 connections

While listening, the program is building a TCP 104 connection table. The output is via the menu "View > Connections" or via the context menu. The connection table is useful for a quick overview of the existing connections, to filter for a connection, to monitor unsafe connections (wireless connection) or when the devices do not behave as expected. To filter for a connection, click in the Connection = "CNo." column of the respective row. The number in the "CNo." column indicates the chronological order in which the connections were monitored. "1" corresponds to the first connection. The column "NCn" indicates the number of connections per station. If not specified, there are multiple connections to this station. In the last connection is then the number of connections.

Each table row corresponds to a connection. The connections are sorted by IP client, IP server, Port server, CNo.

In the column "SYN" You can see the number of messages with SYN, FIN or RESET bit. A number greater than zero indicates connection, disconnections while monitoring. "Messg." specifies the number of received messages. "Start" and "end" is the time of the first or last listened telegram. "Duration" is the difference between start and end. Details are shown in the log file.

Is the time interval between two telegrams greater than two hours, the new message a new connection is assigned. The port number of the client is extended with "-n", wherein n is 2, 3, 4 and so on.


Connections: 245 RTUs: 117 from: 15.01.2013 15:16:28 to: 15.01.2013 22:20:30 Duration: 07:04:01

CNo.	NCn.	IP Client	Port	IP Server	Port	SYN	Messg.	Start		Ende	Duration
48	1	187.58.44.61	4684	209.202.223.69	2404	0	1277	15.01.2013	15:17:12	22:19:23	07:02:10
1	1	187.58.44.63	3487	209.202.223.69	2404	0	1230	15.01.2013	15:16:28	22:20:10	07:03:41
25		187.58.44.64	4099	209.202.223.69	2404	2	1102	15.01.2013	15:16:48	21:33:17	06:16:29
232		187.58.44.64	4100	209.202.223.69	2404	10	12	15.01.2013	21:35:04	21:36:38	00:01:33
233	3	187.58.44.64	4101	209.202.223.69	2404	5	154	15.01.2013	21:36:54	22:20:28	00:43:34
11		187.58.44.66	3295	209.202.223.69	2404	8	126	15.01.2013	15:16:32	15:37:25	00:20:52

The above example is an excerpt from a table with 245 connections and 117 stations. The station 187.58.44.64 has established three connections.

"Copy" copies the connection data in CSV format to the clipboard.
"Save" saves the connection data in the log file.
"Delete" will delete the connection data.

3 Message structure

The message structure is defined by:

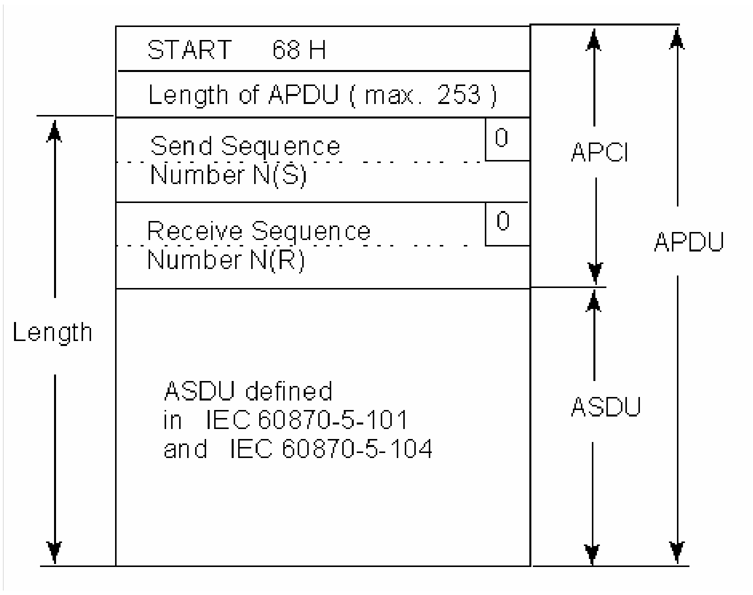
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-104	Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles

The following kinds of messages will be used:

- Data messages with variable length
- Acknowledge messages
- Control messages with constant length.

3.1 Format data message

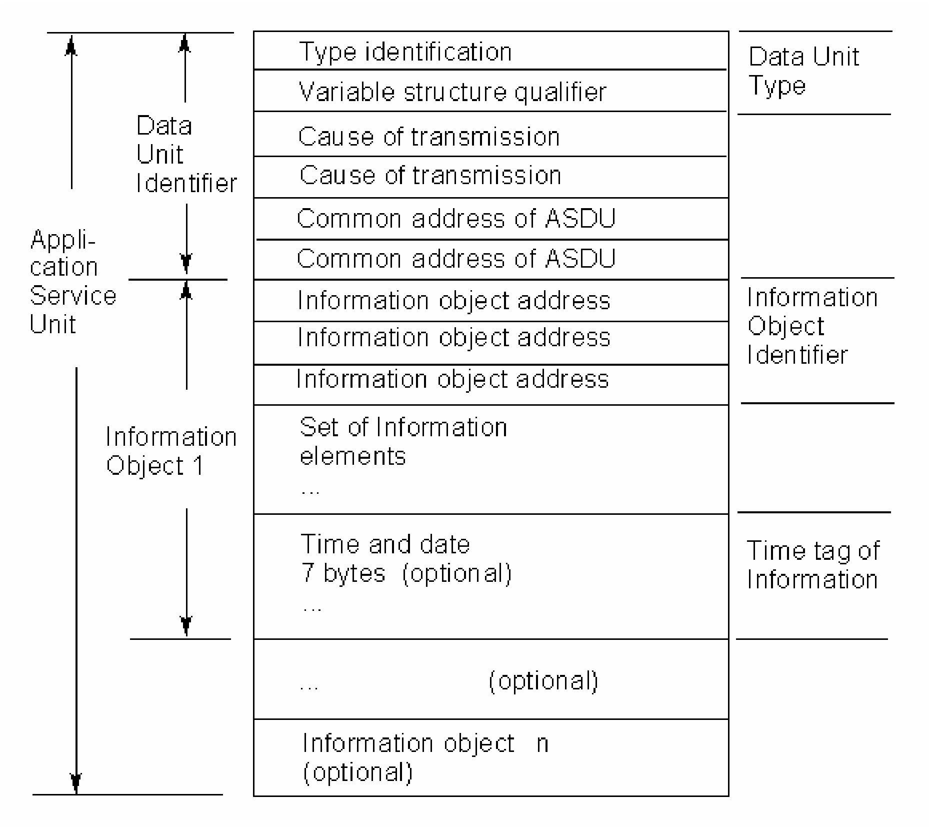
The data message consists of the Application Protocol Control Information (APCI) and the Application System Data Unit (ASDU).


START 68 H
Length of APDU (max. 253)
Send Sequence Number N(S)
0
Receive Sequence Number N(R)
0
ASDU defined in IEC 60870-5-101 and IEC 60870-5-104
Length
APCI
ASDU
APDU

The message length is a maximum of 255 bytes with a maximum 249 bytes of ASDU.

3.2 Format ASDU

ASDU = Application Service Data Unit.



Application Service Unit

Data Unit Identifier

Type identification

Variable structure qualifier

Cause of transmission

Cause of transmission

Common address of ASDU

Common address of ASDU

Information object address

Information object address

Information object address

Set of Information elements
...

Time and date
7 bytes (optional)
...

... (optional)

Information object n
(optional)

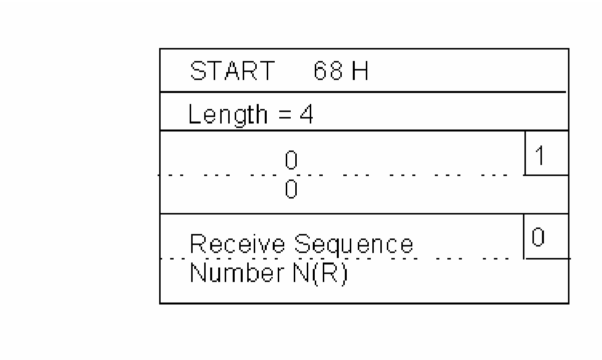
Information Object 1

Data Unit Type

Information Object Identifier

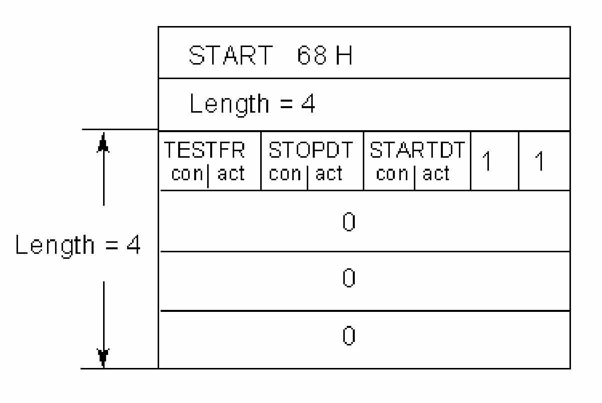
Time tag of Information

3.3 Format ACK message



The message length is 6 bytes.

3.4 Format control message



The message length is 6 bytes.