IEC 870-5-104 Server

IEC 60870-5-104 Server communication protocol

Supported device types and versions

This protocol implements a server-side of IEC-104 communication (known also as IEC 870-5-104 or IEC-104).

Communication supports reading and writing data by means of the IEC 60870-5-104 communication protocol operating on the basis of TCP network communication. D2000 system works in the IEC 60870-5-104 server mode (slave). It is able to communicate with multiple (N) clients (masters). Implementation is according to the IEC 60870-5-104 standard as follows:

- *Originator ASDU address* is 1 byte, it is defined as a line number.
- *ASDU address* is 2 bytes, it is defined as station address. For each station on a line, a different ASDU address must be defined.
- *Cause of transmission* is 2 bytes (it also contains Originator ASDU address)
- *Information object address* IS 3 bytes, it is defined as an I/O tag address.
- The following ASDU types in the direction of monitoring are implemented (from the D2000 system to the control station and also vice-versa in balanced mode):

Table 1

ASDU type	I/O tag type
1 - Single-point information	Dout
2 - Single-point information with time tag	Dout
3 - Double-point information	Dout,Cout
4 - Double-point information with time tag	Dout,Cout
5 - Step position information	Cout
6 - Step position information with time tag	Cout
7 - Bitstring of 32 bits	Cout
8 - Bitstring of 32 bits with time tag	Cout
9 - Measured value, normalized value	Ao
10 - Measured value, normalized value with time tag	Ao
11 - Measured value, scaled value	Cout
12 - Measured value, scaled value with time tag	Cout
13 - Measured value, short floating point value	Aout
14 - Measured value, short floating point value with time tag	Aout
15 - Integrated totals	Cout
16 - Integrated totals with time tag	Cout
20 - Packed single-point information with status change detection	Cout *
21 - Measured value, normalized value without quality descriptor	Ai

30 - Single-point information with time tag CP56Time2a	Dout
31 - Double-point information with CP56Time2a tag	Dout,Cout
32 - Step position information with CP56Time2a tag	Cout
33 - Bitstring of 32 bits with CP56Time2a tag	Cout
34 - Measured value, normalized value with CP56Time2a tag	Aout
35 - Measured value, scaled value with CP56Time2a tag	Cout
36 - Measured value, short floating point value with time tag CP56Time2a	Aout
37 - Integrated totals with time tag CP56Time2a	Cout
241 - 64-bit floating point value (Ipesoft & URAP implementation)	Ao
243 - 64-bit floating point value with time tag CP56Time2a (Ipesoft & URAP implementation)	Ao
251 - Archive data values (Ipesoft's implementation)	none **
252 - D2000 Unival (Ipesoft's implementation)	all

Note: For setting individual bits of the quality byte (SIQ for ASDU 1,2,30; DIQ for ASDU 3,4,31; QDS for ASDU 5..14,20,32..36), the flags A (0.bit), B (1.bit) .. H (7.bit) are used.

For example:

- for ASDU 4: A=DPI bit 0, B=DPI bit 1, C=0, D=0, E=BL bit, F=SB bit, G=NT bit, H=IV bit.
- for ASDU 16: A..E Sequence number bits 0..4, F=CY bit, G=CA bit, H=IV bit

The exception is the bits, which are set directly by a value (e.g. for ASDU 1, the 0.bit is not set by the A flag but by the value of output I/O tag).
If the *Invalid* attribute is set for a new value, the highest bit (*IV*) will be set in the status byte for all ASDUs (except for ASDU 21, which does not have a status byte).

* - *Status* is taken as low 2 bytes, *Status change detection* is taken as highest 2 bytes of a 32-bit integer.

The following ASDU types in the direction of control are implemented (from the control station to D2000, also the opposite direction in balanced mode):

Table 2

ASDU type	I/O tag type
45 - Single command	Di, Qi
46 - Double command	Qi
47 - Regulating step command	Di, Qi
48 - Set point command, normalised value	Ai
49 - Set point command, scaled value	Ci
50 - Set point command, short floating point value	Ai
51 - Bitstring of 32 bit	Ci
58 - Single command with time tag CP56Time2a	Di, Qi
59 - Double command with time tag CP56Time2a	Qi
60 - Regulating step command with time tag CP56Time2a	Di, Qi
61 - Set point command, normalised value with time tag CP56Time2a	Ai
62 - Set point command, scaled value with time tag CP56Time2a	Ci
63 - Set point command, short floating point value with time tag CP56Time2a	Ai

64 - Bitstring of 32 bit with time tag CP56Time2a	Ci
250 - Archive data request command (Ipesoft's implementation)	none **
252 - D2000 Unival (Ipesoft's implementation)	all (except Qi)

Bits of "status" byte (SCO fro ASDU 45,58; DCO for ASDU 46,59; RCO for ASDU 47,60; QOS for ASDU 48..50,61..63) causes setting the A (0.bit), B (1. bit) .. H (7.bit) flags with an exception for the bits which are directly set by the value of a variable (SCO bit 0, DCO and RCS bits 0-1). After receiving a response (positive/negative), the A .. H flags are set according to the bits of the "status" byte.

When writing values, the value of 6 [Activation] is expected as CauseOfTransmission. The response of the controlled station depends on the setting of the CMDC parameter. *Originator ASDU address* will be used the same as is in the received command.

Establishing a connection:

- D2000 KOM process is waiting on a TCP port and, after establishing a connection, is waiting for receiving the StartDT Act U-frame from the client. Then it sends StartDT Con as a response (it is possible to send TestFrame before StartDT Act).
- If the EOI parameter is set, the D2000 KOM process will send ASDU 70 [End of initialization], the initial OA address (configured as a line number) is used as *Originator ASDU address.*
- If the **Synchronisation period** parameter (the **Time parameters** tab) for some of the stations is different from 0, ASDU 103 [Clock synchronisation command] with CauseOfTransmission= 6 [Activation] will be sent in the configured period. The initial OA address (configured as a line number) resp. *Originator ASDU* of the last received ASDU 100 or 101 will be used as *Originator ASDU address*.
- D2000 KOM process sends new values acquired from the D2000 Server process for variables with ASDU 1..14, 20, 21, 30 .. 36 to a client, which sent ASDU 100 [Interrogation Command] and new values for variables with ASDU 15,16,37 to a client, which sent ASDU 101 [Counter Interrogation Command]
- D2000 KOM process accepts time synchronisation using ASDU 103 [Clock synchronisation command] with CauseOfTransmission=6 [Activation] or 3 [Spontaneous]. If CauseOfTransmission= 6, its response dependd on setting of the CMDC parameter. If CauseOfTransmission= 3, it does not respond.
- D2000 KOM process responds to received commands (ASDU 45..51, 58..64) with CauseOfTransmission= 6 [Activation] dependd on setting of the CMDC parameter.

Originator ASDU address (OA)*:* initial *OA* is set as TCP line number in the configuration. The address will be used for the optional sending of the ASDU 70 [End of initialization] at the beginning of a connection and always for sending new values.
After receiving ASDU 100 or 101, the current values of all output I/O tags are sent (which don't have an *Invalid* attribute set) with the same *OA* as contained in ASDU 100 or 101.
As responses to received commands (ASDU 45..51, 58..64), the confirmations using the same ASDUs as received command are sent.

The D2000 system also supports a **balanced mode**. In this mode, the task of controlled and control stations is symmetrical. In this mode, the D2000 system sends commands and ASDUs 100/101. The balanced mode may be used only if it is supported by the partner station. An advantage is that the D2000 system can send ASDU 100 [Interrogation Command] a 101 [Counter Interrogation Command] and receives the current values of input I/O tags (configured as ASDU 1-40) after the connection was disconnected and re-established. It is suitable to configure single-shot commands as ASDUs 45 - 64; they are not repeated after re-establishing the connection.

Writing of an output I/O tag:

- When writing IEC 104 values (ASDUs 1-40), the rules of server protocols apply.
- When writing IEC 104 commands (ASDUs 45-64) in the balanced mode, ASDU is considered to be confirmed (the *Transient* flag is cleared) in dependence on the CMDC parameter. If the connection to a client is lost when writing, the writing success depends on the PW parameter.

Communication line configuration

- Communication line category: TCP/IP-TCP
- TCP Parameters
  - Required to define the server parameters
  - Host: string containing at most 80 characters – the name of the network interface in form of INET (name or numerical address a.b.c.d, e. g. 192.168.0.1) used for receiving clients by the D2000 KOM process. If the name is *ALL* or *, the D2000 KOM process will listen on all network interfaces of the computer, where is running.
  - Port: TCP port number (0..65535), where the D2000 KOM process is listening.
  - Line number: will be used as *Originator ASDU address* (1 byte, 0-255).

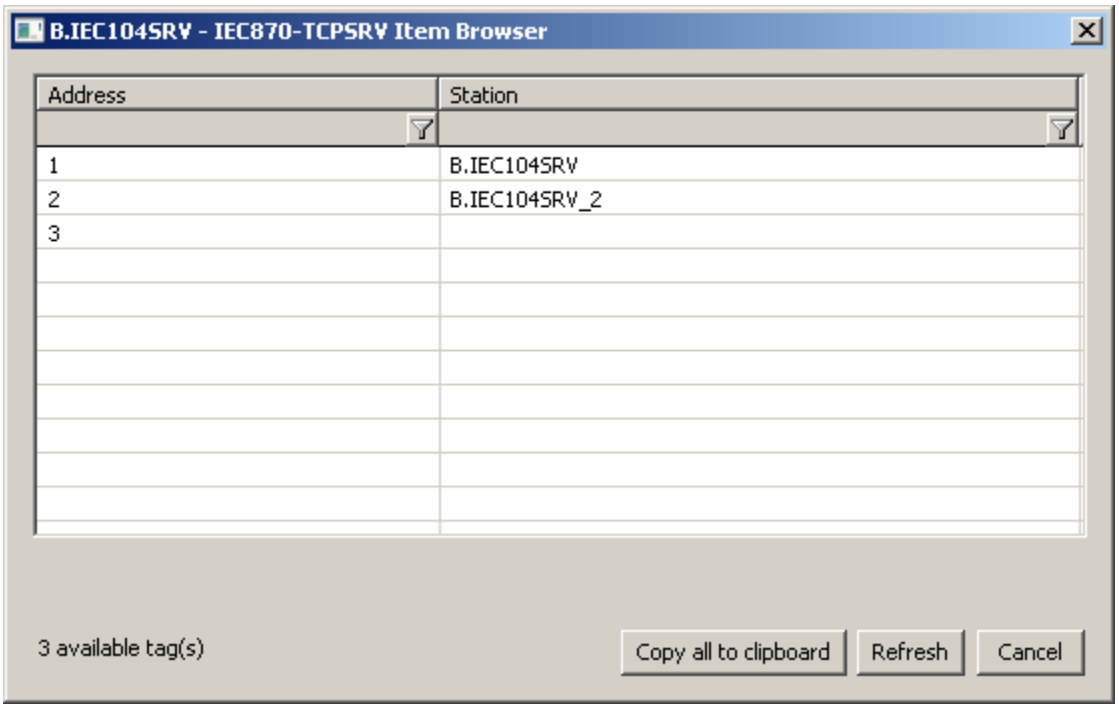
Note: Starting from D2000 version 7.02.004 the flags A to P of the value of the communication line are used for informing about connected active clients. An active client is a client who after establishing the connection sent U-frame StartDT Act, i.e. asked for sending the data. The first connected active client will cause a change of flag A to TRUE, the second flag B, etc up to flag P and continuing again with the first flag A. If the client sends the StopDT Act U-frame (requesting the server to stop sending data) or disconnects, the value of its flag will be changed to FALSE.

Communication station configuration

- Communication protocol: **IEC870-TCP Server**.
- The station address is a number within the range 0...65535, it defines the ASDU address. It can be specified as a decimal number or as a hexadecimal number with a hash at the beginning (e.g. #0A).

Note 2: The protocol supports sending long time stamps (CP56Time2a tag) in local time or UTC time with defined offset (see the Use monotonic UTC time+ parameter).

The **Browse** button opens a browsing dialog for the station address. If the communication is functional, a dialog with the ASDU addresses received so far is displayed. The **Refresh** button can be used to clear the list of received ASDU addresses.



Station protocol parameters

The following parameters can be defined as station protocol parameters:

Table 3

Keyword	Full name	Meaning	Unit	Default value
CMDC	Command Confirm	Confirmation of control ASDU. If CMDC=0, the D2000 KOM process does not confirm any control ASDU from the partner station by replying with an ASDU with an appropriate CauseOfTransmission. If CMDC=1, the D2000 KOM process confirms control ASDUs with CauseOfTransmission=7 (Activation Confirmation). If CMDC=2, the D2000 KOM process confirms control ASDUs with CauseOfTransmission=10 (Activation Termination). If CMDC=3, the D2000 KOM process confirms control ASDUs with CauseOfTransmission=7 and CauseOfTransmission=10.	-	1
D2CLS *D2CPA* *D2VCO*	The parameters are intended for the configuration of a communication station for communication between two D2000 systems using ASDU 252 - D2000 Unival (Ipesoft's implementation). more ...			

D2H64	D2000 64-bit Historical Values	When sending historical values (as an answer to a request for historical data), ASDU 249 will be used, which uses a 64-bit representation of floating points (the same as D2000 internally), instead of default ASDU 251 (which encodes the values as 32-bit floating points) to improve precision. **Note:** Before enabling this parameter, you should verify that also the client supports ASDU 249. This support was implemented in November 2011 for D2000 v8.00.011.	-	False
DBGI	Debug Input	A mask for debug levels of input data. The meaning of bits is as follows: • 0.bit - displays a number of incoming values during General Interrogation • 1.bit - displays all incoming values • 2.bit - balanced mode: requesting Interrogation command was received	-	0
DBGO	Debug Output	A mask for debug levels of output data. The meaning of bits is as follows: • 0.bit - balanced mode: displays a number of outgoing values during General Interrogation • 1.bit - displays all outgoing values	-	0
EOI	End of initialization	If EOI=0, the D2000 KOM process doesn't send ASDU 70 (End of initialisation). If EOI=1 and a client sends StartDT U-frame Act, the D2000 KOM process responds by StartDT Con and sends ASDU 70.	-	0
GISN	GI Send New	If GISN=True, then the D2000 KOM process after receiving the *General Interrogation* command sends also values with newer times than is the time when the command is received. The value of the *GI Send New* parameter must be True to send values with future times in a reply to the *General Interrogation* command.	-	False
ICF3	Ignore Control Field 3 bit 0	Determines behavior if ASDU contains Control Field with bit 0 (test) set in the 3rd byte (Receive). • if ICF3=False (default), ASDU content is to be processed • if ICF3=True, ASDU content is to be ignored The feature is useful when creating a redundant TCP connection (TCP Redundant line + IEC 870-5-104 protocol). That active client should send ASDUs without the Test bit set and the passive client should send ASDUs with the Test bit set.	-	False
III	Ignore Invalids on Interrogation	If this parameter is set on a station, the D2000 KOM process will not send values of I/O tags which are Invalid or Unknown, in a reply for ASDU 100 and 101 (Interrogation/Counter interrogation commands). The parameter can be used e.g. for control applications - if sending Invalid values causes problems in control.	-	False
IT	Ignore Tests	Determines behavior if ASDU contains the highest 7th bit (Test) set in CauseOfTransmission. • if IT=0 (default), ASDU content will be processed • if IT=1, ASDU content will be ignored • if IT=2, a *Weak* attribute will be set The feature is useful when creating a redundant TCP connection. The active client should send ASDUs without the Test bit set and the passive client should send ASDUs with the Test bit set.	-	0
IUA	Ignore Unknown Addresses	If IUA=TRUE, the D2000 KOM process will not show an error on its console or write it into log files in case that incoming value has the address not matching any of the addresses of I/O tags defined in the D2000 system.	-	False
II	Implicit Interrogation	Balanced mode: After connecting the client, the values of all variables are automatically sent without any need for ASDU 100 and 101 [Interrogation/Counter Interrogation Command] requests.	-	False
ICCI	Interrogation Covers Counter Interrogation	As a reply to Interrogation, ASDUs 15,16,37 (Integrated Totals) will be also sent, which are by default requested by ASDU 101 [Counter Interrogation].	-	False
IGO	Interrogation Groups Objects	Optimization of sending values during General Interrogation (answer to Interrogation Command/Counter Interrogation Command). If IGO=True, multiple values will be sent inside a single ASDU (so that the length of ASDU is within maximum defined by the standard - 253 Bytes). This parameter does not influence change-based sending of values during normal communication.	-	False
IWOT	Interrogation WithOut Timestamps	If *Interrogation WithOut Timestamp*=True then values sent as a response to ASDU 100 [Interrogation Command] will be sent as ASDUs without timestamps. For example instead of ASDU 2 (Single-point information with time tag) or ASDU 30 (Single-point information with time tag CP56Time2a) ASDU 1 (Single-point information) will be sent. This behavior is suitable in a situation when the values have been invalidated as a result of communication error and, after the communication is re-established, the values come with old timestamps which causes problems in the D2000 Archive (if the values change only rarely, calculated historical values depending on them will be also invalid till a new value arrives). At the same time, this behavior is strictly according to the IEC standard, which says that the response to Interrogation should not use ASDUs with time stamps.	-	False
K	K	Sending window size i.e. packet quantity, which is sent by the D2000 KOM process without receiving a confirmation (S-frame or I-frame). According to the standard, the default value is 12.	-	12
MC	Maximum Clients	The maximum number of connected clients. The parameter is needed for D2000 OpenVMS, where a task pool containing 2 * MC tasks for client handling (one task for receiving data, one task for sending data) is created during KOM startup. If the value of the *Maximum Clients* parameter is equal to 0, the number of clients is not limited and threads are created dynamically as needed.	-	0
NF	No Flags	If the value of the parameter is True, then the status byte of incoming ASDUs is ignored and not saved into the A .. H flags. Flags of output I/O tags are also ignored and they don't influence the status byte.	-	False
OCIC	Order of Counter IC	Balanced mode: Order of sending of ASDU 101 [Counter Interrogation Command] when initializing the connection. If OCIC<OIC, then ASDU 101 is sent before ASDU 100. If OCIC= 0, ASDU 101 is not sent. The parameter can be defined for each of the stations.	-	0
OIC	Order of IC	Balanced mode: Order of sending of ASDU 100 [Interrogation Command] when initializing the connection. If OIC<OCIC, then ASDU 100 is sent before ASDU 101. If OIC= 0, ASDU 100 is not sent. The parameter can be defined for each of the stations.	-	0
PW	Pessimistic Write	Defines the evaluation of writing success in case of a connection of more than one client. If PW=0, writing a value is considered to be successful if at least one client confirms it (confirmation method is defined by the CMDC parameter). If PW=1, writing must be confirmed by all connected clients. If at least one client doesn't confirm it (e.g. connection failure occurs or the confirmation is negative), writing is considered to be unsuccessful.	-	0

SSN	Send sequence number	The initial *Send sequence number* after the TCP connection is established. According to the standard, having established the connection the *Send sequence number* is set to 0, other than zero could be appropriate e.g. for testing.	-	0
SKO	Standby Keep Open	If True, after changing the status of the D2000 Server process (the D2000 KOM process is connected to) from Hot to Standby state (in a redundant system), connections with clients will not be closed, and listening for new clients will not be aborted.	-	False
SSCF3	Standby Set Control Field	If True, after changing the status of the D2000 Server process (the D2000 KOM process is connected to) from Hot to Standby state (in a redundant system), the lowest bit of the 3rd Control Field byte of information APDUs (APDU containing data or commands) will be set to 1 instead of the standard value of 0. The behavior does not strictly follow the standard and we recommend using the *Standby Set Test Bit* parameter instead of this parameter if it is possible.	-	False
SSTB	Standby Set Test Bit	If True, after changing the status of the D2000 Server process (the D2000 KOM process is connected to) from Hot to Standby state (in a redundant system), the Test bit will be set in *Cause Of Transmission*.	-	False
SWV	Standby Write Values	If True, after changing the status of the D2000 Server process (the D2000 KOM process is connected to) from Hot to Standby state (in a redundant system), the server will send new values to clients.	-	False
W	W	The number of received I-frames, after which the D2000 KOM process sends an S-frame confirmation. According to the standard, the default value is 8. The relation W < K must be true, the standard recommends W = 2/3 * K.	-	8
WT1	Wait Timeout T1	Timeout for receiving the confirmation of a sent I-frame (either confirmation within the I-frame or the S-frame itself) or a U-frame. If the D2000 KOM process does not receive the confirmation within *Wait Timeout T1* time, it closes the TCP connection. According to the standard, the *Wait Timeout T1* default value is 15000 ms	ms	15 000
WT2	Wait Timeout T2	Timeout for sending the confirmation of a received I-frame. *Wait Timeout T2* < *Wait Timeout T1*. If another I-frame (which confirms the received I-frame) is not sent within *Wait Timeout T2* time since the I-frame was received, the D2000 KOM process sends an S-frame confirming the received I-frame to the partner. According to the standard, the *Wait Timeout T2* default value is 10000 ms.	ms	10 000
WT3	Wait Timeout T3	Timeout for sending test frames (TEST ACT U-frame). If no data are sent in any direction for a long time, a TEST ACT U-frame will be sent after the expiration of the *Wait Timeout T3* time by the D2000 KOM process, and a TEST CON U-frame is expected (within *Wait Timeout T1* time after sending). If the *Wait Timeout T3* on the partner side is set to a lower value, it sends the test frames, and the D2000 KOM process replies to them. According to the standard, the *Wait Timeout T2* default value is 20000 ms. Setting the value to 0 disables sending test frames.	ms	20 000
WTN	Wait Timeout No answer	Balanced mode: Timeout for receiving the confirmation of a sent value in a control direction (ASDUs 45 - 64). Receiving e.g. S-frame with RSN (Receive Sequence Number) confirming, that the other party received the previous I-frame doesn't mean, that the I-frame was processed. Within the *Wait Timeout No answer* time interval, the D2000 KOM process waits for receiving the response (e.g. after sending ASDU with TypeIdentificator=45 [Single Command] with CauseOfTransmission=6 [Activation], the receiving of Single Command with CauseOfTransmission=7 [Activation Confirmation] is expected. After the expiration of the *Wait Timeout Tn*, the D2000 KOM process closes the TCP connection.	ms	60 000

A string containing the protocol parameters is being defined as follows:

```
Keyword=value;Keyword=value; ...
```

Example:

```
WTn=10000;WT3=25000;OCIC=0;
```

If a keyword with an invalid value in the initialization string is found, a corresponding default value according to the Table 3 will be used. Defined parameters, except for OIC, OCIC and FST are valid for the **entire** line - i.e. it is enough to define them for one station on the line.

I/O tag configuration

Possible I/O tag types: **Ai, Ao, Ci, Co, Di, Dout, Qi**

- I/O tag address is mapped to the *Information object address*, i.e. it has 3 bytes and must within the range of 0..16777215. It can be specified as a decimal number or as a hexadecimal number with a hash at the beginning (e.g. #0A).
  The I/O tag with an address starting with *%IGNORE* will be ignored.
- Input tags must be of particular types (Ai, Ci, Di, Qi) for received ASDU, see Table 1.
- For a particular type of output tag (Ao, Dout, Co), it is necessary to set an ASDU type, that has to be used, see Table 2 and also Table 1 in the balanced mode.
- Archive for providing old values: if the client requires archive values using ASDU 250, the server sends:
  1. the values of the historical value specified by this input entry field,
  2. if the input entry field is not filled, then the values of the historical value that archives the I/O tag,

3. if the specified historical value does not exist, then the values of the I/O tag that archives the control object of the specified I/O tag,
4. if the control object does not exist (or the archive is not available), the server returns an error.

Specification of a historical value allows configuring e.g. sending 10-minutes averages instead of sending all changes of given I/O tag.

- If the Destination Column is configured, then the values received from the address configured at the I/O tag and above are stored in the corresponding items (e.g. objects with addresses 10, 11, 12 ... according to the number of rows of the destination structure).

Browse

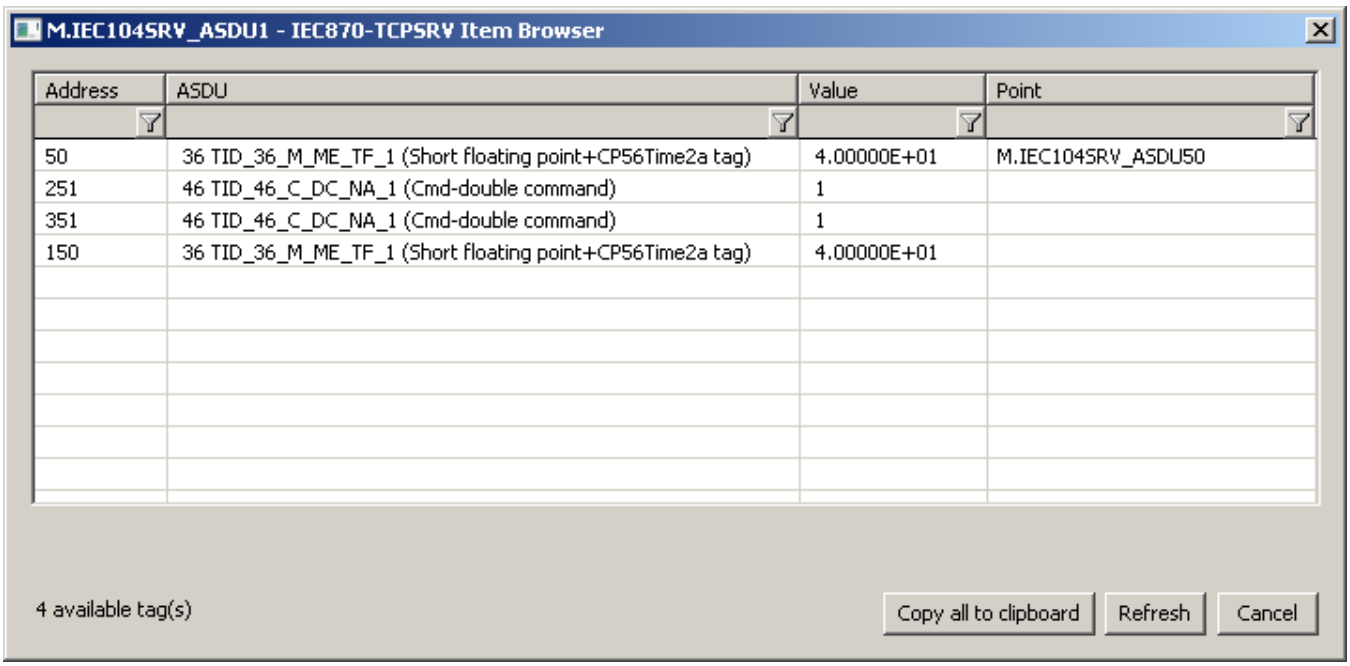
For the I/O tags, it is possible to discover the list of objects, as long as the KOM process is running and communication with a station is established. Clicking the *Browse* button opens the *IEC870-TCPSRV Item Browser* window and displays a list of objects that have been read so far. The object list is created dynamically as a result of received messages.

The list of objects is dynamic, i.e. when a new value arrives in the KOM process, it is updated. Filtering in individual columns is also supported, asterisks can be used in the mask (e.g. *Short*).

Double-clicking on a particular line will cause the A*ddress* parameter to be inserted into the configuration of the I/O tag from which the *IEC870-TCPSRV Ite m Browser* window was opened.

The Refresh button clears the list of values in both the CNF and the KOM process.

The *Value* column contains the received value.



Tell commands

Command	Syntax	Description
STWATCH	STWATCH StationName	Tell command sends Interrogation Command and/or Counter Interrogation Command to the station (based on station parameters).

Literature

Blog

You can read a blog about the IEC 870-5-104 protocol:

- Communication – protocol IEC 104

Document revisions

- Ver. 1.0 – February 5th, 2004
- Ver. 1.1 – December 1st, 2004: extension - support of balanced mode
- Ver. 1.2 – June 15th, 2020: browsing support
- Ver. 1.3 – November 16th, 2023 (support for the Destination Column)

Related pages:

Communication protocols