Action.NET – IEC-60870-5-104
Master Communication Protocol

Summary

1. GENERAL INFORMATION

1.1 Summary

Communication Driver Name: IEC8705104

Current Version: 2016.2

Implementation DLL: T.ProtocolDriver.IEC8705104.dll

Protocol: IEC-60870-5-104 Master standard protocol

Interface: TCP/IP

> **Description**: The Action.Net IEC870504 protocol driver implements comunication with IEDs (Intelligent Eletronic Devices), RTUs (Remote Terminal Units) and IO devices compatible with this protocol, playing role as master station.

IEDs types supported: Any IED compatible with IEC-60870-5-104.

Communication block size: Maximum 253bytes;

Protocol Options: Counters for sending protocol control messages.

Multi-threading: User defined, five threads per node by default.

Max number of nodes: User defined

PC Hardware requirements: Standard PC Ethernet interface board;

PC Software requirements: Action.NET system.

1.2 Supported Object Data (ASDUs)

The protocol uses the same ASDUs defined for IEC-60870-5-101 well as the same object data types. The major difference is be targeted only to network uses, with TCP/IP as the transport layer, instead of serial communication.

M_SP_NA: 1 - Single-point information ;

M_DP_NA: 3 - Double-point information ;

M_ST_NA: 5 - Step position;

M_BO_NA: 7 - Bitstring with 32 bits ;

M_ME_NA: 9 - Measured value, normalized ;

M_ME_NB: 11 - Measured value, scaled value ;

M_ME_NC: 13 - Measured value Float;

M_IT_NA: 15 - Integrated totals ;

C_SC_NA: 45 - Single command ;

C_DC_NA: 46 - Double command ;

C_RC_NA: 47 - Regulating step command ;

C_SE_NA: 48 - Set point command, normalized value ;

C_SE_NC: 50 - Set point command, 32 bits floating point ;

C_BO_NA: 51 – Write 32 bit Bitstring.

It also uses all the 56 bit timestamp variant of the above ASDUs. The code above is used when enrolling points, but if the slave IED sends variants with date and timestamp, the measures and states received will be placed on the quality and timestamp attributes of the correspondent points.

1.3 General Operation

The IEC-60870-5-104 protocol is implemented in Master mode in which it communicates with IEDs that implement the protocol IEC-870-5-104 slave. Various parameterizations are available to accommodate different profiles of protocol implementations.

Master has the following operating sequence:

On start or communication failure

- Send "Start of data transmission – STARTDT";
- Send schedule, if sample time different from zero;
- Do sample readings, according to preset sample times (all classes);

It does an infinity loop:

- Waits for unsolicited messages containing object data that have changed.
- For each "w" (configurable parameter) received messages, or after a certain time without receiving messages, will be sent an "acknowledgment" message with the sequence number of the last information message received.
- Periodically, according with a preset timeout parameter, send "Test Frames" massages in case of none message received during this time.
- On receiving a command request targeted to any remote IED, sends it, according to command parameter details;

2. CHANNEL SETTINGS

2.1 Protocol Options

t0 - Timeout of Connection establishment(s) – Maximum acceptable time, in seconds, for a TCP/IP connection attempt with a remote IED. After this time, the driver close connection and attempt another connection. Values from 1 to 255 are allowed.

t1 - Timeout of send or test APDUs(s) – Maximum waiting time, in seconds, for sending a regular APDU or testing APDU after START DT confirmation received. Values from 1 to 255 are allowed.

t2 - Timeout for ack in case of no data(s) – Maximum waiting time, in seconds, for a pending acknowledgement before sending an acknowledgement for the last received message. Will be sent a message with the sequence number of last received. Values from 1 to 255 are allowed. The t2 time must be less than t1.

t3 - Timeout for send test frames(s) – Maximum waiting time, in seconds, for the arrival of any information (in case of a TCP-IP connection is already established) before sending a TEST-FR. Values allowed are from 1 to 255.

Password for commands: To increase the security of sending commands, normally initiated only by a change in the state of a tag, it is possible here to specify a password of up to nine digits. The communication module will verify this password against the current value, in moment of receiving the command, of *EstimatedValue* attribute tag involved in command. Therefore, in the operation of sending a command through a window, script, etc. this number must be loaded in this attribute. The communication module, after executing the command, changes the value of *EstimatedValue* to ZERO. This verification does not occurs if leaving this option with zero,

Logging Level – You can choose from this list the logging mode created by the communication module.

Logging level	Debug	All messages are registered in the LOG.
	Info	Only Info, Warning and Error messages are logged in the LOG.
	Warning	Only Warning and Error messages are registered in the LOG.
	Error	Only Error messages are registered in the LOG.

The figure below shows the filling of these fields on the channel:

IEC8705104	ProtocolOptions
t0 - Timeout of Connection establishment(s)	30
t1 - Timeout of send or test APDUs(s)	15
t2 - Timeout for ack in case of no Data(s)	10
t3 - Timeout for send test frames(s)	20
Password for commands	3985
Logging Level	Info

2.2 Settings

TCP/IP channels:

- NodeConnections: Defines the maximum number of parallel requests that could be sent to each node (asynchronous communication).

00055.06

3. NODES SETTINGS

Each node is a server station (IED). User may set a single station per channel.

3.1 TCP/IP Communication

IP Address – It must be specified the IED IP address.

Port – Port number to be used. The standard defines port **2404,** by default. User can use custom port numbers.

3.2 Parameters

CommonAddress- Application Layer address

Date sample time – Period of time, in milliseconds, between two consecutive submissions of Date and Time for remote IED synchronization, if necessary. Zero is used to indicate that there is no need for synchronization. Note that the master should not synchronize IEDs synchronized by GPS.

General Interrogation (GI) sample time – Period of time, in milliseconds, between two consecutive submissions of general interrogation requests to an IED. The IED responds by sending blocks of information, as many as are required to send all points.

w – Send ack after received w IFormatAPDUs – Number of information messages received spontaneously before sending an "acknowledgment" with the sequence number of last message received. The allowed values are between 1 and 32767.

k – Messages received to send state variable – Maximum allowed number of pending acknowledgements before slave stops sending new messages. It is recommended that w is at maximum, two thirds of the k value. Values between 1 and 32767 are allowed.

Clock Adjust – Can be set as "True" to adjust the clock on this server compute or "False" to make no adjustment. The module does adjustment changing the machine time to match the one that came as answer to a synchronization message sent. For this to be effective, the slave IED must answer with a time that comes, for example, from a GPS.

IED time bias from GMT - In Action.NET, internally, all timestamps are stored with GMT (UTC) dates. IEDs usually send these dates also in GMT and no adjust is required. The default for this option is Zero. If in the current deployment the IEDs send the timestamps in their local time, we must define in this field, the difference between this time and GMT time. For example in New York, the local time is 4 hours shorter than GMT. For this case, -4 should be specified in this table.

Tag for Comm status - In this field can be indicated the name of an existing tag in the project to receive indication of success / failure in communication from a functional point of view. When doing requests

the module waits a maximum of t2 seconds (defined in Protocol Options, above) to receive a response. In case of failure, the system places the value of this tag in ZERO. In case of success, the system places the value UM in this tag.

The figure below shows the filling of these fields for the main station:

IP	192.168.0.127
Port	2404
CommonAddress	1
Date sample time(ms)	15000
General sample time(ms)	60000
w - Send ack after received w IFormat APDUs	8
k - Messages received to send state variable	12
Clock adjust	False
IED time bias from GMT	0
Tag for comm status	TGIEC.COMMOK

Backup Station – The same communications settings made to an IED could be made to one backup workstation (alternative IED) if there is one in the facility.

4. POINTS SETTINGS

4.1 General

The points can be input or output. The input points, ie points that are acquired by the protocol have basically two main parameters: The point type and address. The output points are used for remote controls, and have an additional address parameter to specify an output operation. In a given IED, addresses are unique no matter what kind of the point.

4.2 Points Type

Action.Net master mode implements:

- Synchronizing remotes IEDs through date and time sending;

- General Interrogation request;

- Receiving unsolicited information frames due to the data changes in remote IED.

- Time tag 56 bits length;

- Digital point single or Double command;

- Select Before Operate Command;

- Point Value Quality analyzing (QDS);

The point types were implemented as their respective objects ASDUs defined in the standard (see list below).

M_SP_NA: 1 - Single-point information

Simple binary input point, assuming 0 or 1. The variants with "timetag" M_SP_TA (= 2) and M_SP_TB (= 30) are also considered in this type. In enrolment only this type is used.

M_DP_NA: 3 - Double-point information ;

Double input point, which can assume states 0 to 3, is usually used for signaling states of switches and circuit breakers. The variants with "timetag" M_DP_TA (= 4) and M_DP_TB (= 31) are also considered in this type. In enrolment only this type is used.

M_ST_NA: 5 - Step position;

Step value, ranges from -64 to +63, mainly used for transformer step position or other position information. The variants with "timetag" M_ST_TA (= 6) and M_ST_TB (= 32) are also considered in this type. In enrolment only this type is used.

M_BO_NA: 7 - Bitstring with 32 bits ;

Status information as a binary string of 32 bits. Action.Net makes no manipulation at all. The configuration is treated as a long number. The variants with "timetag" M_BO_TA (= 8) and M_BO_TB (= 33)) are also considered in this type.

M_ME_NA: 9 - Measured value, normalized ;

Standard Analog measurement using 16-bit signal. Value between -32768 and + 32767. It is calculated as a real number between 0 and 1 before being assigned to the tag in real time. Should be used "scalling"if it´s intended to reproduce the value in engineering units. The variants with "timetag" M_ME_TA (= 10) and M_ME_TD (= 34)) are also considered in this type. In enrrolment only this type is used.

M_ME_NB: 11 - Measured value, scaled value ;

Scalar Analog measurement used for transmission of analog quantities. Also 16-bit value between - 32768 and 32767. The variants with "timetag" M_ME_TB (= 12) and M_ME_TE (= 35) are also considered in this type.

M_ME_NC: 13 - Measured value short floating point;

Analog Measurement on fractional real number format, used for transmission of analog quantities. The measurements are 32-bit fields in the format IEEE STD 754, which implements floating-point numbers. The variants with "timetag" M_ME_TC (= 14) and M_ME_TF (= 36) are also considered in this type.

M_IT_NA: 15 - Integrated totals ;

Integer analog measurement signal. Measurements with 32-bit integer. The variants with "timetag" M_IT_TB (= 16) and M_ME_TC (= 37) are also considered in this type.

C_SC_NA: 45 - Single command ;

Simple command to point (1 bit). Details of the command can be selected by clicking in the button that is in the right side of the field. The number that is the command code resulting from the choice of details can also be entered directly. Each point will be staticly parameterized on the POINTS table, in a way that one point must be configured for opening and another for closing one bit switches.

C_DC_NA: 46 - Double command ;

Double command (2 bits). Details of the command can be selected by clicking the button in the rigth side of the field. Also can be entered directly the number that is the command code resulting from the choice of details. Each point will be staticly parameterized on the POINTS table, in a way that one point must be configured for opening and another for closing two bit switches.

C_RC_NA: 47 - Regulating step command ;

Command for setting step. Normally used to send pulses to step up and down switching transformers. Details of the command can be selected by clicking the button in the rigth side of the field. Also can be entered directly the number that is the command code resulting from the choice of details. Each point will be staticly parameterized on the POINTS table, in a way that one point must be configured to step up and another one to step down the position of the transformer step.

C_SE_NA: 48 - Set point command, normalized value ;

Used to send set points of 16-bit normalized for IEDs that support this type of command. The value to be sent is the one indicated by the "tag" whose address was sent in command.

C_SE_NC: 50 - Set point command, short floating point value ;

Used to send set points with IEEE STD 764 32-bit floating-point format for IEDs that support this type of command. The value to be sent is that indicated by the "tag" whose address was sent in command.

C_BO_NA: 51- Write Bitstring de 32 bits

Used to write a binary state information as a 32-bit string on the IED server. No manipulation whatsoever is made by the driver. The setting is treated as a long unsigned number. The value to be sent is the one contained in the "tag" whose address was sent in the command, at that moment. The tag type must be "long" or AnalogInt, which is a 32-bit integer.

CMDSIGN - Command Signaling

This is an internal type of Action.NET itself to allow configuration of match between output tag and input tag, used to signaling of a command. When choosing the CMDSIGN type, in the definition of the Address column, a different menu appears with the fields to define the necessary parameters.
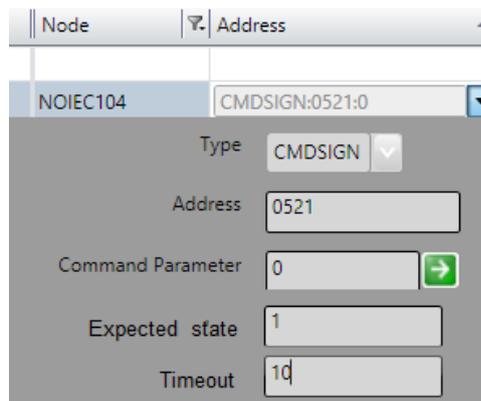
The following figure shows the setting in the POINTS table. The signaling comes in tag A2.DJ.DJ of type M_DP_NA. The two lines in yellow show definition of signaling of commands with the same address (0510) and control code (0 - Open and 1 - Close).

The protocol module uses this two lines to create a static list with all matches on the node. Their information does not create new points in real time.

Nothing else is required for setup. With this list the module will automatically call the transaction creation and verification methods.

We can use this feature of Command Signaling only for digital commands C_SC_NA and C_DC_NA and digital signals M_DP_NA and M_SP_NA.
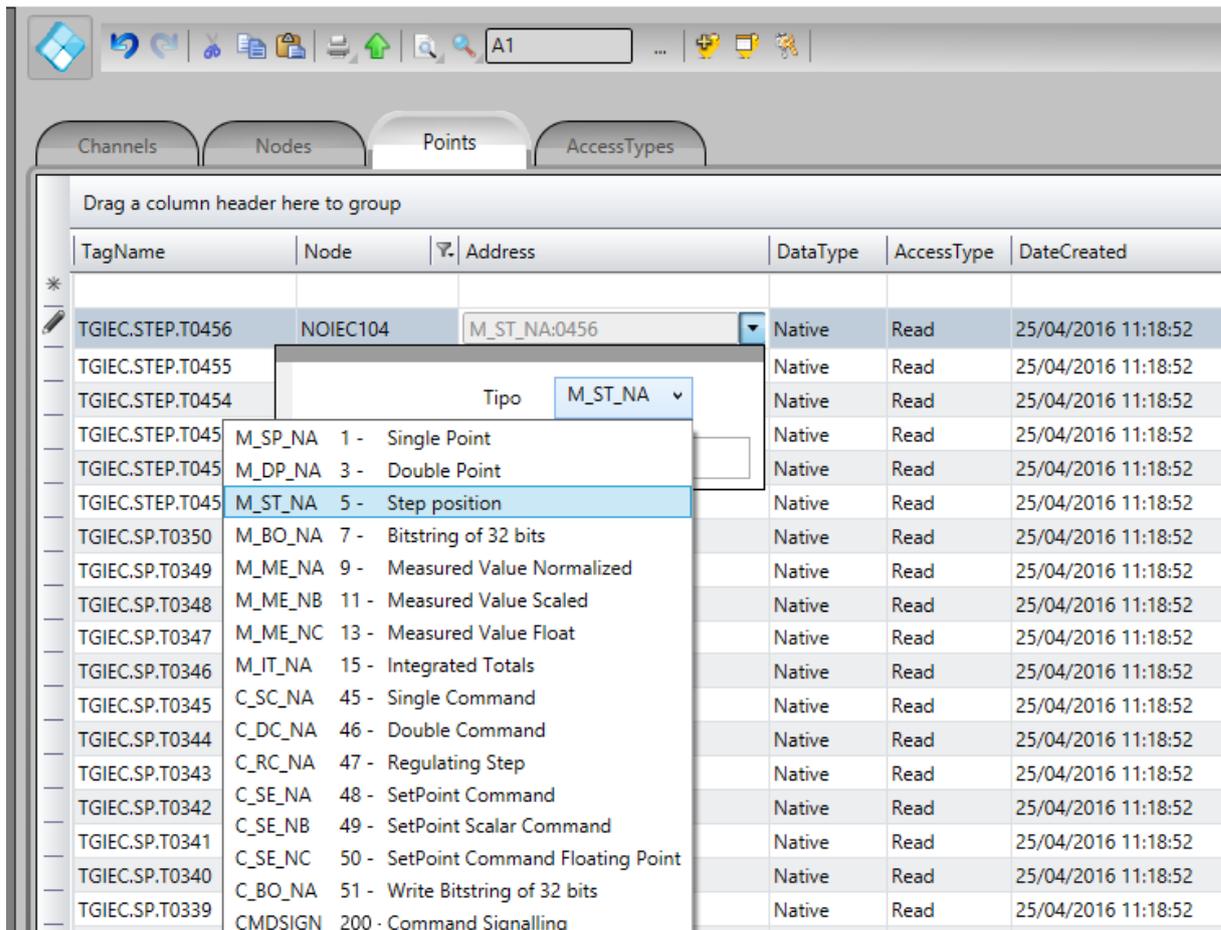
4.3 Point Address

The completion of point addresses is done in the engineering environment, in **Edit> Devices> Points.**

The **Address** field to fill in in the point registration is what the standard calls the **"Information Object Address"**. This is a 3-byte number, for a given IED (node) is not repeated, the address being assigned by the IED manufacturer.

As the figure below, a click on the row of the address column opens a window to select the type and address of the point. A click on the type opens a window with all types of points supported:

To select **Type:**

4.4 Command Parameter

The command parameter is a one-byte code, which details what and how the server IED should execute the command.. In this implementation, as the user registers a point typed as command output, this field shows up to receive this code. If the user knowns code may just type it in the field. If not, click on the button to the right of field for displaying the window with the actions and details available.

The codes generated by choosing the items in the window parameter setting command is formed by calculating the sum of two parts (A and B), first part indicate action, and the second details of the transaction, as defined below:

For Single Command C_SC_NA:

1 = Turn off	(A)
2 = Turn on	(A)
4 = Short Pulse	(B)
8 = Long Pulse	(B)
12 = Persistent Signal	(B)

For Double Command C_DC_NA:

1 = Turn off	(A)

2 = Turn on   (A)

4 = Short Pulse   (B)

8 = Long Pulse   (B)

12 = Persistent Signal   (B)

For Voltage Regulation C_RC_NA:

1 = Down   (A)

2 = Up   (A)

4 = Short Pulse   (B)

8 = Long Pulse   (B)

12 = Persistent Signal   (B)

The remaining options are the **Select** type command - just select the device to be controlled; or the **Execute** type command - send the proper action command. In case of choosing the **Select** command, we must add 128 to the code so far obtained, by the sum of the parts A and B.

Example: code = 9, in a simple command means *Long Pulse* for *Turn on* the remote device.

In order to set the Action.NET with output parameters, follow the procedure below:

(1) One click over the right border of the address shows three command parameters, in the command tab:

      a. Type

      b. Address

      c. Command parameter

And the command options:

      a. Trip

      b. Close

      c. Execute

      d. Select

(2) Select the desired options and when pressing the left arrow (), the binary value corresponding to the selection will be loaded in the command parameter:

(3) If detailing the type of signal to be sent is necessary, before pressing the left arrow click on details and, as in the figure below, select the type of the output signal:

4.5 Access Type

Since it is a communication module in master mode (server), there is need for a few specific characteristics in order to parameterize the **Access Type** field on the **Points** table:

For points with reading types:

M_SP_NA: 1 - Single-point information ;

M_DP_NA: 3 - Double-point information ;

M_ST_NA: 5 - Step position;

M_BO_NA: 7 - Bitstring with 32 bits ;

M_ME_NA: 9 - Measured value, normalized ;

M_ME_NB: 11 - Measured value, scaled value ;

M_ME_NC: 13 - Measured value Float;

M_IT_NA: 15 - Integrated totals ;

The Access Type must be defined with:

ReadOnStartup = On (Attention, it is important to do a general reading when starting);

ReadPooling = Always;

ReadPoolongRate: 500 mili

WriteEvent = Changed;

AccepUnsolictited = On;

For points with command types:

C_SC_NA: 45 - Single command ;

C_DC_NA: 46 - Double command ;

C_RC_NA: 47 - Regulating step command ;

C_SE_NA: 48 - Set point command, normalized value ;

C_SE_NC: 50 - Set point command, 32 bits floating point ;

C_BO_NA: 51- Write Bitstring de 32 bits

The Access Type must be defined with:

ReadPooling = Never;

WriteEnable = On

WriteEvent = Changed;