IEC-60870-5-101 Master

The SCADA IEC870-5-101 driver implements communication with IEDs (Intelligent Electronic Devices), RTUs (Remote Terminal Units), and IO devices compatible with this protocol. This allows it to act as a master station.

Summary Information

Communication Driver Name: IEC8705101

Current Version: 2014.2

Implementation DLL: T.ProtocolDriver.IEC8705101.dll

Protocol: IEC-870-5-101 Master standard protocol

Interface: TCP/IP or Serial

IEDs types supported: Any IED compatible with IEC-60870-5-101

Communication block size: Maximum 250 bytes, FT 1.2 format

Protocol Options: Number of octets used by a link layer, application layer, data objects, and transmission cause

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

Max number of nodes: User defined

PC Hardware requirements: Standard PC Ethernet interface board, RS485, or RS232 port

Supported Objects (ASDUs)

- 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
- M_EP_TA: 17 - Equipment protection with Time
- 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

In SCADA, each Object Data type has three variants, one without a timestamp and two that have a timestamp (23 bits and 56 bits). By default, users do not have to specify the variants that will be used. This is processed in a transparent way.

General Operation

The IEC-60870-5-101 protocol is implemented in master mode where it communicates with IEDs that implement the IEC-870-5-101 protocol slave. The frame used for the data exchange is FT 1.2, non-balanced (slave does not send unsolicited data). There is a large range of settings options that are used to match different usage profiles.

Master has the following operating sequence:

On start or Communication Failure

- Start initialization procedures on the Slave(s)
- Send the schedule if the time is different from zero
- Do cycle readings according to preset sample times (all classes)

Infinity Loop

- If a request to send a command is received, send the command according to the parameter details
- If the sampling time of the group has expired, do the reading
- If the periodic time for sending a schedule has expired and if the time value is different from zero, send the schedule
- On receiving a data request: if there is an indication for new events, do the event's request (class 1)
- On receiving an error frame or timed out request, restart the communication procedure (go to the first step)

Channel Configuration

Protocol Options

CommonAddress Num Octets – The number of bytes used for the address of the application layer in the targeted slave station. It can be 1 or 2 bytes

LinkAddress Num Octets – The number of bytes used for the address of the link layer in the targeted slave station. It can be 1 or 2 bytes

ObjectAddress Num Octets – The number of bytes used for the address of the data object. It can be 1, 2, or 3 bytes

CauseOfTransmission Num Octets – The number of bytes used to show the cause of the data transmission. It can be 1 or 2 bytes

Settings

Serial:

- **DataBits**: 8
- **StopBits:** 1 or 2
- Extra port settings of the remote slave IED

TCP/IP channels:

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

Node Configuration

Each node is a Server station (IED). Many nodes can be associated to each channel

TCP/IP Communication:

- **IP Address =** The IED's IP address
- **Port** = The Port number

Serial:

- The settings are displayed in the Settings section above

Common Parameters

Common Address = The address of the IED's application layer

LinkAddress = The address of the IED's link layer

Synchronism sample time = A period of time, in milliseconds, between two consecutive submissions of Date/Time and remote IEDs. Zero is used to indicate that there is no need for synchronization. Note that IEDs that are synchronized by GPS should not be synchronized by the master

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

Status sample time = A length of time, in milliseconds, between two consecutive requests for changes that occur in class 1 and class 2 points. The IED responds by sending blocks of information. It sends as many as are needed to show the changes occurred. Normally, this period should be set to a short value. For example,1000 milliseconds

General Counters Sample Time = A general timer for counter requests, in milliseconds. The IED responds with as many information blocks as necessary

Clock Adjust = This should be enabled if the Master Station needs to be synchronized by remote/slave IED date/hour. This is useful if the remote/slave IED is synchronized by GPS

Backup Station =The same settings made to the main station can be made to one backup workstation (an alternative IED) if there is one in the facility

---

Point Configuration

Points can be input or output. Input points are acquired by the protocol and have basically two main parameters: point type and address. Output points are used for remote controls and have an additional parameter used to specify the type of output operation. In a given IED, point addresses are unique.

Grouping

IEC870-5-101 provides a groups of Points feature. In this implementation, they are not considered. Instead, there is a general read considering all points, and a general counters read considering all timers.

This implementation supports two standard classes:

- Class 1: Priority, captured from event occurrences, always with timestamp (even ASDUs)
- Class 2: Non priority, captured from cycle readings, without timestamp (odd ASDUs)

Note that the concepts of class and point differ from each other. Thus, a given point, that has a changed state, could generate a class 1 even that should be processed before the next class 2 reading. To avoid inconsistencies, only class 2 cyclical readings of point can trigger a change in point status on SCADA. Class 1 events solely generate SCADA events.

Point Types

The Master communication mode implements:

- Single digital or double digital readings
- Analog point readings
- Counter readings
- 24 or 56-bit time tags
- Single digital or double digital commands
- Link layer address length variation, IED address length variation and point address length variation
- Select before operate command
- Point quality analysis (QDS)
- Zero and one sequence message analysis (SQ)

The point types were implemented according to the following:

M_SP_NA: 1 - **Single-point information**

- Simple binary input point, assuming 0 or 1. Variants with “timetag” M_SP_TA (=2) and M_SP_TB (= 30) are also considered in this type.

M_DP_NA: 3 - Double-point information

- Double input point can assume states 0 to 3 and is usually used for signaling the state of switches and circuit breakers. Variants with “timetag” M_DP_TA (= 4) and M_DP_TB (= 31) are also considered in this type.

M_ST_NA: 5 - Step position

- Step value, ranging from -64 to +63, is mainly used for a transformer step position or other position information. Variants with “timetag” M_ST_TA (= 6) and M_ST_TB (= 32) are also considered in this type.

M_BO_NA: 7 - Bitstring with 32 bits

- Status information as a binary string of 32 bits. SCADA makes no manipulation at all. The configuration is treated as a long number. 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 a 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. Scaling should be used if the value will be reproduced in engineering units. Variants with “timetag” M_ME_TA (= 10) and M_ME_TD (= 34)) are also considered in this type.

M_ME_NB: 11 - Measured value, scaled value

- Scalar analog measurement used for the transmission of analog quantities. Also, a 16-bit value between -32768 and 32767. 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 in a fractional real number format and is used for the transmission of analog quantities. The measurements are 32-bit fields in the format of IEEE STD 754, which implements floating-point numbers. 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 a 32-bit integer. Variants with “timetag” M_IT_TB (= 16) and M_ME_TC (= 37) are also considered in this type.

M_EP_TA: 17 - Equipment protection with Time

- Change of state event information with timestamp. It uses a byte for quality, with status information in the two least significant bits. This type uses 24-bit timestamps.

C_SC_NA: 45 - Single command

- Simple command to point (1 bit). Details of the command can be selected by clicking the button that is on the right side of the field. It is also possible to enter the number of the command code that results from the choice of details. 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 on the right side of the field. It is also possible to enter the number of the command code that results from the choice of details. One point must be configured for opening and another for closing two-bit switches.

C_RC_NA: 47 - Regulating step command

- Command for setting a step. Normally used to send pulses to the steps that switch transformers up and down. Details of the command can be selected by clicking the button on the right side of the field. It is also possible to enter the number of the command code that results from the choice of details. One point must be configured to step up and another one to step down the position of the transformer.

C_SE_NA: 48 - Set point command, normalized value

- For sending set points of 16 bits normalized to IEDs that support this type of command. The value that will be sent is indicated by the address of the SCADA tag that was sent in the command.

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

- For sending set points of 32 bits in an IEEE STD 764 floating-point format to IEDs that support this type of command. The value that will be sent is indicated by the address of the SCADA tag that was sent in the command.

Point Address

The “Information Object Address” is the address field that is filled in when registering a point. It is a number that is 2 or 3 bytes long, as chosen in the “Protocol Options.” Two bytes are most commonly used for this number, so the range is from 0 to 65535. It must be unique for the given IED. These addresses are set by the IED manufacturer.

Command Parameter

The command parameter is used as a code of one byte, which details the command type to be executed into a remote IED. When the user registers a point typed as command output, this field appears, and the user can fill it in. If the code is already known, the user can just type it into the field. If not, click on the button on the right side of this field to display a window with the available actions and details.

The code generated by choosing the items in the parameter setting command window is obtained by calculating the sum of two parts (A and B). The first part indicates the action, and the second part indicated the 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 Command (select the device that will be controlled) or the Execute Command (send the proper action command). The select command option adds 128 to the code obtained from the sum of the A and B parts.

Example: Code = 9 in a simple command means Long Pulse to Turn on the remote device.

Access Type

In Slave mode, the Access Type field should be set as indicated below:

For reading points:

- 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
- M_EP_TA: 17 - Equipment protection with Time

The Access Type must be set as:

- ReadOnStartup= On
- ReadPooling= Always
- ReadPoolongRate: 500 mili
- WriteEvent= Changed
- AccepUnsolictited = On

For command points:

- 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

The Access Type must be set as:

- ReadPooling = Never
- WriteEnable = On
- WriteEvent= Changed