IEC-60870-5-101
Master Communication Protocol

Table of Contents

1. GENERAL INFORMATION

1.1 Summary

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
Description: The SCADA IEC870-5-101 protocol driver implements comunication with IEDs (Intelligent Eletronic Devices), RTUs (Remote Terminal Units) and IO devices compatible with this protocol, acting as a master station.
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 octects used by link layer and 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

1.2 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;

On SCADA, each type of Object Data listed above has three variants: the first one without timestamp and the other two with timestamp (24 bits and 56 bits). On SCADA, by default, users do not have to specify the variants intended to be used. This is processed in a transparent way.

1.3 General Operation

Protocol IEC-60870-5-101 is implemented in master mode, in which it communicates with IEDs that implement protocol IEC-870-5-101 slave. The frame used for data exchange is FT 1.2, non-balanced (slave doesn´t send unsolicited data). There is a large range of settings options for matching different usage profiles.

Master has the following operating sequence:

On start or communication failure
- As first step, start initialization procedures on the Slave(s);
- Send schedule, if time different from zero;
- Do cycle readings according to preset sample times (all classes);

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

2.   CHANNEL SETTINGS

2.1   Protocol Options

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

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

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

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

2.2   Settings

Serial:

DataBits: 8
StopBits: 1 or 2
Extra port settings according to remote slave IED.

TCP/IP channels:
- NodeConnections: Defines the maximum number of parallel requests that can be sent to each node (asynchronous communication).

3.   NODES SETTINGS

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

3.1   TCP/IP Communication

IP Address – IED's IP address
Port – Port Number

3.2   Serial Communication

The settings are those displayed in the Channel Settings section above.

3.3   Common Parameters

Common Address – IED application layer address

LinkAddress – IED link layer address

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

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.

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

General Counters Sample Time – General timer for counter request, in milliseconds. IED responds with information blocks, as many as necessary.

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

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

4.   POINT SETTINGS

4.1 General

Points can be input or output. The input points i.e. points that are acquired by the protocol 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.

4.2 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 classes listed in the standard:

● 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, if its state has changed, could generate a class 1 event that should be processed before the next class 2 reading. By design, only class 2 cyclical readings of point can trigger a change in point status on SCADA, to avoid inconsistencies. Class 1 events solely generate SCADA events.

4.3 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 as their respective objects 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.
M_DP_NA: 3 - Double-point information
Double input point which can assume states 0 to 3, and 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.

M_ST_NA: 5 - Step position
Step value, ranging 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.

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. 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 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 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.

M_ME_NB: 11 - Measured value, scaled value
Scalar analog measurement used for transmission of analog quantities. Also a 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 in a 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 a 32-bit integer. The 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´s also possible to enter the number that is the command code resulting from the choice of details directly. 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´s also possible to enter the number that is the command code resulting from the choice of details directly. 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 switching transformers up and down. Details of the command can be selected by clicking the button on the right side of the field. It´s also possible to enter the number that is the command code resulting from the choice of details directly. 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 to be sent is that indicated by the SCADA tag whose address 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 to be sent is that indicated by the SCADA tag whose address was sent in the command.

4.4   Point Address

The Address field to be filled in when registering a point is what the standard calls "Information Object Address." It is a number 2 or 3 bytes long, as chosen in the "Protocol Options." In the most common usage two bytes are used for this number, so the range is from 0 to 65535. For a given IED it must be unique. These addresses are set by the IED manufacturer.

4.5   Command Parameter

The command parameter is implemented as a code of one byte, which details the command type to be executed into a remote IED. In this implementation, as the user registers a point typed as command output, this field shows up to be filled in by the user. If the code is already known, the user can just type it into this field. If not, click on the button on the right side of this field for displaying a window with the actions and details available.

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), where the first part indicates the action, and the second 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 - just select the device to 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 parts A and B.

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

4.6   Access Type

Acting on 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;