

“Best of” the IEC 60870-5 User Group Maillist Archive

This file contains a collection of the most commonly requested information posted to the IEC 60870-5 User Group Maillist. The advantage of using an Adobe PDF file for the maillist archive is that it can be viewed online or downloaded for offline reading.

The bookmarks in this document will enable quick navigation through the following discussion topics. A string search can be done using the standard Windows key sequence (Ctrl-F).

The file is organized with bookmarks in the left window to track message threads. All web links are still active, even when viewing the downloaded document.

Click on a bookmark in the left window to view the corresponding message in the right window. Use the scroll bar on the right window to see additional pages. When reading several messages sequentially, leave mouse cursor on bookmarks in left hand column to mark you position in the list of messages to read. The window divider may be dragged to show more of either pane.

You may wish to save a copy of this file to your computer for faster access in the future. To do this in an Adobe file, click on the "diskette" on the small Adobe toolbar at the top of the document (and not the standard IE/Netscape File, Save As function), then choose the directory where you would like to save the file.

Please feel free to send comments or suggestions for this document to me at ehall@tmw-usa.com.

Links in this document:

[Data frame "8,N,1" on IEC 60870-5-101](#)

[Assignment of information object addresses](#)

[Questions on 870-5-101 Balanced/Unbalanced modes](#)

[IEEE Std 754](#)

[Difference between Modbus and IEC 870-5](#)

[IEC870-5-101 vs. 103](#)

[Where to purchase IEC Documents](#)

-----Original Message-----

From: West, Andrew C

Sent: Tuesday, March 29, 2005 2:23 AM

To: iec60870-5@trianglemicroworks.com

Subject: RE: [Iec60870-5] Basics 101 & 103 protocol

Maruti Aswale <maruti.aswale@softdel.com> asks:

> May I get some basic brief on 101 & 103 protocol, from end user's
> point of view? viz. functionality, data points, etc.
> I ve worked on Modbus protocol, so u may compare with Modbus while
> explaining.

This is a very open-ended question.

Each protocol has a specific purpose:

Modbus is a DCS protocol that reports the state of a set of data points each time that data is scanned. It does not report changes on those points that occur between scans. Its purpose is to report the "current state" of a system. Modbus has a "general" data structure of boolean and integer values that can be interpreted in any way that the system wishes.

IEC 60870-5-101 is a SCADA protocol specifically intended for electric power applications. It reports changes in state of the monitored data points and can report time-stamps for these changes. It is able to prioritize the data reporting in order to send high priority data more quickly. It includes some power-system specific data types for monitoring some particular power devices (e.g. transformer tap positions) and has specific control types to ensure that only the correct output is changed when a command is issued. The protocol includes a concept of a current state for most data points but generally only reports the changes to those points. The data is strongly typed: each data type is expected to be interpreted in the specific way it is defined in the standard. It is not generally acceptable to reinterpret values as a generic binary data value that can be interpreted in any way the user chooses.

IEC 60870-5-103 is somewhat similar to -101 except that it includes specific data types for modeling power system protection devices. These devices have the characteristic that some of the data they report will only relate to some specific types of power system event (such as switching a circuit breaker to avoid an overload) and when these events occur they report a set of data values measured in association with that event. Because of this, these devices report some data as having a state or a change of state (as -101 does) and some data is reported only when one of these monitored events occur and has no "value" or "does not exist" at other times. This protocol has specific data types that relate to characteristics of the systems that they monitor such as the duration of fault conditions, etc.

The IEC protocols have a layered architecture. Some data link control messages act as proxies for application layer messages (e.g. poll requests).

A thorough knowledge of Modbus is of limited use in understanding the detail of the IEC protocols because they have relatively little in common.

The IEC standards must be read carefully because the descriptions for each feature are generally only presented once. The -101 and -103 companion standards refer to selections of features (described in other parts of the IEC 60870 series) that are used in these protocols.

This is a very brief summary of some of the features of these protocols.

Others may identify other features of the protocols that they find particularly interesting or that they think differentiate the protocols.

Andrew West

SCADA Communications Architect

From: Andrew West [mailto:andrew.west@ieee.org]
Sent: Wednesday, May 01, 2002 11:48 PM
To: iec870-5@trianglemicroworks.com
Subject: [iec870-5] RE: Data frame "8,N,1" on IEC 60870-5-101

M. Harisman asks:

> We would like to implement IEC 60870-5-101 protocol on existing Radio Data Network where it only support "8,N,1" async data/bit frame.

> As we understand from IEC 60870-5-101 documentation, the standard also regulated this data/bit frame to be "8,E,1".

> We have worked with SAT and Microsol XCell RTU, and we could not found a feature to change this "8,E,1" data/bit frame. It's look like they are strictly follow the standard as well. We assume that all of RTU Manufacturers also did the same for this protocol.

It is NECESSARY to support the parity bit in order to achieve a Hamming distance of 4 with frame format FT1.2. Without the parity bit, the Hamming distance is reduced to 2. With Hamming distance 2, the frame can meet Integrity Class 1. With the parity bit, the frame is capable of meeting Integrity Class 2.

Refer to IEC 60870-5-1 for an explanation of Data Integrity requirements, Integrity Classes and residual error probability. Refer also to IEC 60870-1-5 for a discussion of undetectable error patterns caused by different encoding of data. IEC 60870-5-101 Addendum 2 also includes an appendix discussing error detection in the frame format.

While the application data from IEC 60870-5-101 could be sent over a system that does not support parity, this would not provide the required level of data integrity. It would not comply with the standard and must not be described as being an IEC 60870-5-101 implementation.

Andrew West
Spokesperson, IEC TC57 WG03

Assignment of information object addresses

Question: I have a question regarding interpretation of the following text on page 25 of the IEC 60870-5-101 document: "The INFORMATION OBJECT IDENTIFIER consists only of the INFORMATION OBJECTADDRESS. In most cases the COMMON ADDRESS OF ASDUs together with the INFORMATION OBJECT ADDRESS distinguishes the complete SET OF INFORMATION ELEMENTs within a specific system.

The combination of both addresses shall be unambiguous per system. The TYPE IDENTIFICATION is not a part of a COMMON ADDRESS or an INFORMATION OBJECT ADDRESS."

Now referring to the IEC 60870-5-5 manual discussions of the command procedures in Figure 16 (page 73). Suppose a single command is performed and single point information is returned in the monitored direction. Can the single command ASDU and the single point information ASDU use the same information object address since they refer to the same data, or are they required to use a different information object address because they are different ASDU types?

Response (12 Oct 1998): Similar questions are well known! The pure rule says in general: Each specific information object has to have its own, unambiguous object address. This is advantageous in case of mixing both directions. I know, there are some users that define the same addresses in command and monitoring direction. I would not prefer and recommend this! Referring to the procedures shown in 5-5: The command procedure, which uses the specific command object addresses, is a separate procedure to the procedure that transmits the return information as single points. The command procedure has a different software source and a different destination as the return information. It makes sense to separate the addresses!.

Questions on 870-5-101 Balanced/Unbalanced modes.

Question (4 Nov 1998): Is it possible for the use of 101 in the balanced and unbalanced modes ('mixed') over the same physical link? For me, this would be similar to having 'two protocols 101' over the same link (physical).

Response (8 Nov 1998): This is definitely not possible due to the fact that the balanced mode is only defined for point-to-point connections. It is impossible in any case to mix it with a multipoint-line! Lines needed to be polled and this means use the pure unbalanced mode. Note: we are just speaking about the link layer only! Interrogations and requests of information points by the application layer functionality are possible, off course! The link layer procedures (defined in 870-5-2) are independent from the application layer procedures (defined in 870-5-5).

IEEE Std 754

Question (04 Aug 1999): The format of the floating point numbers according to IEC870-5-101 calculates as follows: $x = 0.\text{mantissa} * 2^{(\text{exponent} - 127)}$, which results e.g. in a smallest positive number of $2^{(-149)}$. Other documents suggest a calculation $x = 1.\text{mantissa} * 2^{(\text{exponent} - 127)}$. The smallest positive number would then be $1.0 * 2^{(-127)}$.

All the found documents refer to the standard IEEE Std 754. Does anybody know which format has to be used in 101 and which one is the real IEEE 754 standard?

Response: IEC 60870-5-101 floating point numbers use the IEEE Std 754 format. See also IEC 60870-5-4 Clause 6.5

The IEEE Std 754 allows for "normalized" (implied 1 to the left of the binary point) and "denormalized" values. The IEEE standard gives the full description, but basically:

*For exponent > 0, the value is $1.\text{fraction} * 2^{(\text{exponent}-127)}$*

*For exponent = 0, the value is $0.\text{fraction} * 2^{-126}$*

*The smallest IEEE 754 short floating point number is (binary) $0.000000000000000000000001 * 2^{-126} = 2^{-149} = 1.4 * 10^{-45}$*

Difference between Modbus and IEC 870-5

Question (4 Aug 1999): Tell me how our protocol iec/iso870-5 is different that of MODBUS

Response (5 Aug 1999): Here follows some differences of Modbus and IEC:

While modbus is "industry oriented", IEC is "electrical utility" oriented. Sure you can control a substation using both protocols, when you think that you need only to receive BI, AI and send BO (and AO sometimes). But, in that way, you would need a lot of work, on the application side, in order to deliver the most common demands of the electrical applications . For example, I'll tell you some:

- Select-before execute: When you want to operate a breaker, for example, you send a message selecting the equipment. If there is any problem (equipment not ready,

interlock, etc), you receive a message telling that it is not possible to make the maneuver. If everything is ok, you receive an activation confirmation, and you can send the execute command. This brings safety to your system.

- Time-Stamp on events: I think that the greatest problem with Modbus for this application is that you cannot send time stamped events. This means that, in your system, you will have only sequence of events (without time), but not event list with time. I've seen some Modbus applications that, when the master receives some binary input for event, it polls some registers and bring analog values for the time of occurrence. You can see that this is not a safe solution (and there is a lot of work on both sides).

- Status of indications and analog values: In IEC it's possible to put more information in a message than just the value. If you send an analog value, you can set some flags stating if that value is valid, if it's manually generated, and so on. In modbus, you send only the value, so the master doesn't if that value is valid or not. It means that you need to make some other mechanisms to handle that.

You can see that while modbus is "just a bunch of bits", IEC has much more functionality. If you choose modbus, you will have to implement master and slave in order to obtain that functionality. And since you have to implement on both sides, you cannot assure that systems from different vendors will have the same.

By the other hand, Modbus is a very fast protocol (it packs a lot of information in just one message). Regarding data integrity, it's very safe, since you always have to poll the process (there is no spontaneous sending).

IEC870-5-101 vs. 103

Question (5 Aug 1999): Does anyone have nice, easy to understand comparison table between IEC870-5-101 and IEC870-5-103?

I need to explain when and where can we use 101 and when 103.

Response: IEC870-5-101 is for "Basic telecontrol tasks" used for telecontrol information between RTU and control center.

IEC870-5-103 is the "Informative interface of protection equipment" and for information transmission between a protection equipment and the RTU.

Where to purchase IEC Documents

Question (4 Nov 1999): I am a new subscriber in the list. I would appreciate to anyone who can help me to find the iec870-5 standard specifications, in particular the 101, 102, 103 and 104 profiles.

Response: The IEC 60870-5 specification documents are only available through the IEC or authorized sales outlets. The IEC web site allows online purchase of the documents. From the IEC website www.iec.ch, select "IEC Web Store" and then select "Search and Buy". Enter a publication number of "60870-5". This will give a list of the documents and the format they are available in (hard-copy, Adobe Acrobat PDF, and CD-ROM).

For a list of authorized sales outlets for IEC documents, see: www.iec.ch/cs1sot-e.htm

Also see the web site www.standards.com.au/Catalogue enter standard number 60870, and select the "Both" button (Australian and International standards).

The Australian Standard AS 60870 series correspond exactly to the English text of the IEC 60870 series, and may be available at a lower price when purchased on-line.
