International Journal of Advanced Science and Technology
Volume 8, July, 2009

Compartmentalization of Protocols in SCADA Communication

[1]Dong-joo Kang and [2]Rosslin John Robles

[1]Hongik University, Korea
[2]Department of Multimedia Engineering, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
roslin_john@yahoo.com

Abstract

In SCADA systems, Communication is very important. In communication, protocols are needed to be implemented to avoid some problems. In the current state of SCADA communication, two protocols are widely used, the T101 or IEC 60870-5-101 (IEC101) and the DNP3 (Distributed Network Protocol). In this paper, we present each protocol and discuss the specifications of T101 and DNP3. This can help SCADA operators to select which protocol is suited for the operations of their SCADA systems.

Keywords: *SCADA, IEC 60870-5-101, DNP3, T101*

1. Introduction

Supervisory control and data acquisition system or SCADA refers to the combination of telemetry and data acquisition. SCADA includes the collecting of the information via a RTU (remote terminal unit), PLC's (Programmable Logic Controllers) and IED's (Intelligent electronic devices), transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays.

Three of the most important part of a SCADA system is Master Station, Remote Terminal (RTU, PLC, IED) and the communication between them. In order to have good communication between them, there must be a communication protocol. DNP3 and T101 are two of the most common protocols today. It is important to determine which protocol should be applied if you are planning a SCADA system. In the next sections of this paper, the DNP3 and T101 will be discussed and compared.

2. Protocols in SCADA Communication

In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. [1] These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols is now improved and contain extensions to operate over TCP/IP. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced. RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols.

Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. This paper discusses and compares T101 and DNP3.

These two open communication protocols that provide for interoperability between systems for telecontrol applications. Both are now competing within the world market. DNP is widely used in North America, South America, South Africa, Asia and Australia, while IEC 60870-5-101 or T101 is strongly supported in the Europe.

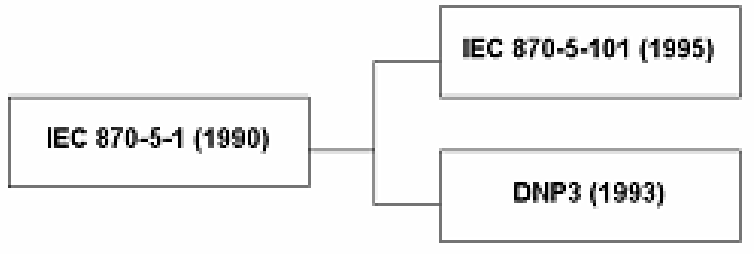

Figure 1. Standard Development

3. IEC 60870-5

IEC 60870-5 is the collection of standards produced by the IEC(International Electrotechnical Commission). It was created to provide an open standard for the transmission of SCADA telemetry control and information. It provides a detailed functional description for telecontrol equipment and systems for controlling geographically widespread processes specifically for SCADA systems. The standard is intended for application in the electrical industries, and has data objects that are specifically intended for such applications. It is also applicable to general SCADA applications in any industry. But IEC 60870-5 protocol is primarily used in the electrical industries of European countries.[6]

When the IEC 60870-5 was initially completed in 1995 with the publication of the IEC 870-5-101 profile, it covered only transmission over relatively low bandwidth bit-serial communication circuits. With the increasingly widespread use of network communications technology, IEC 60870-5 now also provides for communications over networks using the TCP/IP protocol suite. This same sequence of development occurred for DNP3.

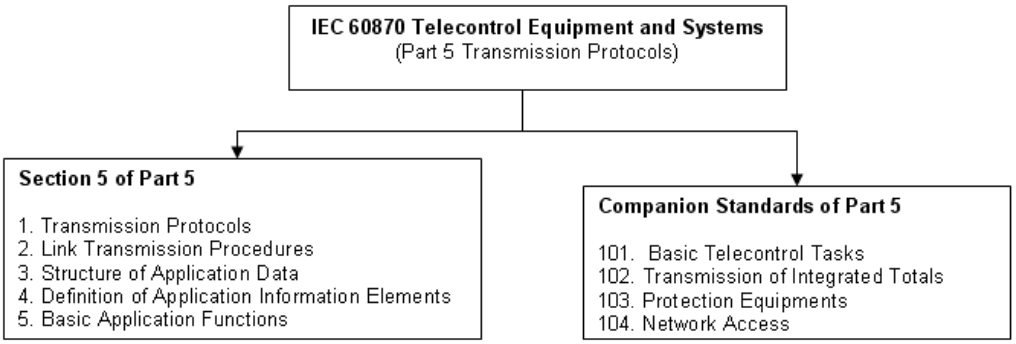

Figure 2. IEC 60870 Structure

3.1. T101

T101 or IEC 60870-5-101 (IEC101) is an international standard prepared by TC57 for power system monitoring, control & associated communications. This is compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and uses standard asynchronous serial tele-control channel interface between DTE and DCE. The standard is suitable for multiple configurations like point-to-point, star, mutidropped etc. [7]

3.2. T101 features

60870-5-101 or T101 have many features such as the following:

- Supports unbalanced (master initiated message) & balanced (master/slave initiated message) modes of data transfer.
- Link address and ASDU addresses are provided for classifying the end station and different sectors under the same.
- Data is classified into different information objects and each information object is provided with a specific address.
- Facility to classify the data into high priority (class-1) and low priority (class-2) and transfer the same using separate mechanisms.
- Possibility of classifying the data into different groups (1-16) to get the data according to the group by issuing specific group interrogation commands from the master & obtaining data under all the groups by issuing a general interrogation.
- Cyclic & Spontaneous data updating schemes are provided.
- Facility for time synchronization
- Schemes for transfer of files

3.3. Types supported by T101

Distributed Control System components are usually included in SCADA. IEDs, RTUs or PLCs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these RTUs and PLCs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves. [5]

3.4. Remote Terminal Unit

- Single indication without / with 24 / with 56 bit timestamps.
- Double indication without / with 24 / with 56 bit timestamps.

- Step position information without / with 24 / with 56 bit timestamps.
- Measured value – normalized, scaled, short floating point without / with timestamps.
- Bitstring of 32 bit without / with timestamps.
- Integrated totals (counters) without / with timestamps.
- Packed events (start & tripping) of protection equipments
- Single commands
- Double commands
- Regulating step command
- Set point commands of various data formats
- Bitstring commands
- Interrogation commands
- Clock synchronization & delay acquisition commands
- Test & reset commands

4. DNP3 Protocol

The DNP3 or Distributed Network Protocol is a set of communications protocols used between components in process automation systems. [2] It is usually used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities.

It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA systems. It is used by SCADA Master Stations or Control Centers, Remote Terminal Units, and Intelligent Electronic Devices.

It is primarily used for communications between a master station and IEDs or RTU's. DNP3 supports multiple-slave, peer-to-peer and multiple-master communications. It supports the operational modes of polled and quiescent operation. The latter is also referred to as reporting by exception.

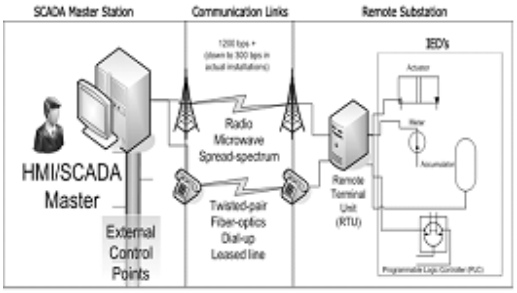

Figure 3. Overview of the DNP3 Protocol

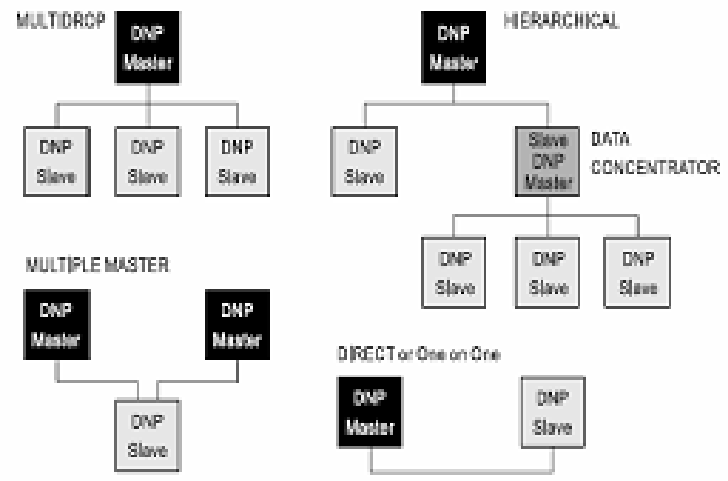

Figure 4. Network Topologies of DNP3

4.1. DNP3 Security

Although the protocol was designed to be very reliable, it was not designed to be secure from attacks by hackers and other malevolent forces that could potentially wish to disrupt control systems to disable critical infrastructure. This was a major oversight.

Because smart grid applications generally assume access by third parties to the same physical networks and underlying IP infrastructure of the grid, much work has been done to add Secure Authentication features to the DNP3 protocol. The DNP3 protocol is now compliant with IEC 62351-5. Some vendors, such as Itron, implement elliptic curve cryptography which the US NSA considers sufficient to protect information as "top secret" with only 384 bits. Implementation of ECC over DNP3 is not very widespread yet.

The DNP3 protocol is also referenced in IEEE Std. IEEE 1379-2000, which recommends a set of best practices for implementing modern SCADA Master-RTU/IED communication links. These include not just encryption but other practices that enhance security against well known intrusion methods.

4.2. DNP3 in SCADA Communication

The DNP3 protocol is utilized in communication between various SCADA system components. These system components include the SCADA master or HMI, the Remote Terminal Units, and Intelligent Electronic Devices. [3]

Operators of SCADA systems can monitor the DNP3 protocol within their operations to increase system reliability. This will reduce customer roil by decreasing downtime. DNP3 protocol was designed to avoid being distorted by legacy equipment, as well as EMI noise and low-grade transmission channels. While it adds network reliability, the DNP3 protocol does not make provisions for communications security. [4]

4.3. Advantages of using DNP3

DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. It is intended for SCADA (Supervisory Control and Data Acquisition) applications. It is not a general purpose protocol like those found on the Internet for transmitting email, hypertext documents, SQL queries, multimedia and huge files. [5]

The reasons for the adoption of DNP3 by users are primarily:

- It is an open protocol
- It is optimized for SCADA communications
- It provides interoperability between different
- vendor's equipment
- It is supported by a substantial number of
- SCADA equipment manufacturers
- It will provide immediate and long-term
- benefits to users

4.4. DNP3 Technical details

The DNP3 protocol has significant features that make it more robust, efficient, and self compatible than older protocols such as Modbus, at the cost of somewhat higher complexity.

DNP3 is, in standard networking terms, mostly a layer 2 protocol. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data. The DNP3 frame strongly resembles, but is not identical to the FT3 frame. It makes heavy use of Cyclic redundancy check codes to detect errors.

The improved bandwidth efficiency is accomplished through event oriented data reporting. The Remote Terminal Unit is initially interrogated with what DNP3 terms a "Class 0 poll." This causes the RTU to send all static point data to the Master station. Then, as the data points generate events, these events can be placed in one of three buffers whose status is reported on every Remote Terminal Unit response.

If there is data in that buffer, the buffer data flag is set. The Master can then see that there should be event data to be retrieved when issuing a poll for Class 1, Class 2, or Class 3. In other words, after a Class 0 poll, only significant data changes are sent. This can result in significantly more responsive data retrieval than polling everything, all the time, irrespective of whether it has changed significantly.

The Remote Terminal Unit can also be configured to spontaneously report Class 1, 2, or 3 data, when it becomes available.

The DNP3 protocol supports time synchronization with an RTU. The DNP Protocol has time stamped variants of all point data objects so that even with infrequent RTU polling, it is still possible to receive enough data to reconstruct a sequence of events of what happened in between the polls.

The DNP3 protocol has a substantial library of common point-oriented objects. The focus of this extensive library was to eliminate the need for bit-mapping data over other objects, as is often done in many Modbus installations. For example, floating point number variants are available, so there is no need to map the number on to a pair of 16 bit registers.

A Remote Terminal Unit for the DNP3 protocol can be a very small, simple embedded device, or it can be a very large, complex rack filled with equipment. The DNP User Group has established four levels of subsets of the protocol for RTU compliance. The DNP Users Group has published test procedures for Levels 1 and 2, the simplest implementations.

5. Comparison of T101 and DNP3

The Following table shows the comparison of both protocols, the DNP3 and the T101.

Table 1. Comparison of T101 and DNP3

	DNP3	T101
Organization	DNP user s group	IEC TC 57 WG 03
Standard	Open industry specification	IEC Standard
Dominant market	North America	Europe
Architecture	4-layer architecture Also supports 7 layer TCP/IP or UDP/IP	3-layer EPA architecture
Main coverage	Application Layer (Services and Protocol)	Application Layer (Services and Protocol)
Device Addressing	Link contains both source and destination address both always 16 bits Application layer does not contains address 32 b point addresses of each data type per device	Link address could be 0, 1, 2 bytes Unbalanced link contains slave address Balanced link is point to point so link address is optional (may be included for security)
Parameter setting control	Change some communication related parameters; more under development	Few
Cyclic transmission	Available but interval cannot be remotely adjusted	Eliminates static data poll message from master Interrupted by event triggered communication request
Open for other encoding solutions	Yes open for other encoding solutions like XML	No

6. Other SCADA Protocols

T101 and DNP3 are the most common SCADA protocols that are used in SCADA systems. Aside form T101 and DNP3 the following protocols are also utilized in SCADA systems.

6.1. Modbus RTU

Modbus RTU is a serial communications protocol published by Modicon in 1979 for use with its programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices. The main reasons for the extensive use of Modbus over other communications protocols are: It is openly published and royalty-free, Relatively easy industrial network to deploy and it moves raw bits or words without placing many restrictions on vendors. [9]

Modbus allows for communication between many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

6.2. RP-570

RP570 is a protocol used between an RTU (Remote Terminal Unit) in a substation and the FE (Front End), which is usually the SCADA software in the Control Center.

RP570 was developed by ABB in beginning of 1990. It was based on IEC 57 part 5-1, presently known as IEC 60870. Known variations are RP571, ADLP80 and ADLP180. [10]

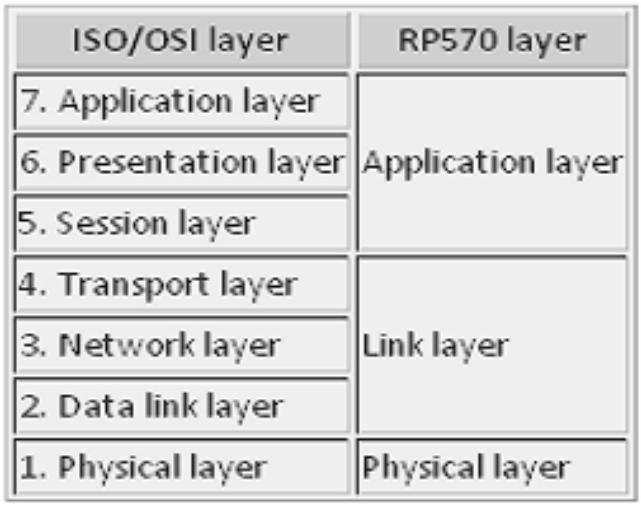

Figure 5. RP-570 by Layer

6.3. Profibus

Profibus devices communicate using the standardized PROFIBUS DP (Decentralized Periphery) communication profile which defines the rules governing communication. At the heart of the communication profile is what is known as the master/slave concept, whereby a

master (active communication peer) polls the associated slaves (passive communication peers) cyclically. When polled, a slave will react by sending a response frame to the polling master. A request frame contains the output data, e.g., setpoint speed of a drive, and the associated response frame contains the input data, e.g., the latest measured value from a sensor. In one bus cycle, the master polls, e.g., exchanges I/O data with, all associated slaves. This polling cycle is repeated as fast as possible.

In parallel with this type of communication, which is described as cyclic and supports the regular exchange of input and output data between a master and its slaves, parameter data, e.g., device settings, can also be transmitted via PROFIBUS. This action is initiated by the master (typically under user program control) between I/O cycles to read and/or write slave parameter data. This type of communication is referred to as acyclic communication.

There can be more than one master on a PROFIBUS system. In such systems, access rights are passed from one master to the next (token passing).

In order to meet the specific requirements of the various fields of application in the best ways possible, the PROFIBUS communication system has been expanded beyond its basic functionality to include a number of additional levels supporting special functions. There are currently three such protocol levels: DP-V0, DP-V1 and DP-V2. [11]

6.4. Conitel

Continel protocol is an asynchronous communications protocol used in many Supervisory Control and Data Acquisition (SCADA) systems. CONITEL Message blocks are composed of 31 bits plus a message synchronization "start bit" at the front of the first message block and an End of Message (EOM) bit at the end of each block. The protocol may be used either in a point-to-point or in a multi-drop configuration. The protocol can be used in either half or full-duplex operation. Communications security is provided by a 5-bit Bose-Chaudhuri cyclic

code which is included with each message block.

All communications exchanges in CONITEL protocol are initiated by the host. The remote cannot initiate any exchange with the host nor can the remote directly address or communicate with another remote. The remote will return a response to the host for all valid messages sent by the host and addressed to the remote. The only exception to this is in broadcast (all station) messages which produce no response from any remote. Also, all messages received by the remote are validated by checking the BCH code. If the BCH code is not valid, the remote will ignore the message; no action or response will be initiated.

7. Conclusion

IEC 60870-5-101/104 and DNP3 have basically the same functionality. They both provide solutions to first level of Data Acquisition Interoperability. Many factors are needed when selecting a protocol to be used like the kind of utility where SCADA will be implemented before choosing the proper protocol. The location should also be considered. Like for example if your system is located in America, it is better to use DNP3 since it is better to get technical assistance in case something is wrong. As discussed, DNP3 is popular in America.

Since DNP3 and T101 are open Standards, SCADA operators should monitor the development, and make contributions when appropriate, to T101 and DNP3. They should also pursue the developers to include security features on the protocols. This could help develop or improve the protocols in SCADA communication. In the future we are planning to study and include other SCADA protocols.

Acknowledgement

This work was supported by the Security Engineering Research Center, granted by the Korea Ministry of Knowledge Economy.

References

[1]SCADA - Wikipedia http://en.wikipedia.org/wiki/SCADA Accessed: December 2008
[2] DNP3 - Wikipedia http://en.wikipedia.org/wiki/DNP3 Accessed: December 2008
[3] DNP Users Group - Overview of the DNP3 Protocol http://www.dnp.org/About/Default.aspx Accessed: December 2008
[4] DPS Telecom - DNP3 Protocol http://www.dpstele.com/dpsnews/techinfo/dnp3_knowledge_base/dnp3_protocol.php Accessed: December 2008
[5] A DNP3 Protocol Primer. Revision A (March 2005)
[6] C. Clarke, D. Reynders, E. Wright (2004) Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems
[7] IEC 60870-5-101 - Wikipedia http://en.wikipedia.org/wiki/IEC_60870-5-101 Accessed: December 2008
[8] J. Makhija, L.R.Subramanyan (2003) Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus
[9] Wikipedia - Modbus http://en.wikipedia.org/wiki/Modbus Accessed: December 2008
[10] RP570 protocol http://www.serialmon.com/protocols/rp570.html Accessed: December 2008
[11] PI International "PROFIBUS communication protocol" http://pa.profibus.com/pb_communication_protocol/index.html Accessed: December 2008
[12] CONITEL 2020 PROTOCOL EMULATION http://www.miille.com/conitel.pdf Accessed: December 2008