

# The Taxonomy of Advanced SCADA Communication Protocols

Debnath Bhattacharyya<sup>1)</sup>

## Abstract

Communication is very important in SCADA systems. 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 system.

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 are 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

---

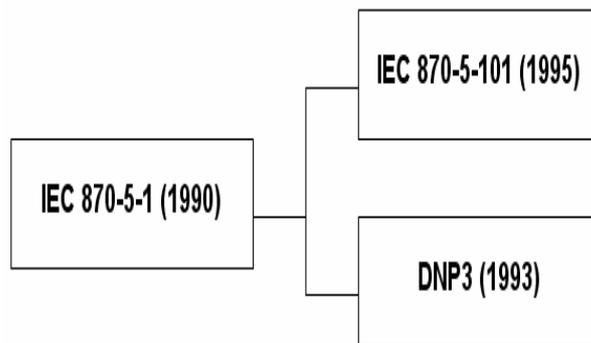
Received(July 17, 2008), Review request(July 18, 2008), Review Result(1st:August 07, 2008, 2nd:August 27, 2008)

Accepted(December 31, 2008)

<sup>1)</sup>Faculty Member, Computer Science and Engineering Department Heritage Institute of Technology, Kolkata-700107, INDIA  
email: debnathb@gmail.com

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. This paper discusses and compare 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.

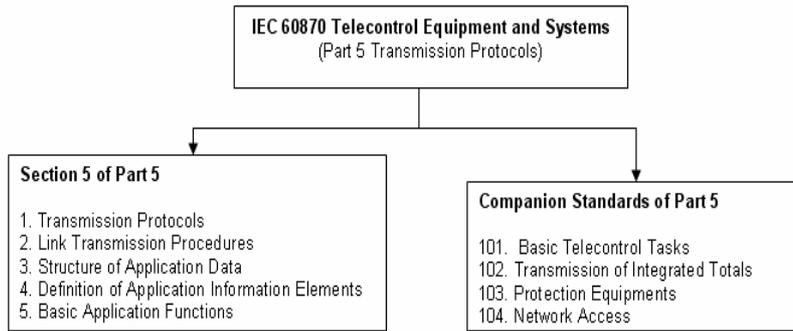


[Fig. 1] Standard development

### 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[2].

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.



[Fig. 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, multidropped etc[3].

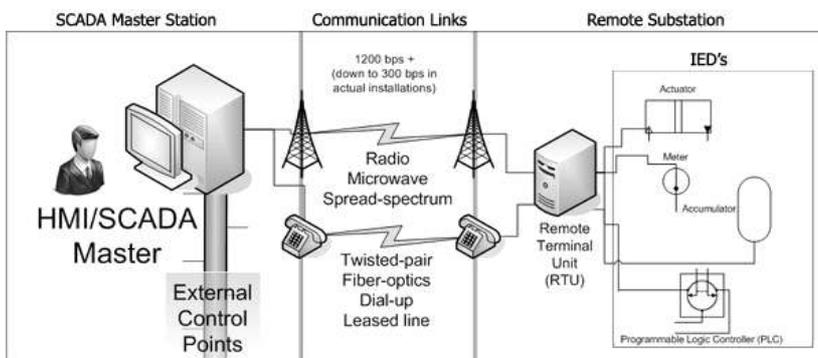
### 3.2 T101 features

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

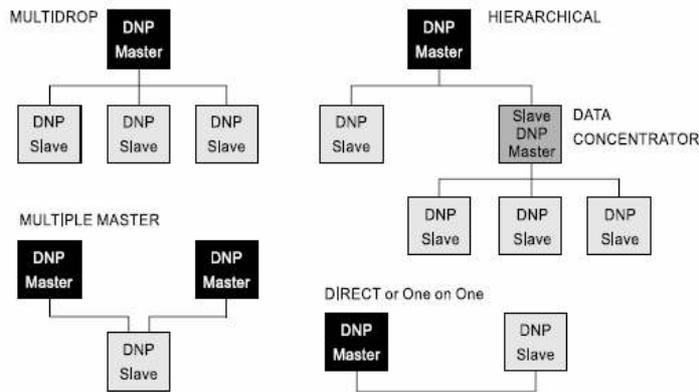
- Supports unbalanced (master initiated message) & balanced (master/slave initiated message) modes of data transfer.
- Link address and ASDU addresses are provided for classifying the end station and different sectors under the same.
- Data is classified into different information objects and each information 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

### 4. DNP3 Protocol

The DNP3 or Distributed Network Protocol is a set of communications protocols used between components in process automation systems[4]. It is usually used 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.



[Fig. 3] Overview of the DNP3 protocol



[Fig. 4] Network topologies of DNP3

#### 4.1 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[5].

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[6].

#### 4.2 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[7].

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

### 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
<b>Organization</b>	DNP user s group	IEC TC 57 WG 03
<b>Standard</b>	Open industry specification	IEC Standard
<b>Dominant market</b>	North America	Europe
<b>Architecture</b>	4-layer architecture Also supports 7 layer TCP/IP or UDP/IP	3-layer EPA architecture
<b>Main coverage</b>	Application Layer (Services and Protocol)	Application Layer (Services and Protocol)
<b>Device Addressing</b>	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)
<b>Parameter setting control</b>	Change some communication related parameters; more under development	Few
<b>Cyclic transmission</b>	Available but interval cannot be remotely adjusted	Eliminates static data poll message from master  Interrupted by event triggered communication request
<b>Open for other encoding solutions</b>	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 from 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[8].

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

ISO/OSI layer	RP570 layer
7. Application layer	Application layer
6. Presentation layer	
5. Session layer	
4. Transport layer	Link layer
3. Network layer	
2. Data link layer	
1. Physical layer	Physical layer

[Fig. 5] RP-570 by layer

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[9].

## 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[10].

#### **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.

## References

- [1] SCADA - Wikipedia <http://en.wikipedia.org/wiki/SCADA> Accessed: December 2008
- [2] C. Clarke, D. Reynders and E. Wright, Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, 2004.
- [3] IEC 60870-5-101 - Wikipedia [http://en.wikipedia.org/wiki/IEC\\_60870-5-101](http://en.wikipedia.org/wiki/IEC_60870-5-101), Accessed: December 2008
- [4] DNP3 - Wikipedia <http://en.wikipedia.org/wiki/DNP3>, Accessed: December 2008
- [5] DNP Users Group, Overview of the DNP3 Protocol, <http://www.dnp.org/About/Default.aspx>  
Accessed: December 2008
- [6] DPS Telecom - DNP3 Protocol [http://www.dpstele.com/dpsnews/techinfo/dnp3\\_knowledge\\_base/dnp3\\_protocol.php](http://www.dpstele.com/dpsnews/techinfo/dnp3_knowledge_base/dnp3_protocol.php)  
Accessed: December 2008
- [7] A DNP3 Protocol Primer Revision A, March 2005.
- [8] Wikipedia - Modbus <http://en.wikipedia.org/wiki/Modbus>, Accessed: December 2008
- [9] RP570 protocol <http://www.serialmon.com/protocols/rp570.html>, Accessed: December 2008
- [10] PI International, "PROFIBUS communication protocol"  
[http://pa.profibus.com/pb\\_communication\\_protocol/index.html](http://pa.profibus.com/pb_communication_protocol/index.html), Accessed: December 2008
- [11] J. Makhija and L.R.Subramanyan, Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus, 2003.
- [12] CONITEL 2020 PROTOCOL EMULATION <http://www.miille.com/conitel.pdf>  
Accessed: December 2008

## Authors



**Debnath Bhattacharyya**

2004 : Allahabad Agricultural Institute, A Deemed University, Allahabad, M.Sc (IT)

2008 : West Bengal University of Technology, Kolkata, M.Tech in Computer Science and Engineering

Research Interests : Biometric Authentication, Pattern Recognition, Security and medical Imaging.

