

SCADA PROTOCOLS AND COMMUNICATION TRENDS

By Rao Kalapatapu

1.0 INTRODUCTION

The present day Supervisory Control and Data Acquisition (SCADA) systems consisting of SCADA hosts, Remote Terminal Units (RTUs) and field devices monitor and control process equipment and systems from multiple locations and exchange data from various distributed control systems along the local and wide area networks.

SCADA system operation involves real time data exchange from the field devices as well as with other control systems such as DCS (Distributed Control and PI (Plant Information) systems).

A typical RTU in the field contains a central processor, set of Input /Output modules and communication devices to connect to field devices. The RTUs are similar to Programmable Logic Controllers (PLCs). PLCs are used with in a local area such as factory floor and are connected together usually by a local area network; where as RTUs are used in remote locations and connected by a Wide Area Network; Other wise both have CPU, I/O units and communication ports. Hence most of the discussion in this paper also applicable to PLC systems

These RTUs in turn are connected to the SCADA control system servers and workstations, as well as other local and remote area networks by means of phone lines, cables, leased lines, radios, fiber optics and/or a combination of these based on availability at each of these sites

2. 0 PROTOCOLS

The RTUs are pre-programmed to communicate with the central station SCADA and other networked systems in protocols that are designed to deliver reports on the status of all the input and output devices in the field.

Protocols are similar to languages, which allow the RTU/SCADA units to communicate with each other. All network architectures are loosely based on ISO (International Standards Organization) standard seven layer OSI (Open Systems Interconnection) model as below:

Layer 7 – Application
Layer 6 – Presentation
Layer 5 – Session
Layer 4 - Transport
Layer 3 – Network

Layer 2 – Data Link
Layer 1 - Physical

The object of the OSI model is to establish a framework that will allow any system or network to connect and exchange signals, messages packets and addresses. The model makes it possible for communications to become independent of the devised system and shield the user from the need to understand the complexity of the network.

In general, the bottom four layers cover the physical wiring, network and communication protocols of the local and wide area networks such as Ethernet and Frame Relay. TCP/IP (Transport Control protocol / Internet Protocol suite is a different open standard which is a similar open standard used by all and is discussed in detail in Section 3.

The presentation and session layers usually deal with establishing and then terminating the session between the two hosts. Not all networks use these layers

The Application (Layer 7) and above is where a typical PLC/RTU Protocol (such as Modbus) will provide the data at a typical SCADA workstation/ server in a user format from the field RTUs and local PLC systems.

2.1 SCADA /RTU PROTOCOLS

A large part of any complex SCADA system design is involved in matching the protocol and communication parameters between connecting devices. There are about 200 such real time user layer and application protocols. These include both proprietary and non- proprietary protocols, some of which are listed below:

- Allen Bradley DF1,DH and DH+
- GE Fanuc
- Siemens Sinaut
- Mitsubishi
- Modbus RTU / ASCII
- Omron
- Toshiba
- Westinghouse
- Other Vendor Protocols

The industry is now moving away from many of the old and proprietary protocols.

The following RTU/ PLC protocols are emerging as virtual standards in modern SCADA systems

2.1.1 MODBUS

The point-to-point Modbus protocol has become a virtual standard for RTU and PLC communications. During communication on a Modbus network, the protocol determines how each controller will know device address, recognize a message addressed to it determine the action to be taken and extract any information / data attached to it. There are a number of expansions to fix these shortcomings.

Modbus is, in many companies, a de facto standard in spite of its shortcomings. It cannot, for instance, handle large positive and negative numbers. This has resulted in a number of companies specific expansions of the protocol, such as Bristol, Daniels, ENRON and others. The idea behind Modbus, a command set operating on 16 bit registers has been used by all PLC manufacturers in the past

2.1.2 MODBUS X

The non-proprietary Modbus X expansion has been adopted by a number of companies and utilities and by SCADA software suppliers. It fixes the Modbus shortcomings, makes it man readable and able to handle positive and negative numbers with up to 9 digits of resolution, with an exponent range from -99 to +99. Point protocol, designed to read and write to individual I/O (Input Output) points in PLCs on a factory floor. The ModbusX expansion of the protocol is a universal, non-proprietary expansion, which permits handling large process variables in plain ASCII with sign and exponent, capabilities that are missing in Modbus. With the universal ModbusX expanded protocol_it is no longer necessary to experiment with different proprietary expansions of the protocol.

2.1.3 DNP (Distributed Network Protocol)

A member restricted protocol, used in some Electric Power systems. The DNP protocol has gone through various iterations. Presently it is up to version 3.0. The DNP association has rules, which tend to restrict the use of the protocol, and major SCADA software suppliers have been slow in implementing the protocol.

2.1.4 ASCII

The dominating computer protocol is ASCII, American Standard Code for Information Interchange. Virtually all computers, printers, modems and many sensors, actuators and flow computers now communicate in ASCII.

2.1.5 IEEE 60870

This protocol is mostly used in power transmission and distribution systems IEC 60870-5-101 is an International Communications Protocol Standard for the Telecontrol of Electric Power transmission systems, which is being widely adopted in many countries throughout the world.

2.1.6 PROTOCOLS FOR LOCAL DEVICES

The local area networks / protocols from sensors/ field devices to the PLC/RTU and from PLC/RTU to SCADA are

Sensor Networks: These are simple basic on/off field devices connecting networks

Fieldbus Networks: These are used to connect analog and smart field devices such as valve actuators, pumps and other field control systems

Control Networks: These are used for peer to peer connections between control systems such as SCADA/DCS/Analyzer/Safety PLC systems

Safety Buses: These are used for deterministic time sensitive safety type device connections

With the above open type industry standard emerging protocols and networks, availability of drivers and programming software can exist from many if not all SCADA system vendors

2.2 COMMUNICATION TRENDS

As in any data communication network, many types of communication media are supported from PLC/RTU to central/ distributed SCADA systems via local and wide area networks. A local Area network is contained within a local geographical area such as a building or a campus and consists of few buildings within closed proximity. On the other hand, a wide area network is a network that connects many local area networks spread across different cities at least 100 Kilometers (67 miles) apart.

The types of wide area networks include

- Analog point to point and multi-point modem networks
- Frame relay/Cell relay type point to point and multi-point networks
- Wireless Radio/ Satellite networks
- Fiberoptic based networks

At present time, a SCADA network may be built around many of the above possible combinations of networks and transmission protocols. More computer power is to be provided from the SCADA hosts since more data is required to meet the information demands of the present day corporate networks. Thus the

communication and network environment they operate are to be continuously evaluated for improvements and upgraded as time goes by.

2.3 LEGACY NETWORKS

The existing SCADA protocols share certain characteristics that make them very dependable in what may be termed as "robust but older/ legacy " networks.

These networks are often used very low speed namely 300 - 1200 bits per sec (bps). The data is usually asynchronous (no time synchronization) and remote terminal units are polled over a single multi-point circuit. All this polling and response must happen in a very short time often measured in fractions of a minute.

At present, to meet this higher demand for data, SCADA equipment manufacturers, system designers and users started looking for higher speed devices. There is a very large existing infrastructure of phone lines, private wire and microwave that operate at voice grade frequencies, where there is a bandwidth of about 3000 hertz. This is sufficient to pass for example a 9600 bps fast poll modem. Fast poll modems work like 1200 modems to the extent that they pass data over voice grade lines, use 4-wire phone lines and work in multi-drop mode.

In addition, the new faster networks, and their protocols interact with existing SCADA protocols and present some interesting challenges. The network protocols such as frame relay, Ethernet, and IP, each have time sensitive characteristics that will generate delays, cause short gaps in the data, or not transmit some Data Carrier Detect (DCD) signal transitions. These delays may cause SCADA protocols to assume errors in the links. If this can be overcome, then there are many new and faster communication networks available

If this can be overcome, then there are many new and faster communication networks available.

2.4 TELCOMMUNICATIONS

In the communication world, there exists two types of networks, namely circuit switched and packet switched networks. The circuit switched network establishes direct connection between two or more stations by means of switches, which is normally done with telephone dial up modem networks. On the other hand, there is a general move towards a packet style operation where the data is handled in packets prefixed with some addressing. This in a packet switched network, data is routed in best possible route in a complex meshed private or public wide or local area network. Packet switched networks are more cost effective, since a dedicated network is not needed from start to finish.

Telecommunications facilities switch, combine, amplify and transmit information over chosen media. The hardware consists of transmitters to convert the voice/data signals to suite the transmission media, wiring, switches, routers, bridged and multiplexers to amplify and carry the signals to a receiving station.

Described below are few of the current day networks that may be used for remote SCADA transmissions from remote and local area nodes in wired or wireless networks.

2.4.1 Frame Relay

Frame relay is a packet switched network. The data packets of frame relay networks may have no direct correspondence to the size of SCADA poll/response packets. Therefore, a SCADA packet will often be broken up into several frame relay packets by the network, with delays between the frame relay data packets. Typically communication system vendors such as Sprint, MCI and AT & T type of packet switching use this when transporting large data through large geographical distance. Thus they carry the data encapsulated for transportation by their frame relay protocols via their routers in all available multi path meshed long haul network. The frame is thus a data communication service provided by telecom carriers across a network with one or more points. Cost is based on three elements: committed information rates, access circuit and port speed.

2.4.2 ETHERNET

Ethernet is one of the first Local Area Networks introduced by Xerox, in early 70s. This type of network underlined a radical change in the way computing is carried out. Rather than using terminals to access shared mainframe or mini-computer, the user now works directly at a single user computer. The computer in turn is connected to a local network giving the user shared access to information stored and to common peripheral equipment such as printers and fax machines. This resulted in changes in wide area networking. LAN to LAN connectivity is made use of instead of terminal to computer resulting in requirements for higher speed of communication.

Ethernet is also a packet-oriented protocol. Ethernet packets are generated without regard to the incoming data protocols. Ethernet devices have protocol rules to obey, which are related to the needs of the Ethernet, so as to allow variety of possible devices that may be connected to an Ethernet network similar to frame relay. These are local area based but can be applied to wide area when from network to network since we have 100MB and Gigabit Ethernet routers which can do this type of transfer

2.4.3 ATM

ATM stands for Asynchronous Transfer Mode which is a cell relay type broadband connection oriented switching service that carries data/ video/audio information in fixed length of 48 bytes with a 5 byte header for a total of 53 bytes which is called a cell. Broadband is a form of network modulation in which multiple channels are formed by dividing the transmission medium (such as fiberoptic cable) in to discrete frequency segments)

This is a global standard. For integrated, high speed broadband networks that can handle any kind of information including data, voice, and video as stated above

2.4.5 Fiberoptic Networks

Around the same time, computers were becoming more prevalent in the office. Networking these computers together was desirable and beneficial. When linking these computers over a long distance, the existing voice-optimized WANs were used. Because computers send data instead of voice and data has different characteristics and so these WANs did not send computer data very efficiently. To address these concerns, ITU-T (International Telecommunication Union– Telecommunications is an agency of United Nations formally CCITT) and other standards groups started work in the 1980s to establish a series of recommendations for the transmission, switching, signaling and control techniques. These are required to implement an intelligent fiber-based network that could solve current limitations and would allow networks to be able to efficiently carry services of the future. This network was termed Broadband Integrated Services Digital Network (B-ISDN). By 1990, decisions had been made to base B-ISDN on SONET/SDH (Synchronous Optical Network/Synchronous Digital Hierarchy) and ATM at speeds varying from 55 Mbits per sec to N multiples of 55Mbits per sec which is now already defined up 4696Mbits per sec.

These can be used for long distance distributed SCADA system transmission of data by private or public switched networks at speeds of 51.8 Mbps to 2.48Gpbs based on above technologies such as SONET/SDH or private fiberoptic based Siemen's Open Transport Network (OTN).

2.4.6 TCP/IP Networks

TCP/IP networks have the same packet characteristics of frame relay and Ethernet networks. There is no relationship between the IP packets and the incoming SCADA poll/response data packets. TCP is a protocols developed in late 70s by Department of Defense for providing interoperability among several equipment vendors.

In year 1989 Internet has evolved (of course every one takes credit including Al Gore) from ARPANET (Advanced Research Project Agency Network) of

Department of Defense. Internet is a collection of independent Packet Switched Networks that are loosely interconnected to act as a Coordinated network. Unlike OSI, TCP/IP is not a true international standard, but an open standard that is widely used internationally.

2.4.7 IP Addressing

IP addressing is based on the concept of hosts and networks. A host is essentially anything on the network that is capable of receiving and transmitting IP packets on the network, such as a SCADA RTU/ SCADA workstation or a smart field device such as a smart control valve. . It is not to be confused with a server: Servers and client workstations are all IP hosts.

The hosts are connected together by one or more networks. The IP address of any host consists of its network address plus its own host address on the network. IP addressing uses one address for both network and host addresses. How much of the address is used for the network portion and how much for the host portion varies from network to network

An IP address is 32 bits wide, and it is composed of two parts: the network number, and the host number [1, 2, and 3]. By convention, it is expressed as four decimal numbers separated by periods, such as "200.1.2.3" representing the decimal value of each of the four bytes. Valid addresses thus range from 0.0.0.0 to 255.255.255.255.

2.4.8 Virtual SCADA Networks

The Internet has grown immensely over the last 15 years. Leveraging the availability of the Internet and wireless technology, SCADA vendors found remote access solutions, which allow virtually every telemetry and monitoring device to be connected to the Internet and thereby to your terminal of choice. It enables you to be connected to your network or device, without being confined to the office.

2.4.9 Wireless Networks

Wireless networks come in many flavors and styles. These include

- Satellite networks
- Licensed VHF and UHF point to point and multi-point Radio
- Spreadspectrum License free (900 MHz, 2.4 GHZ, 5.8Ghz and 24 GHz)
- Point to point Microwave

With in a narrow range of a building or campus, wireless data can be moved from node to node with privately owned spread spectrum radio networks. Broader ranges require some form of public network. The most common method is dial up

over cellular, Cellular digital packet data (CDPD) networks or by using Specialized Mobile Radio (SMR) or private carrier wireless networks.

3.0 SCADA SYSTEM DESIGN CHALLENGES

As can be seen above, we are surrounded by a multitude of options, and faced with tedious and challenging task to harness these current day and upcoming future technologies in the existing systems as well as in the newer systems in a cost effective and expeditious manner.

We need to review how we can maintain our older /legacy SCADA systems to provide the best possible control and monitoring by gradually upgrading

- Field Remote Terminal Units and field device wiring/networks
- Control Room central SCADA units and local area networks they reside
- Communication networks between the field PLC/ RTUs and the central SCADA systems/ other control and IT networks.
- Interfaces between control room SCADA and other control/IT networks

For new systems we need to review the following:

- Consider open non-proprietary standards and protocols for RTU/SCADA Control and Monitoring.
- Analyze wire and wireless communication systems for cost effective systems.
- Check for industry proven and easily upgradable systems.
- Interchangeable software and hardware from one vendor to other.
- Ownership of programs and system software code after purchase of systems.

The newer RTUs come in variety of flavors and include communication connectivity through serial Modbus, Modbus/TCP, Ethernet and a host of other protocols. The remote processors are equipped with smart modems for wireless or leased telephone / satellite connectivity. In all cases the data is serial and depending on the amount of data, it ca be transferred quite fast with 9600/19.2 bps modems and wide area networks.

The present day designs will be using distributed processing and peer-to-peer communication from field to the control room. For example, as explained earlier each local RTU can have its own unique I/P address similar to unique tag names we had for sensors and switches during last couple of decades. These I/P units are then polled by any local/ PC/RTU/PLC/ Terminal Server, once every few seconds or as needed to get real time operating data from the field.

For example, the CEO of XYZ company may only need the daily production reports from the oil/ gas well fields, the SCADA manager may need only operation and maintenance reports and a shift operator may need only real time data on his MMI console. All these are being done now with the SCADA systems using off the shelf hardware and software products available on the market today.

The cost of operating this local and wide area networks is to be taken in to consideration when designing a SCADA system. For example, a typical cost of leasing a 1.5 Mbit T1 line runs in to around \$700 to \$1000 per month for 1000 miles distance. But the cost of owning a 1000 Mile, ten strand fiber optic cable line with a capacity up to two Gbit/sec per two fibers installed cost of around \$5 Million. So the monthly loan payment over 20 years will have a loan payment of around \$ 25,000 per month. But to get an equivalent leased line, you can see that it will be cost prohibitive and can not be compared on equal footing. Even though fiber optic cable costs appears very high, the operation and maintenance costs are low and the capacity is unlimited for all future expansions where as in the case of leased lines, the costs increase quite rapidly when bandwidth requirements reach 1Mbits/sec and above.

Also, it is to be noted that due to advances in technology and possible custom and off the shelf hardware and software availability, the distinction between RTUs, PLCs, DCS and PCs are disappearing. All these now overlap each other with respect to functionality, protocols, hardware and software. The main requirement for all these networks is, they have to operate in real time deterministic mode so that the process and production data can be received and sent in a timely manner to all required places on the local and wide area networks.

4.0 CONCLUSION

A review of available technologies for design, operation and maintenance of SCADA systems from user's point of view is described in this paper. SCADA systems, whether of the latest design or systems that have been in operation for years, can usually be migrated to the high-speed networks and open non-proprietary protocols with a little bit of planning and study of available options. System designers must be familiar with issues of functionality, transmission delays, polling cycles, data processing requirements and available technologies. In addition, proprietary and vendor specific protocols and programs should be

avoided at all costs in lieu of open standards and easily interchangeable software and hardware from one vendor to other.

Final question for SCADA Experts! Will SCADA work well over cellular telephone links or the public Internet? Probable but much caution is required. Cellular phone networks are designed for short-term conversations, have low data rates, and are susceptible to call disconnection at this time. Unless a SCADA system is designed for short-term dial up calls, it is unlikely to be a satisfactory alternative. The Internet will have delays similar to that of old packet switched X-25 Networks (used for example, in credit card processing) and may also suffer packet loss that can be as high as 10% or more during severe congestion periods. The Internet may be acceptable for some remote monitoring and data retrieval, but not for real time data collection and control needs

It appears that private and semi private network, such as cable both copper and fiber optic, phone lines and /or satellite will be the communications choice. Open non proprietary protocols such as Modbus, Ethernet, TCP/IP with application protocols such as OPC/OBBC will be the best choice because of their availability from any SCADA vendor and provide simplicity of design and installation as well as ease of system operation and maintenance.

5.0 REFERENCES

- “Electronic Communication Design” by Andrew F Inglis
- “The Irvin Handbook of Telecommunication” by James Harry Green
- “Automation Selection” by Dick Caro
- “SCADA” by Stuart A. Boyer”
- “Practical SCADA For Industry” by David Bailey& Edwin Wright’
- “Telecom & networking Glossary “ By Robert Mastin
- “Optimizing SCADA network Communications” A paper By John McCain & Russel Straayer from Data Com for Business
- Various vendor literature from PLC/RTU suppliers

Author’s Bio data

Rao Kalapatapu is a Senior Engineer with wide range of experience in design and installation of SCADA, DCS, PLC and other Control systems for Oil and Gas pipelines, Chemical and Petrochemical Projects. He is a Professional Engineer from States of Texas and Utah. Rao is a senior member of ISA. He can be reached at vrkalapatapu @hotmail.com.

End