

**NCS TIB 04-1**



---

---

**NATIONAL COMMUNICATIONS SYSTEM**

---

---

**TECHNICAL INFORMATION BULLETIN 04-1**

**Supervisory Control and Data  
Acquisition (SCADA) Systems**

**October 2004**

**OFFICE OF THE MANAGER  
NATIONAL COMMUNICATIONS SYSTEM  
P.O. Box 4052  
Arlington, VA 22204-4052**





**Office of the Manager  
National Communications System**

**October 2004**

**By**

**Communication Technologies, Inc.  
14151 Newbrook Drive, Suite 400  
Chantilly, Virginia 20151  
703-961-9088 (Voice)  
703-961-1330 (Fax)  
[www.comtechnologies.com](http://www.comtechnologies.com)**



NCS TECHNICAL INFORMATION BULLETIN 04-1

**SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS**

October 2004

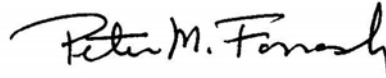
PROJECT OFFICER

APPROVED FOR PUBLICATION:



DALE BARR

Sr. Electronics Engineer  
Technology and Programs Division



PETER M. FONASH

Chief, Technology  
and Programs Division

FOREWORD

Among the responsibilities assigned to the National Communications System, is the management of the Federal Telecommunications Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunications Standards Committee identifies, develops, and coordinates proposed Federal Standards which either contribute to the interoperability of functionally similar Federal telecommunications systems or to the achievement of a compatible and efficient interface between computer and telecommunications systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development efforts with appropriate technical committees of the International Organization for Standardization, the International Telecommunication Union-Telecommunications Standardization Sector, and the American National Standards Institute. This Technical Information Bulletin presents an overview of an effort which is contributing to the development of compatible Federal and national standards in the area of SCADA systems. It has been prepared to inform interested Federal and industry activities. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

National Communications System  
Attn: N2  
P. O. Box 4052  
Arlington, VA 22204-4052



# **Supervisory Control and Data Acquisition (SCADA) Systems**

## **Abstract**

The goal of this Technical Information Bulletin (TIB) is to examine Supervisory Control and Data Acquisition (SCADA) systems and how they may be used by the National Communications System (NCS) in support of National Security and Emergency Preparedness (NS/EP) communications and Critical Infrastructure Protection (CIP). An overview of SCADA is provided, and security concerns are addressed and examined with respect to NS/EP and CIP implementation. The current and future status of National, International, and Industry standards relating to SCADA systems is examined. Observations on future trends will be presented. Finally, recommendations on what the NCS should focus on with regards SCADA systems and their application in an NS/EP and CIP environment are presented.





## Table of Contents

Executive Summary .....	ES-1
1.0 Introduction.....	1
2.0 SCADA Overview .....	4
2.1 Field Data Interface Devices.....	6
2.2 Communications Network .....	7
2.3 Central Host Computer .....	7
2.4 Operator Workstations and Software Components.....	8
3.0 SCADA Architectures .....	10
3.1 Monolithic SCADA Systems.....	10
3.2 Distributed SCADA Systems.....	10
3.3 Networked SCADA Systems.....	12
4.0 SCADA Protocols.....	15
4.1 IEC 60870-5-101 .....	15
4.2 DNP3.....	19
5.0 Deploying SCADA Systems.....	31
5.1 Twisted-Pair Metallic Cable .....	31
5.2 Coaxial Metallic Cable .....	31
5.3 Fiber Optic Cable.....	32
5.4 Power Line Carrier.....	33
5.5 Satellites.....	34
5.6 Leased Telephone Lines .....	35
5.7 Very High Frequency Radio .....	35
5.8 Ultra High Frequency Radio.....	36
5.8.1 Point-to-Point.....	36
5.8.2 Multiple Address Radio Systems.....	37
5.8.3 Spread Spectrum Radio.....	38
5.9 Microwave Radio.....	38
6.0 Security and Vulnerability of SCADA Systems.....	41
6.1 Attacks Against SCADA Systems.....	41
6.2 Developing a SCADA Security Strategy .....	46
7.0 SCADA Standards Organizations.....	49
7.1 The Institute of Electrical and Electronics Engineers (IEEE) .....	49
7.2 American National Standards Institute .....	49
7.3 Electric Power Research Institute .....	50
7.4 International Electrotechnical Commission.....	51
7.5 DNP3 Users Group .....	52
8.0 Observations and Conclusions.....	54
9.0 Recommendations.....	55
Appendix A - Acronyms.....	57
Appendix B - References.....	60
Appendix C - Bibliography.....	61

## List of Figures

Figure 2.1: Current SCADA Communications Media.....	5
Figure 2.2: Typical SCADA System .....	5
Figure 3.1: First Generation SCADA Architecture .....	11
Figure 3.2: Second Generation SCADA Architecture.....	12
Figure 3.3: Third Generation SCADA System.....	13
Figure 4.1: Enhanced Performance Architecture.....	16
Figure 4.2: Structure of ADSUs in IEC 60870-5-101 (1995-11.....	19
Figure 4.3: DNP3 Client Server Relationship.....	22
Figure 4.4: Common DNP3 Architectures in Use Today .....	24
Figure 4.5: DNP3 Layers .....	26
Figure 6.1: Relationship Between Corporate and SCADA .....	46

## List of Tables

Table 1.1: Matrix of NE/EP Requirements.....	2
Table 5.1: Twisted-Pair Advantages/Disadvantages .....	31
Table 5.2: Coaxial Cable Advantages/Disadvantages .....	32
Table 5.3: Fiber Optic Cable Advantages/Disadvantages .....	33
Table 5.4: Power Line Carrier Advantages/Disadvantages .....	34
Table 5.5: Satellite Advantages/Disadvantages.....	35
Table 5.6: Leased Circuits Advantages/Disadvantages.....	35
Table 5.7: VHF Radio Advantages/Disadvantages .....	36
Table 5.8: Point-to-Point UHF Radio Advantages/.....	37
Table 5.9: MARS UHF Radio Advantages/Disadvantages .....	38
Table 5.10: Spread Spectrum Radio Advantages/Disadvantages .....	38
Table 5.11: Microwave Radio Advantages/Disadvantages .....	40
Table 6.1: SCADA Attack Matrix .....	43

## Executive Summary

The National Communications System (NCS), Technology and Programs Division (N2) develops and implements national level programs that provide for an enduring and effective telecommunications infrastructure to fulfill National Security and Emergency Preparedness (NS/EP) requirements under all circumstances. It also develops and implements plans for technology development, procedures, and strategic architectures. These improve the reliability, interoperability, and infrastructure protection of the Federal Government's owned or commercially provided NS/EP telecommunications and related Information Systems (IS) resources, ensuring the Federal Government receives the maximum benefit of emerging technologies. Technologies are also evaluated for their use in NS/EP and Critical Infrastructure Protection (CIP) missions. N2 analyzes new technologies that may offer substantial operational and performance improvement for NS/EP applications.

SCADA systems have been used in the Utilities industry in the United States (U.S.) since the 1960s. These systems are used to monitor critical infrastructure systems and provide early warning of potential disaster situations. One of the most important aspects of SCADA has been its ability to evolve with the ever-changing face of technology that is now referred to as Information Technology (IT) systems. SCADA has evolved from a monolithic architecture to a networked architecture.

This Technical Information Bulletin (TIB) focuses on:

- Introducing the concepts of SCADA systems
- Identifying what components make up a typical SCADA system
- Plotting the evolution of SCADA systems through its monolithic, distributed, and networked evolution
- Looking at the ways in which a SCADA system can be deployed
- Examining the protocols used in these systems currently as well as the standards and potential future SCADA protocols

Based upon the analysis in this TIB, the following generalized observations and conclusions are as follows:

- SCADA systems have been around since the 1960s and have evolved as technology changes
- Today's SCADA systems are able to take advantage of the evolution from mainframe-based to client/server architectures. These systems use common communications protocols like Ethernet and TCP/IP to transmit data from the field to the master control unit.

- SCADA protocols have also evolved from closed proprietary systems to an open system allowing designers to choose equipment that can help them monitor their unique system using equipment from mixed vendors

The NCS should:

- Undertake to analyze IEC 60870-5, DNP3, and UCA 2.0 to see which one may suit their NS/EP and CIP missions best
- Monitor and participate as appropriate in the IEEE standards process as it relates to SCADA systems, which are being developed through the IEEE Power Engineering Society
- Participate in the ANSI-HSSP. This panel is looking into refining and creating standards critical to Homeland Security. They are looking at Utilities in particular which heavily utilize SCADA systems.
- Monitor and participate as appropriate in the IEC standards process as it relates to SCADA systems. More specifically, participate in the development of the UCA 2.0 specification.

Specific conclusions and recommendations are contained in Sections 8 and 9.

## 1.0 Introduction

The National Communications System (NCS) was established through a Presidential Memorandum signed by President John Kennedy on August 21, 1963. The memorandum assigned NCS the responsibility of providing necessary communications for the Federal Government under national emergency conditions by linking together, improving, and expanding the communication capabilities of the various agencies.

In April 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness (NS/EP) Telecommunications Functions*, which broadened the mission and focus of the National Communications System. Since that time, the NCS has been assisting the President and the Executive Office of the President (EOP) in exercising wartime and non-wartime emergency telecommunications and in coordinating the planning for, and provisioning of, NS/EP communications for the Federal Government under all circumstances. In this regard, the Office of the Manager, NCS (OMNCS), particularly its Technology and Programs Division (N2), always seeks to improve the Federal Government's ability to respond to National Security and Emergency Preparedness situations. As part of this mission, the N2 division identifies new technologies that enhance NS/EP communications capabilities and ensures key NS/EP features such as priority, interoperability, reliability, availability, and security are supported by emerging standards. In concert with this approach, the N2 manages the Federal Telecommunications Standards Program. Additionally, the N2 division directs efforts in both NS/EP management and applications services.

National Security and Emergency Preparedness requirements fall into the areas [1] [2] as shown in Table 1.1, and are identified in the Convergence Task Force Report [3].

The goal of this Technical Information Bulletin (TIB) is to:

- Examine Supervisory Control and Data Acquisition (SCADA) systems
- Describe how SCADA systems have evolved since being deployed in the 1960s
- Examine how SCADA protocols have evolved from strictly proprietary to the development of open protocols which allow equipment from various manufacturers to work together
- Addresses the security aspects of SCADA systems
- Examines the standards that currently exist or are being drafted to help support the growth of these systems
- Observations, conclusions, and recommendations on how these technologies could support the NCS and their NS/EP and CIP mission

**Table 1.1: Matrix of NE/EP Requirements**

<b>Functional Requirement</b>	<b>Description</b>
Enhanced Priority Treatment	Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic
Secure Networks	These services ensure the availability and survivability of the network, prevent corruption of or unauthorized access to the data, and provide for expanded encryption techniques and user authentication
Restorability	Should a service disruption occur, voice and data services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis
International Connectivity	Voice and data services must provide access to and egress from international carriers
Interoperability	Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks
Mobility	The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service (PCS), cellular, satellite, High Frequency (HF) radio)
Nationwide Coverage	Voice and data services must be readily available to support the National security leadership and inter- and intra-agency emergency operations, wherever they are located
Survivability	Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war
Voice Band Service	The service must provide voice band service in support of presidential communications
Scaleable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements
Addressability	Addressability is the ability to easily route voice and data traffic to NS/EP users regardless of user location or deployment status. Means by which this may be accomplished include “follow me” or functional numbering, call forwarding, and functional directories

<b>Functional Requirement</b>	<b>Description</b>
Affordability	The service must leverage new Public Network (PN) capabilities to minimize cost. Means by which this may be accomplished favor the use of Commercial Off-The-Shelf (COTS) technologies and services and existing infrastructure
Reliability	The capability of an information or telecommunications system to perform consistently and precisely according to its specifications and design requirements, and to do so with high confidence

## 2.0 SCADA Overview

SCADA is an acronym for Supervisory Control and Data Acquisition. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals. A SCADA system gathers information (such as where a leak on a pipeline has occurred), transfers the information back to a central site, then alerts the home station that a leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. These systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or very complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system. Traditionally, SCADA systems have made use of the Public Switched Network (PSN) for monitoring purposes. Today many systems are monitored using the infrastructure of the corporate Local Area Network (LAN)/Wide Area Network (WAN). Wireless technologies are now being widely deployed for purposes of monitoring.

SCADA systems consist of:

- One or more field data interface devices, usually RTUs, or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators
- A communications system used to transfer data between field data interface devices and control units and the computers in the SCADA central host. The system can be radio, telephone, cable, satellite, etc., or any combination of these.
- A central host computer server or servers (sometimes called a SCADA Center, master station, or Master Terminal Unit (MTU))
- A collection of standard and/or custom software [sometimes called Human Machine Interface (HMI) software or Man Machine Interface (MMI) software] systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices

Figure 2.1 shows a very basic SCADA system, while Figure 2.2 shows a typical SCADA system. Each of the above system components will be discussed in detail in the next sections.



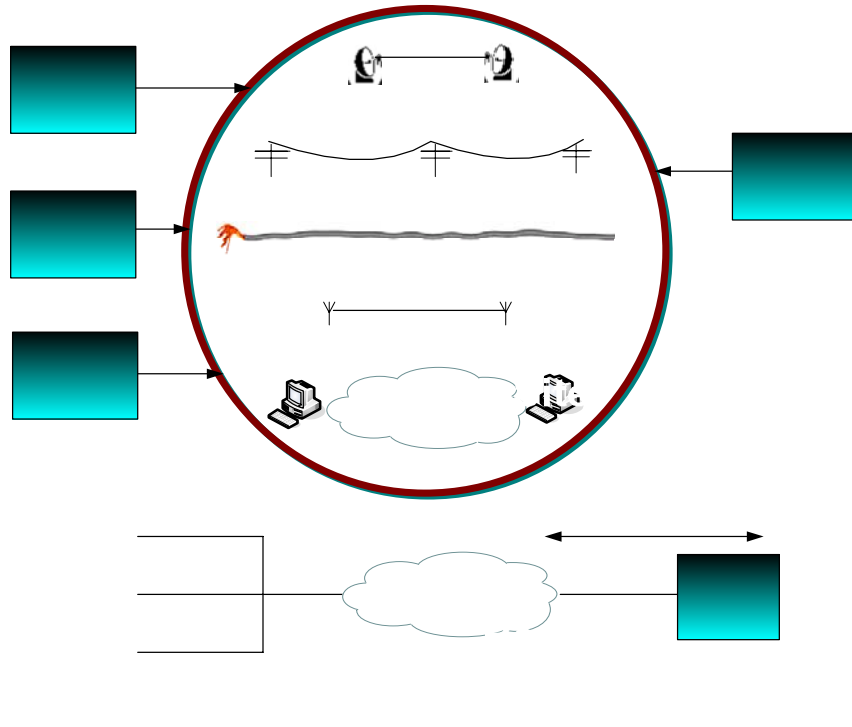


Figure 2.1: Current SCADA Communications Media

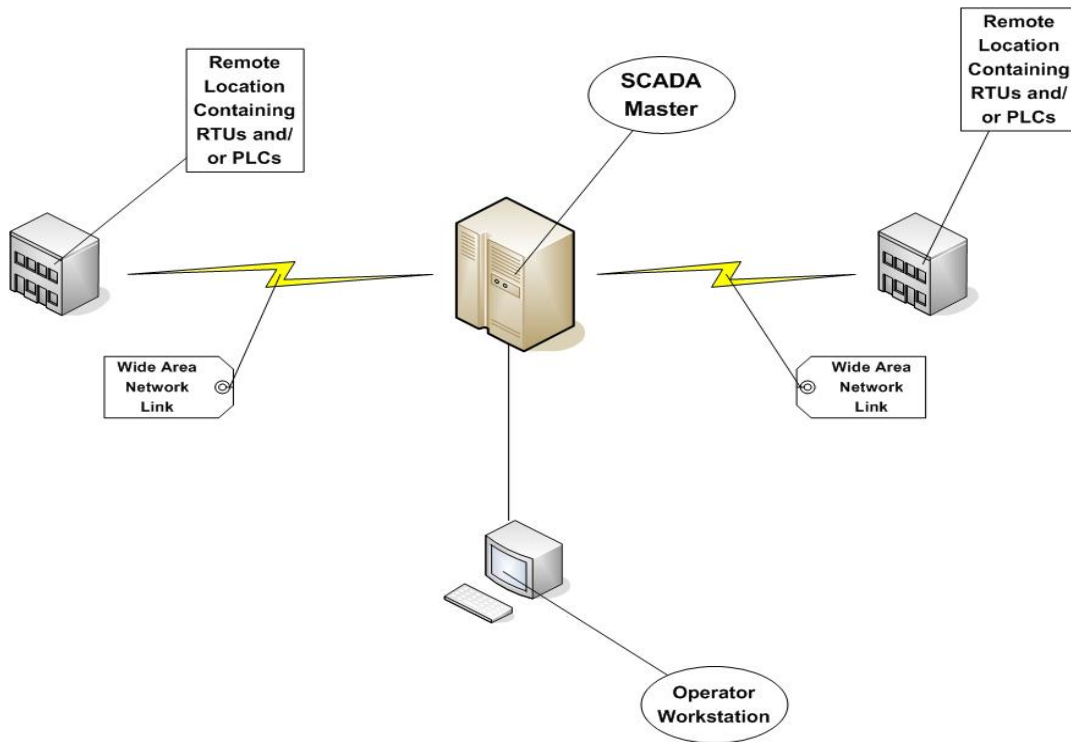


Figure 2.2: Typical SCADA System [4]

## 2.1 Field Data Interface Devices

Field data interface devices form the "eyes and ears" of a SCADA system. Devices such as reservoir level meters, water flow meters, valve position transmitters, temperature transmitters, power consumption meters, and pressure meters all provide information that can tell an experienced operator how well a water distribution system is performing. In addition, equipment such as electric valve actuators, motor control switchboards, and electronic chemical dosing facilities can be used to form the "hands" of the SCADA system and assist in automating the process of distributing water.

However, before any automation or remote monitoring can be achieved, the information that is passed to and from the field data interface devices must be converted to a form that is compatible with the language of the SCADA system. To achieve this, some form of electronic field data interface is required. RTUs, also known as Remote Telemetry Units, provide this interface. They are primarily used to convert electronic signals received from field interface devices into the language (known as the communication protocol) used to transmit the data over a communication channel.

The instructions for the automation of field data interface devices, such as pump control logic, are usually stored locally. This is largely due to the limited bandwidth typical of communications links between the SCADA central host computer and the field data interface devices. Such instructions are traditionally held within the PLCs, which have in the past been physically separate from RTUs. A PLC is a device used to automate monitoring and control of industrial facilities. It can be used as a stand-alone or in conjunction with a SCADA or other system. PLCs connect directly to field data interface devices and incorporate programmed intelligence in the form of logical procedures that will be executed in the event of certain field conditions.

PLCs have their origins in the automation industry and therefore are often used in manufacturing and process plant applications. The need for PLCs to connect to communication channels was not great in these applications, as they often were only required to replace traditional relay logic systems or pneumatic controllers. SCADA systems, on the other hand, have origins in early telemetry applications, where it was only necessary to know basic information from a remote source. The RTUs connected to these systems had no need for control programming because the local control algorithm was held in the relay switching logic.

As PLCs were used more often to replace relay switching logic control systems, telemetry was used more and more with PLCs at the remote sites. It became desirable to influence the program within the PLC through the use of a remote signal. This is in effect the "Supervisory Control" part of the acronym SCADA. Where only a simple local control program was required, it became possible to store this program within the RTU and perform the control within that device. At the same time, traditional PLCs included communications modules that would allow PLCs to report the state of the control program to a computer plugged into the PLC or to a remote computer via a telephone line. PLC and RTU manufacturers therefore compete for the same market.

As a result of these developments, the line between PLCs and RTUs has blurred and the terminology is virtually interchangeable. For the sake of simplicity, the term RTU will be used to refer to a remote field data interface device; however, such a device could include automation programming that traditionally would have been classified as a PLC.

## **2.2 Communications Network**

The communications network is intended to provide the means by which data can be transferred between the central host computer servers and the field-based RTUs. The Communication Network refers to the equipment needed to transfer data to and from different sites. The medium used can either be cable, telephone or radio.

The use of cable is usually implemented in a factory. This is not practical for systems covering large geographical areas because of the high cost of the cables, conduits and the extensive labor in installing them. The use of telephone lines (i.e., leased or dial-up) is a more economical solution for systems with large coverage. The leased line is used for systems requiring on-line connection with the remote stations. This is expensive since one telephone line will be needed per site. Dial-up lines can be used on systems requiring updates at regular intervals (e.g., hourly updates). Here ordinary telephone lines can be used. The host can dial a particular number of a remote site to get the readings and send commands.

Remote sites are usually not accessible by telephone lines. The use of radio offers an economical solution. Radio modems are used to connect the remote sites to the host. An on-line operation can also be implemented on the radio system. For locations where a direct radio link cannot be established, a radio repeater is used to link these sites.

Historically, SCADA networks have been dedicated networks; however, with the increased deployment of office LANs and WANs as a solution for interoffice computer networking, there exists the possibility to integrate SCADA LANs into everyday office computer networks.

The foremost advantage of this arrangement is that there is no need to invest in a separate computer network for SCADA operator terminals. In addition, there is an easy path to integrating SCADA data with existing office applications, such as spreadsheets, work management systems, data history databases, Geographic Information System (GIS) systems, and water distribution modeling systems.

## **2.3 Central Host Computer**

The central host computer or master station is most often a single computer or a network of computer servers that provide a man-machine operator interface to the SCADA system. The computers process the information received from and sent to the RTU sites and present it to human operators in a form that the operators can work with. Operator terminals are connected to the central host computer by a LAN/WAN so that the viewing

screens and associated data can be displayed for the operators. Recent SCADA systems are able to offer high resolution computer graphics to display a graphical user interface or mimic screen of the site or water supply network in question. Historically, SCADA vendors offered proprietary hardware, operating systems, and software that was largely incompatible with other vendors' SCADA systems. Expanding the system required a further contract with the original SCADA vendor. Host computer platforms characteristically employed UNIX-based architecture, and the host computer network was physically removed from any office-computing domain.

However, with the increased use of the personal computer, computer networking has become commonplace in the office and as a result, SCADA systems are now available that can network with office-based personal computers. Indeed, many of today's SCADA systems can reside on computer servers that are identical to those servers and computers used for traditional office applications. This has opened a range of possibilities for the linking of SCADA systems to office-based applications such as GIS systems, hydraulic modeling software, drawing management systems, work scheduling systems, and information databases.

## **2.4 Operator Workstations and Software Components**

Operator workstations are most often computer terminals that are networked with the SCADA central host computer. The central host computer acts as a server for the SCADA application, and the operator terminals are clients that request and send information to the central host computer based on the request and action of the operators.

An important aspect of every SCADA system is the computer software used within the system. The most obvious software component is the operator interface or Man Machine Interface/Human Machine Interface (MMI/HMI) package; however, software of some form pervades all levels of a SCADA system. Depending on the size and nature of the SCADA application, software can be a significant cost item when developing, maintaining, and expanding a SCADA system. When software is well defined, designed, written, checked, and tested, a successful SCADA system will likely be produced. Poor performances in any of these project phases will very easily cause a SCADA project to fail.

Many SCADA systems employ commercial proprietary software upon which the SCADA system is developed. The proprietary software often is configured for a specific hardware platform and may not interface with the software or hardware produced by competing vendors. A wide range of commercial off-the-shelf (COTS) software products also are available, some of which may suit the required application. COTS software usually is more flexible, and will interface with different types of hardware and software. Generally, the focus of proprietary software is on processes and control functionality, while COTS software emphasizes compatibility with a variety of equipment and instrumentation. It is therefore important to ensure that adequate planning is undertaken to select the software systems appropriate to any new SCADA system.

Software products typically used within a SCADA system are as follows:

- Central host computer operating system: Software used to control the central host computer hardware. The software can be based on UNIX or other popular operating systems.
- Operator terminal operating system: Software used to control the central host computer hardware. The software is usually the same as the central host computer operating system. This software, along with that for the central host computer, usually contributes to the networking of the central host and the operator terminals.
- Central host computer application: Software that handles the transmittal and reception of data to and from the RTUs and the central host. The software also provides the graphical user interface which offers site mimic screens, alarm pages, trend pages, and control functions.
- Operator terminal application: Application that enables users to access information available on the central host computer application. It is usually a subset of the software used on the central host computers.
- Communications protocol drivers: Software that is usually based within the central host and the RTUs, and is required to control the translation and interpretation of the data between ends of the communications links in the system. The protocol drivers prepare the data for use either at the field devices or the central host end of the system.
- Communications network management software: Software required to control the communications network and to allow the communications networks themselves to be monitored for performance and failures.
- RTU automation software: Software that allows engineering staff to configure and maintain the application housed within the RTUs (or PLCs). Most often this includes the local automation application and any data processing tasks that are performed within the RTU.

The preceding software products provide the building blocks for the application-specific software, which must be defined, designed, written, tested, and deployed for each SCADA system.

### **3.0 SCADA Architectures**

SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology. The following sections will provide a description of the following three generations of SCADA systems:

- First Generation – Monolithic
- Second Generation – Distributed
- Third Generation – Networked

#### **3.1 Monolithic SCADA Systems**

When SCADA systems were first developed, the concept of computing in general centered on “mainframe” systems. Networks were generally non-existent, and each centralized system stood alone. As a result, SCADA systems were standalone systems with virtually no connectivity to other systems.

The Wide Area Networks (WANs) that were implemented to communicate with remote terminal units (RTUs) were designed with a single purpose in mind—that of communicating with RTUs in the field and nothing else. In addition, WAN protocols in use today were largely unknown at the time.

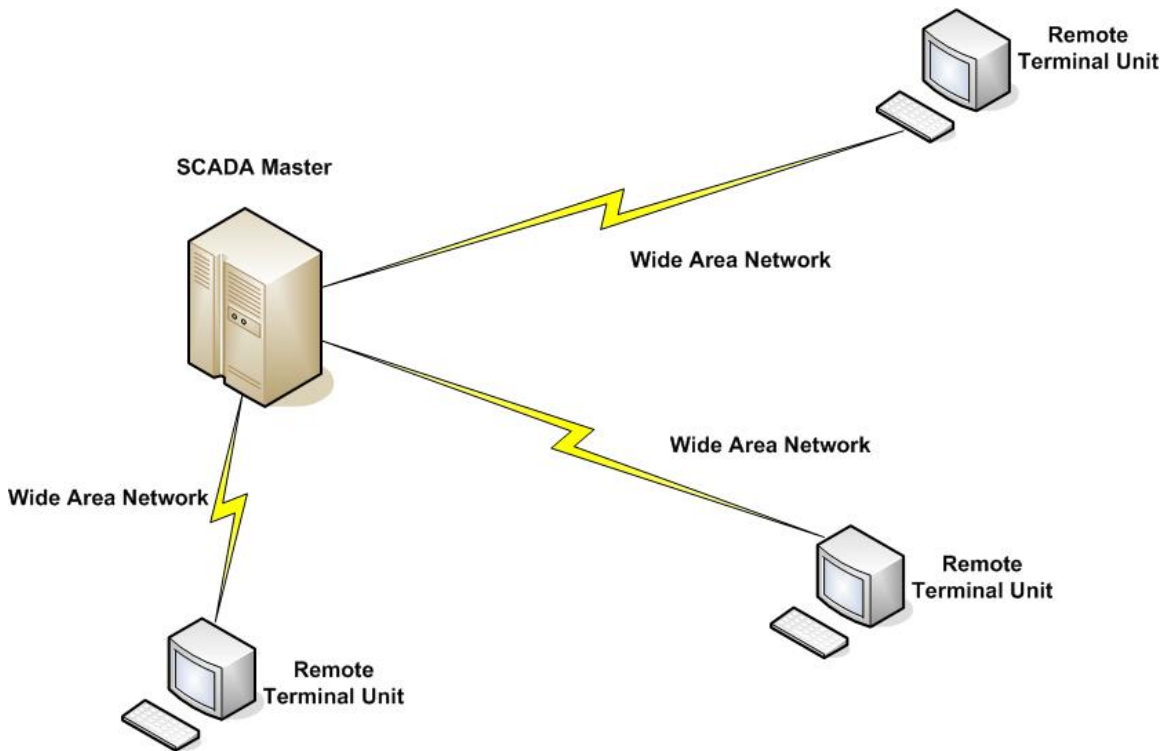
The communication protocols in use on SCADA networks were developed by vendors of RTU equipment and were often proprietary. In addition, these protocols were generally very “lean”, supporting virtually no functionality beyond that required scanning and controlling points within the remote device. Also, it was generally not feasible to intermingle other types of data traffic with RTU communications on the network.

Connectivity to the SCADA master station itself was very limited by the system vendor. Connections to the master typically were done at the bus level via a proprietary adapter or controller plugged into the Central Processing Unit (CPU) backplane.

Redundancy in these first generation systems was accomplished by the use of two identically equipped mainframe systems, a primary and a backup, connected at the bus level. The standby system’s primary function was to monitor the primary and take over in the event of a detected failure. This type of standby operation meant that little or no processing was done on the standby system. Figure 3.1 shows a typical first generation SCADA architecture.

#### **3.2 Distributed SCADA Systems**

The next generation of SCADA systems took advantage of developments and improvement in system miniaturization and Local Area Networking (LAN) technology to

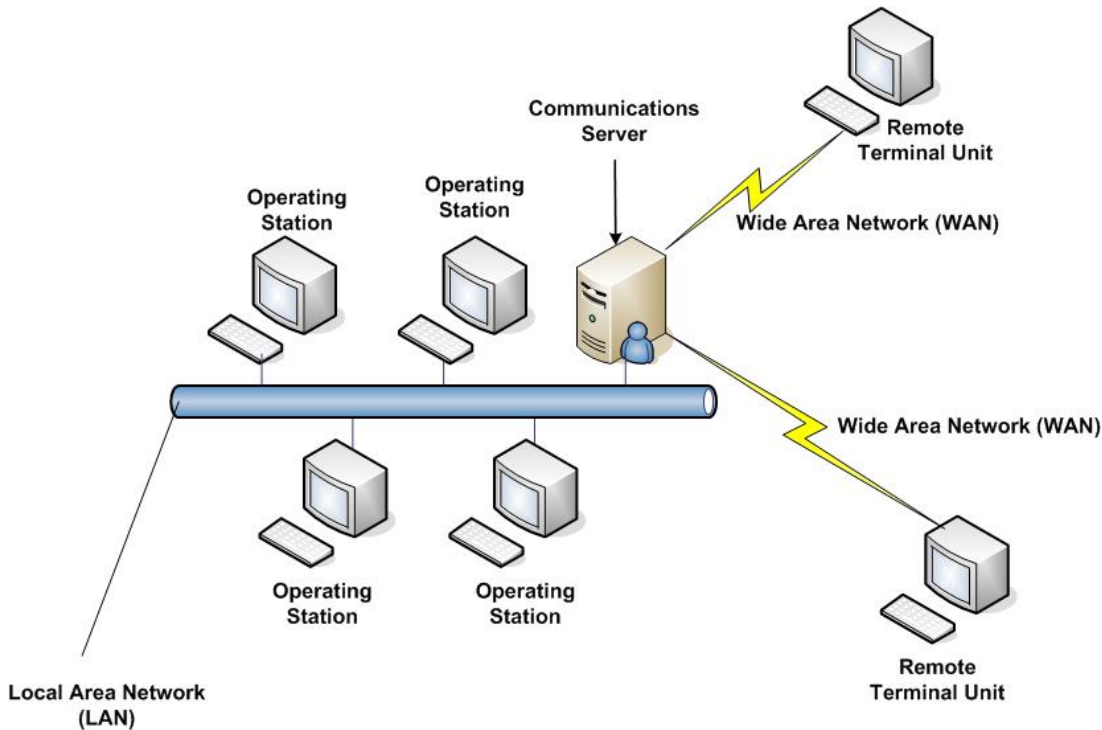


**Figure 3.1: First Generation SCADA Architecture [5]**

distribute the processing across multiple systems. Multiple stations, each with a specific function, were connected to a LAN and shared information with each other in real-time. These stations were typically of the mini-computer class, smaller and less expensive than their first generation processors.

Some of these distributed stations served as communications processors, primarily communicating with field devices such as RTUs. Some served as operator interfaces, providing the human-machine interface (HMI) for system operators. Still others served as calculation processors or database servers. The distribution of individual SCADA system functions across multiple systems provided more processing power for the system as a whole than would have been available in a single processor. The networks that connected these individual systems were generally based on LAN protocols and were not capable of reaching beyond the limits of the local environment.

Some of the LAN protocols that were used were of a proprietary nature, where the vendor created its own network protocol or version thereof rather than pulling an existing one off the shelf. This allowed a vendor to optimize its LAN protocol for real-time traffic, but it limited (or effectively eliminated) the connection of network from other vendors to the SCADA LAN. Figure 3.2 depicts typical second generation SCADA architecture.



**Figure 3.2: Second Generation SCADA Architecture [5]**

Distribution of system functionality across network-connected systems served not only to increase processing power, but also to improve the redundancy and reliability of the system as a whole. Rather than the simple primary/standby failover scheme that was utilized in many first generation systems, the distributed architecture often kept all stations on the LAN in an online state all of the time. For example, if an HMI station were to fail, another HMI station could be used to operate the system, without waiting for failover from the primary system to the secondary.

The WAN used to communicate with devices in the field were largely unchanged by the development of LAN connectivity between local stations at the SCADA master. These external communications networks were still limited to RTU protocols and were not available for other types of network traffic.

As was the case with the first generation of systems, the second generation of SCADA systems was also limited to hardware, software, and peripheral devices that were provided or at least selected by the vendor.

### 3.3 Networked SCADA Systems

The current generation of SCADA master station architecture is closely related to that of the second generation, with the primary difference being that of an open system architecture rather than a vendor controlled, proprietary environment. There are still multiple networked systems, sharing master station functions. There are still RTUs utilizing protocols that are vendor-proprietary. The major improvement in the third generation is that of opening the system architecture, utilizing open standards and

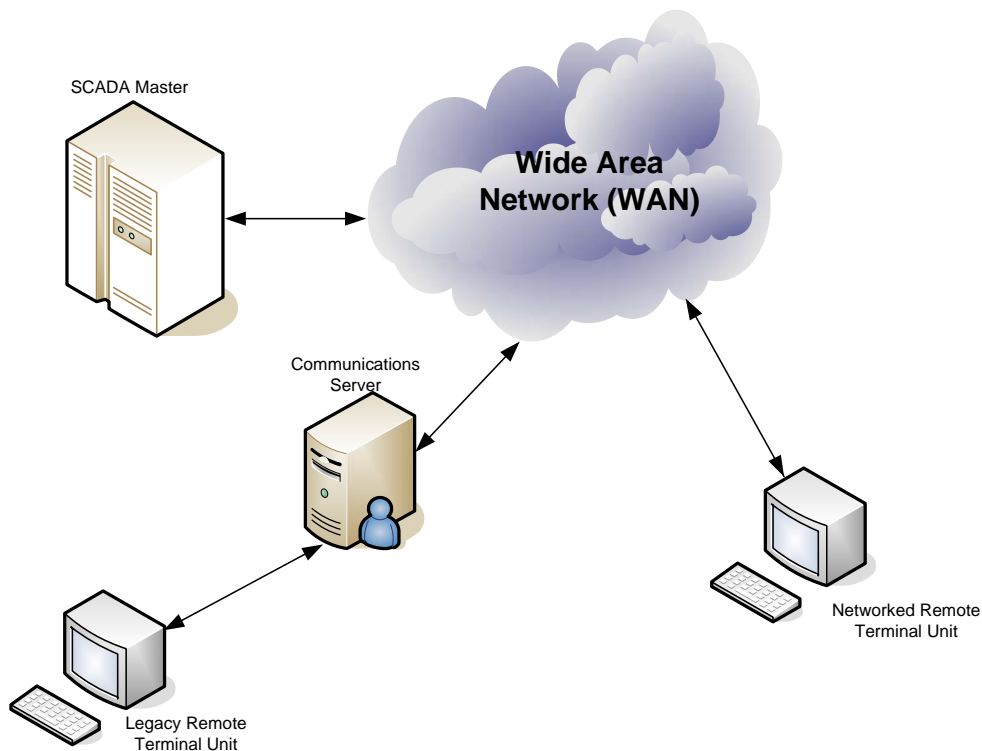


protocols and making it possible to distribute SCADA functionality across a WAN and not just a LAN.

Open standards eliminate a number of the limitations of previous generations of SCADA systems. The utilization of off-the-shelf systems makes it easier for the user to connect third party peripheral devices (such as monitors, printers, disk drives, tape drives, etc.) to the system and/or the network.

As they have moved to “open” or “off-the-shelf” systems, SCADA vendors have gradually gotten out of the hardware development business. These vendors have looked to system vendors such as Compaq, Hewlett-Packard, and Sun Microsystems for their expertise in developing the basic computer platforms and operating system software. This allows SCADA vendors to concentrate their development in an area where they can add specific value to the system—that of SCADA master station software.

The major improvement in third generation SCADA systems comes from the use of WAN protocols such as the Internet Protocol (IP) for communication between the master station and communications equipment. This allows the portion of the master station that is responsible for communications with the field devices to be separated from the master station “proper” across a WAN. Vendors are now producing RTUs that can communicate with the master station using an Ethernet connection. Figure 3.3 represents a networked SCADA system.



**Figure 3.3: Third Generation SCADA System [5]**

Another advantage brought about by the distribution of SCADA functionality over a WAN is that of disaster survivability. The distribution of SCADA processing across a LAN in second-generation systems improves reliability, but in the event of a total loss of the facility housing the SCADA master, the entire system could be lost as well. By distributing the processing across physically separate locations, it becomes possible to build a SCADA system that can survive a total loss of any one location. For some organizations that see SCADA as a super-critical function, this is a real benefit.

## **4.0 SCADA Protocols**

In a SCADA system, the RTU accepts commands to operate control points, sets analog output levels, and responds to requests. It provides status, analog and accumulated data to the SCADA master station. The data representations sent are not identified in any fashion other than by unique addressing. The addressing is designed to correlate with the SCADA master station database. The RTU has no knowledge of which unique parameters it is monitoring in the real world. It simply monitors certain points and stores the information in a local addressing scheme. The SCADA master station is the part of the system that should “know” that the first status point of RTU number 27 is the status of a certain circuit breaker of a given substation. This represents the predominant SCADA systems and protocols in use in the utility industry today.

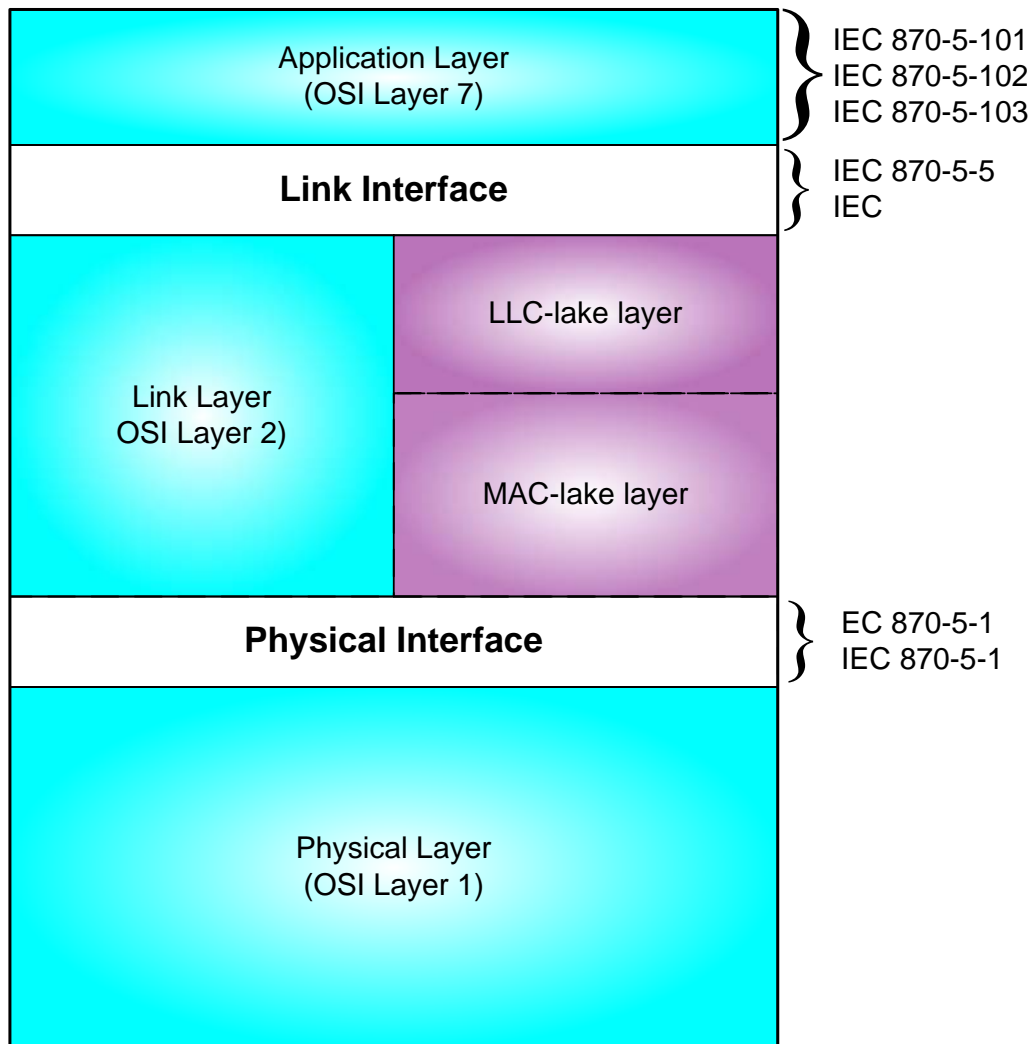
Each protocol consists of two message sets or pairs. One set forms the master protocol, containing the valid statements for master station initiation or response, and the other set is the RTU protocol, containing the valid statements an RTU can initiate and respond to. In most but not all cases, these pairs can be considered a poll or request for information or action and a confirming response.

The SCADA protocol between master and RTU forms a viable model for RTU-to-Intelligent Electronic Device (IED) communications. Currently, in industry, there are several different protocols in use. The most popular are International Electrotechnical Commission (IEC) 60870-5 series, specifically IEC 60870-5-101 (commonly referred to as 101) and Distributed Network Protocol version 3 (DNP3).

### **4.1 IEC 60870-5-101**

IEC 60870-5 specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer Enhanced Performance Architecture (EPA) reference model (see Figure 4.1) for efficient implementation within RTUs, meters, relays, and other Intelligent Electronic Devices (IEDs). Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the Open System Interconnection (OSI) application layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set.

Standard profiles are necessary for uniform application of the IEC 60870-5 standards. A profile is a set of parameters defining the way a device acts. Such profiles have been and are being created. The 101 profile is described in detail following the description of the applicable standards.



**Figure 4.1: Enhanced Performance Architecture**

- IEC 60870-5-1 (1990-02) specifies the basic requirements for services to be provided by the data link and physical layers for telecontrol applications. In particular, it specifies standards on coding, formatting, and synchronizing data frames of variable and fixed lengths that meet specified data integrity requirements.
- IEC-60870-5-2 (1992-04) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because some point-to-point topologies do not require either source or destination addressing.
- IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic standards that may be used to support a great variety of present and future telecontrol applications. This section of IEC 60870-5 describes the general structure of

application data and basic rules to specify application data units without specifying details about information fields and their contents.

- IEC 60870-5-4 (1993-08) provides rules for defining information data elements and a common set of information elements, particularly digital and analog process variables that are frequently used in telecontrol applications.
- IEC 60870-5-5 (1995-06) defines basic application functions that perform standard procedures for telecontrol systems, which are procedures that reside beyond layer 7 (application layer) of the ISO reference model. These utilize standard services of the application layer. The specifications in IEC 60870-5-5 (1995-06) serve as basic standards for application profiles that are then created in detail for specific telecontrol tasks.

Each application profile will use a specific selection of the defined functions. Any basic application functions not found in a standards document but necessary for defining certain telecontrol applications should be specified within the profile. Examples of such telecontrol functions include station initialization, cyclic data transmission, data acquisition by polling, clock synchronization, and station configuration.

The Standard 101 Profile provides structures that are also directly applicable to the interface between RTUs and IEDs. It contains all the elements of a protocol necessary to provide an unambiguous profile definition so vendors may create products that interoperate fully.

At the physical layer, the Standard 101 Profile additionally allows the selection of International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standards that are compatible with Electronic Industries Association (EIA) standards RS-232<sup>1</sup> and RS-485<sup>2</sup>, and also support fiber optics interfaces.

The Standard 101 Profile specifies frame format FT 1.2, chosen from those offered in IEC 60870-5-1 (1990-02) to provide the required data integrity together with the maximum efficiency available for acceptable convenience of implementation. FT 1.2 is basically asynchronous and can be implemented using standard Universal Asynchronous Receiver/Transmitters (UARTs). Formats with both fixed and variable block length are permitted.

At the data link layer, the Standard 101 Profile specifies whether an unbalanced (includes multi-drop) or balanced (includes point-to-point) transmission mode is used together with which link procedures (and corresponding link function codes) are to be used. Also specified is an unambiguous number (address) for each link.

The link transmission procedures selected from IEC 60870-5-2 (1992-04) specify that SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPOND message transactions should be supported as necessary for the functionality of the end device. Additionally,

---

<sup>1</sup> Interface Between Data Terminal Equipment

<sup>2</sup> Electrical Characteristics Of Generators And Receivers For Use In Balanced Digital Multipoint Systems

The Standard 101 Profile defines the necessary rules for devices that will operate in the unbalanced (multi-drop) and balanced (point-to-point) transmission modes.

The Standard 101 Profile defines appropriate Application Service Data Units (ASDUs) from a given general structure in IEC 60870-5-3 (1992-09). The sizes and the contents of individual information fields of ASDUs are specified according to the declaration rules for information elements defined in the document IEC 60870-5-4 (1993-08).

Type information defines structure, type, and format for information object(s), and a set has been predefined for a number of information objects. The predefined information elements and type information do not preclude the addition by vendors of new information elements and types that follow the rules defined by IEC 60870-5-4 (1993-08) and the Standard 101 Profile. Information elements in the Standard 101 Profile have been defined for protection equipment, voltage regulators, and metered values to interface these devices as IEDs to the RTU.

The Standard 101 Profile utilizes the following basic application functions, defined in IEC 60870-5-5 (1995-06), within the user layer:

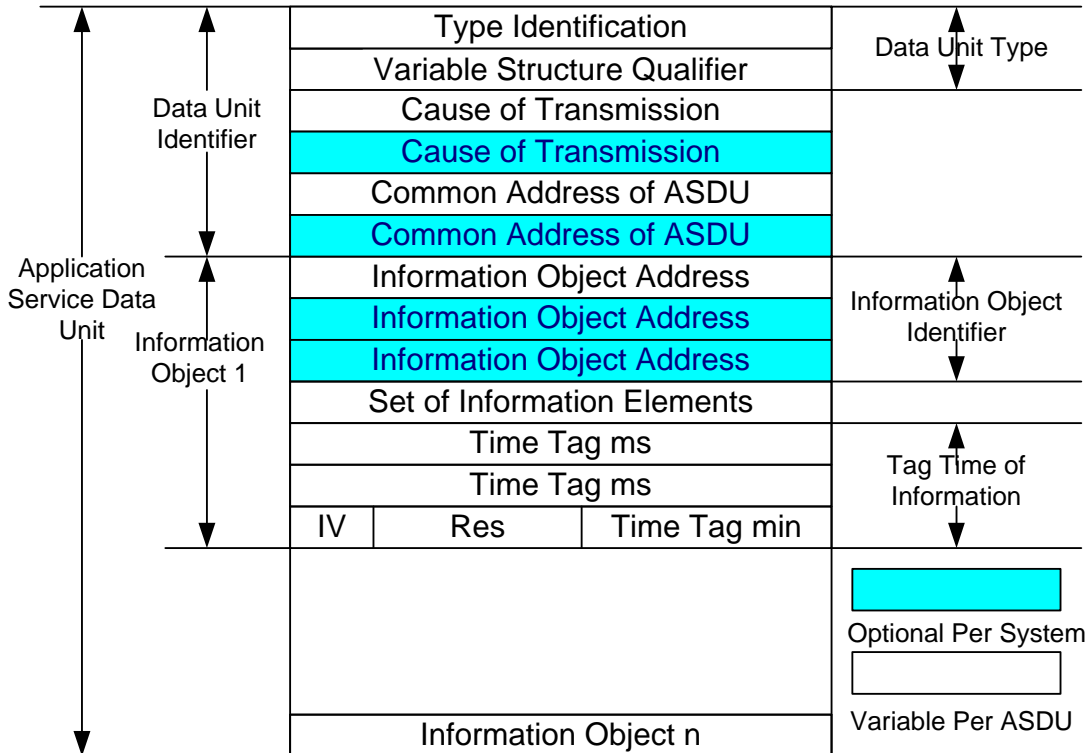
- a) Station initialization
- b) Cyclic data transmission
- c) General interrogation
- d) Command transmission
- e) Data acquisition by polling
- f) Acquisition of events
- g) Parameter loading
- h) File transfer
- i) Clock synchronization
- j) Transmission of integrated totals
- k) Test procedure

Finally, the Standard 101 Profile defines parameters that support interoperability among multi-vendor devices within a system. These parameters are defined in 60870-5-102 and 60870-5-105. [6] The Standard 101 Profile provides a checklist that vendors can use to describe their devices from a protocol perspective. These parameters include baud rate, common address of ASDU field length, link transmission procedure, basic application functions, etc., Also contained in the check list is the information that should be contained in the ASDU in both the control and monitor directions. This will assist the SCADA engineers to configure their particular system.

The Standard 101 Profile application layer specifies the structure of the ASDU, as shown in Figure 4.1. The fields indicated as being optional per system will be determined by a system level parameter shared by all devices in the system. For instance, the size of the

common address of ASDU is determined by a fixed system parameter, in this case one or two octets (bytes).

The Standard 101 Profile also defines two new terms not found in the IEC 60870-5-1 through 60870-5 base documents. The control direction refers to transmission from the controlling station to a controlled station. The monitor direction is the direction of transmission from a controlled station to the controlling station. Figure 4.2 shows the structure of ASDUs as defined in the IEC 60870-5-101 specification.



Data Unit Identifier:=CP16+8a+8b (Type Identification, Variable Structure Qualifier, Cause of Transmission, Common Address)  
 Fixed system parameter a:=number of octets of Common Address (1 or 2)  
 Fixed system parameter b:=number of octets of Cause of Transmission (1 or 2)  
 Information Object:=CPSc+8j+8t (Information Object Address, Set of Information Elements, Time Tag (opt.))  
 Fixed system parameter c:=number of octets of Set of Addresses (1, 2 or 3)  
 Variable parameter j:=number of octets of Set of Information Elements  
 Variable parameter t:=3 if Time Tag is present, 0 if Time Tag is not present

**Figure 4.2: Structure of ADSUs in IEC 60870-5-101 (1995-11) [6]**

## 4.2 DNP3

Protocols define the rules by which devices talk with each other, and DNP3 is a protocol for transmission of data from point A to point B using serial communications. It has been

used primarily by utilities like the electric companies, but it operates suitably in other areas.

The DNP3 is specifically developed for inter-device communication involving SCADA RTUs, and provides for both RTU-to-IED and master-to-RTU/IED. It is based on the three-layer enhanced performance architecture (EPA) model contained in the IEC 60870-5 standards, with some alterations to meet additional requirements of a variety of users in the electric utility industry.

DNP3 was developed with the following goals:

- *High data integrity.* The DNP3 data link layer uses a variation of the IEC 60870-5-1 (1990-02) frame format FT3. Both data link layer frames and application layer messages may be transmitted using confirmed service.
- *Flexible structure.* The DNP3 application layer is object-based, with a structure that allows a range of implementations while retaining interoperability.
- *Multiple applications.* DNP3 can be used in several modes, including:
  1. Polled only
  2. Polled report-by-exception
  3. Unsolicited report-by-exception (quiescent mode)
  4. Mixture of modes 1. through 3.

It can also be used with several physical layers, and as a layered protocol is suitable for operation over local and some wide area networks.

- *Minimized overhead.* DNP3 was designed for existing wire-pair data links with operating bit rates as low as 1200 bit/s and attempts to use a minimum of overhead while retaining flexibility. Selection of a data reporting method, such as report-by-exception, further reduces overhead.
- *Open standard.* DNP3 is a non-proprietary, evolving standard controlled by a users group whose members include RTU, IED, and master station vendors, and representatives of the electric utility and system consulting community.

A typical organization may have a centralized operations center that monitors the state of all the equipment in each of its substations. In the operations center, a computer stores all of the incoming data and displays the system for the human operators. Substations have many devices that need monitoring (are circuit breakers opened or closed?), current sensors (how much current is flowing?) and voltage transducers (what is the line potential?). That only scratches the surface; a utility is interested in monitoring many parameters, too numerous to discuss here. The operations personnel often need to switch sections of the power grid into or out of service. One or more computers are situated in the substation to collect the data for transmission to the master station in the operations center. The substation computers are also called upon to energize or de-energize the breakers and voltage regulators.



DNP3 provides the rules for substation computers and master station computers to communicate data and control commands. DNP3 is a non-proprietary protocol that is available to anyone. Only a nominal fee is charged for documentation, but otherwise it is available worldwide with no restrictions. This means a utility can purchase master station and substation computing equipment from any manufacturer and be assured that they will reliably talk to each other. Vendors compete based upon their computer equipment's features, costs and quality factors instead of who has the best protocol. Utilities are not stuck with one manufacturer after the initial sale.

The substation computer gathers data for transmission to the master such as:

- Binary input data that is useful to monitor two-state devices. For example, a circuit breaker is closed or tripped, or a pipeline pressure alarm shows normal or excessive.
- Analog input data that conveys voltages, currents, power, reservoir water levels and temperatures
- Count input data that reports kilowatt hours of energy
- Files that contain configuration data

The master station issues control commands that take the form of:

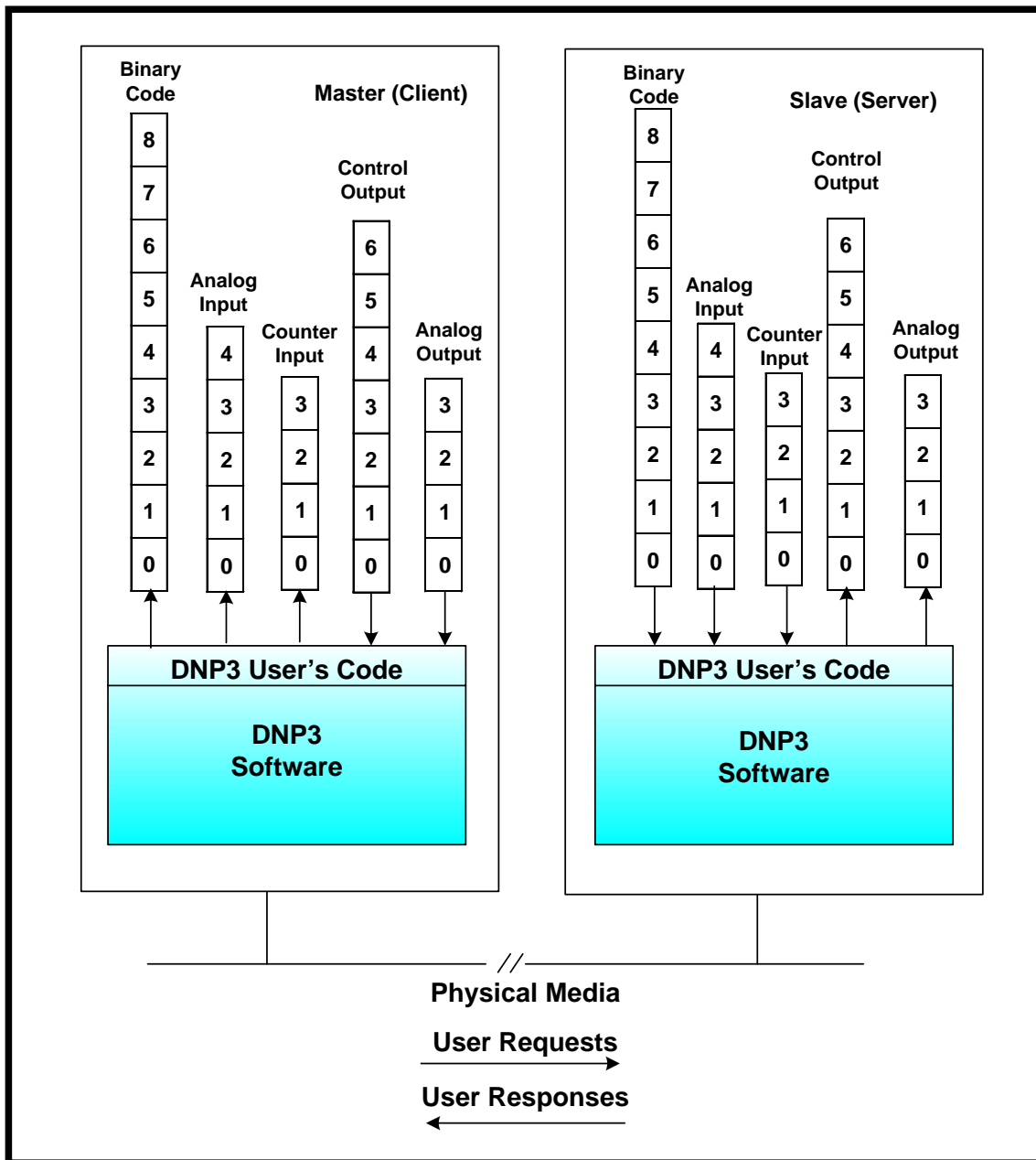
- Close or trip a circuit breaker, raise or lower a gate, and open or close a valve
- Analog output values to set a regulated pressure or set a desired voltage level

Other things the computers talk to each other about are synchronizing the time and date, sending historical or logged data, waveform data, etc.

DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. It is not a general purpose protocol for transmitting hypertext, multimedia or huge files.

Figure 4.3 shows the client-server relationship and gives a simplistic view of the databases and software processes involved. The master or client is on the left side of Figure 4.3, and the slave or server is on the right side.

A series of square blocks at the top of the server depicts its databases and output devices. The various data types are conceptually organized as arrays. An array of binary input values represents states of physical or logical Boolean devices. Values in the analog input array represent input quantities that the server measured or computed. An array of counters represents count values, such as kilowatt hours, that are ever increasing (until they reach a maximum and then roll over to zero and start counting again). Control outputs are organized into an array representing physical or logical on-off, raise-lower and trip-close points. Lastly, the array of analog outputs represents physical or logical analog quantities such as those used for setpoints.



**Figure 4.3: DNP3 Client Server Relationship [7]**

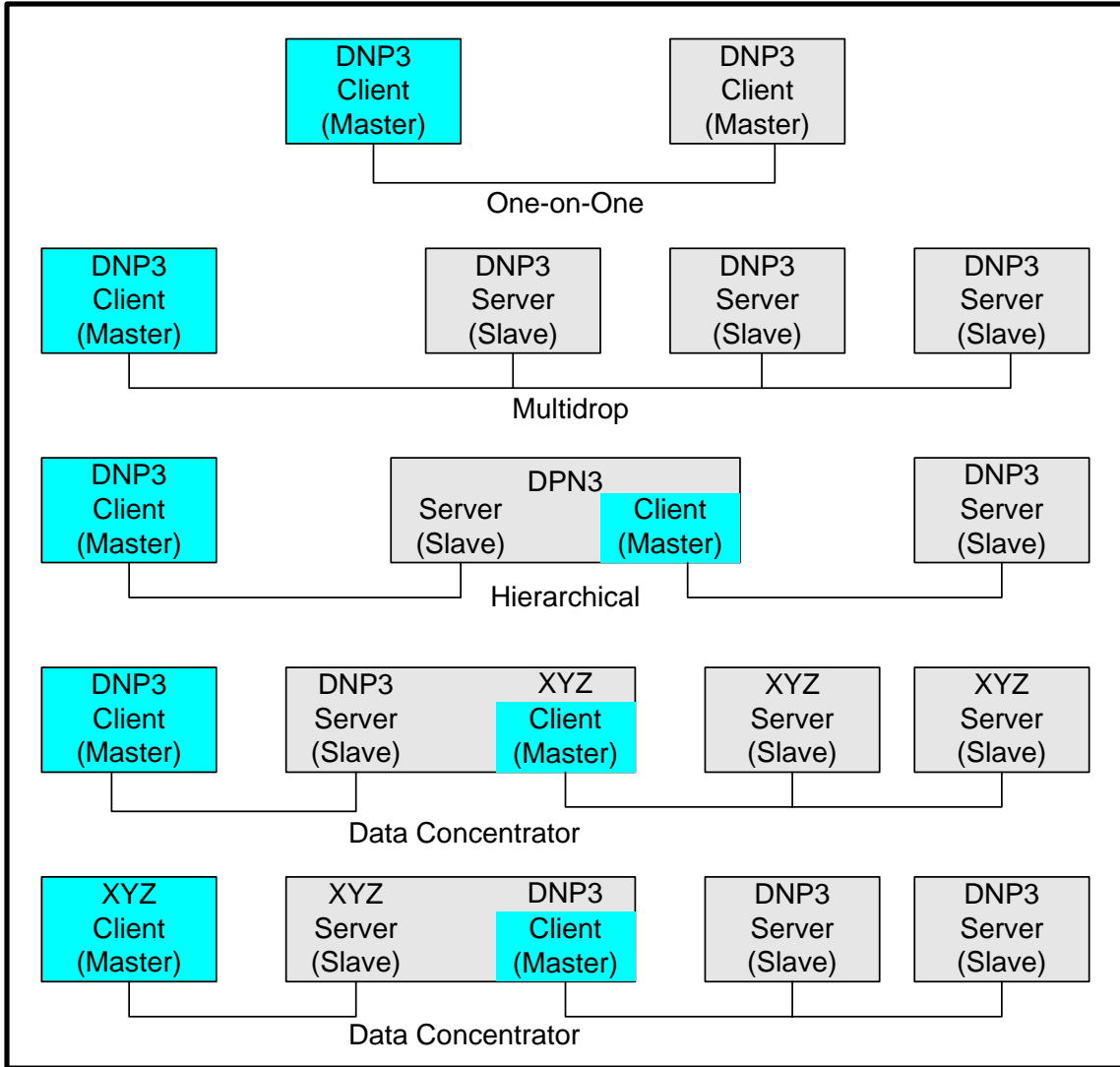
The elements of the arrays are labeled 0 through N - 1 where N is the number of blocks shown for the respective data type. In DNP3 terminology, the element numbers are called the point indexes. Indexes are zero-based in DNP3, that is, the lowest element is always identified as zero (some protocols use 1-based indexing).

Notice that the DNP3 client, or master, also has a similar database for the input data types (binary, analog and counter). The master, or client, uses values in its database for the specific purposes of displaying system states, closed-loop control, alarm notification,

billing, etc. An objective of the client is to keep its database updated. It accomplishes this by sending requests to the server (slave) asking it to return the values in the server's database. This is termed polling. The server responds to the client's request by transmitting the contents of its database. Arrows are drawn at the bottom of Figure 4.1 showing the direction of the requests (toward the server) and the direction of the responses (toward the client). Later we will discuss systems whereby the slaves transmit responses without being asked.

The client and the server shown in Figure 4.3 each have two software layers. The top layer is the DNP3 user layer. In the client, it is the software that interacts between the database and initiates the requests for the server's data. In the server, it is the software that fetches the requested data from the server's database for responding to client requests. It is interesting to note that if no physical separation of the client and server existed, eliminating the DNP3 might be possible by connecting these two upper layers together. However, since physical or possibly logical separation of the client and server exists, DNP3 software is placed at a lower level. The DNP3 user's code uses the DNP3 software for transmission of requests or responses to the matching DNP3 user's code at the other end.

Data types and software layers will be discussed later in the report. However, it is important to first examine a few typical system architectures where DNP3 is used. Figure 4.4 shows common system architectures in use today. At the top is a simple one-on-one system having one master station and one slave. The physical connection between the two is typically a dedicated or dial-up telephone line.



**Figure 4.4: Common DNP3 Architectures in Use Today [7]**

The second type of system is known as a multidrop design. One master station communicates with multiple slave devices. Conversations are typically between the client and one server at a time. The master requests data from the first slave, then moves onto the next slave for its data, and continually interrogates each slave in a round robin order. The communication media is a multi-dropped telephone line, fiber optic cable, or radio. Each slave can hear messages from the master and is only permitted to respond to messages addressed to itself. Slaves may or may not be able to hear each other.

In some multidrop forms, communications are peer-to-peer. A station may operate as a client for gathering information or sending commands to the server in another station. Then, it may change roles to become a server to another station.

The middle row in Figure 4.4 shows a hierarchical type system where the device in the middle is a server to the client at the left and is a client with respect to the server on the right. The middle device is often termed a sub-master.

Both lines at the bottom of Figure 4.4 show data concentrator applications and protocol converters. A device may gather data from multiple servers on the right side of the figure and store this data in its database where it is retrievable by a master station client on the left side of the figure. This design is often seen in substations where the data concentrator collects information from local intelligent devices for transmission to the master station.

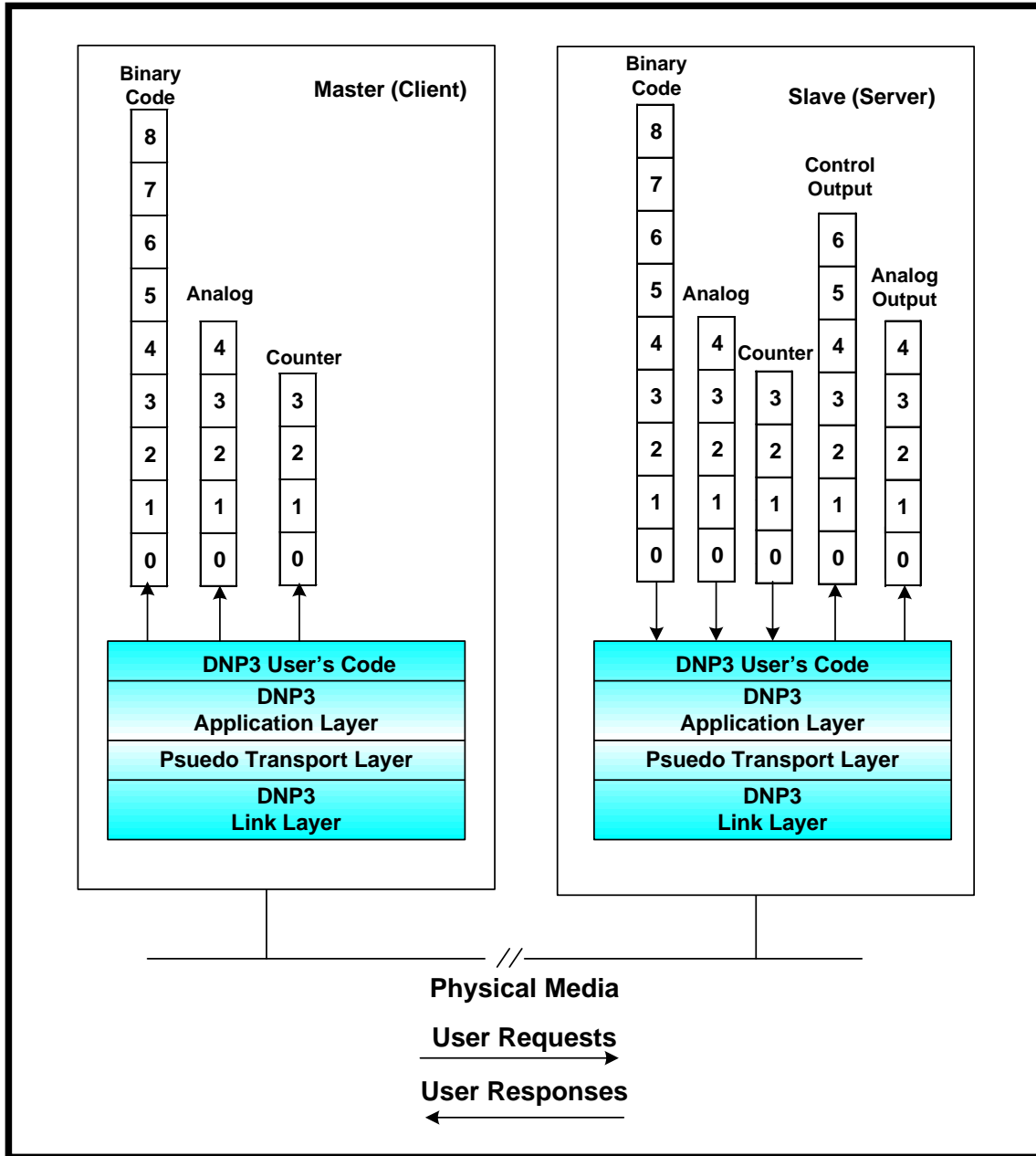
In recent years, several vendors have used Transport Control Protocol/Internet Protocol (TCP/IP) to transport DNP3 messages in lieu of the media discussed above. Link layer frames, which have not been discussed yet, are embedded into TCP/IP packets. This approach has enabled DNP3 to take advantage of Internet technology and permitted economical data collection and control between widely separated devices.

Many communication circuits between the devices are susceptible to noise and signal distortion. The DNP3 software is layered to provide reliable data transmission and to affect an organized approach to the transmission of data and commands. Figure 4.5 shows the DNP3 architecture layers.

The link layer has the responsibility of making the physical link reliable. It does this by providing error detection and duplicate frame detection. The link layer sends and receives packets, which in DNP3 terminology are called frames. Sometimes transmission of more than one frame is necessary to transport all of the information from one device to another. A DNP3 frame consists of a header and data section. The header specifies the frame size, which DNP3 station should receive the frame, which DNP3 device sent the frame, and data link control information. The data section is commonly called the payload and contains the data passed down from the layers above.

Every frame begins with two sync bytes that help the receivers determine where the frame begins. The length specifies the number of octets in the remainder of the frame, not including Cyclical Redundancy Check (CRC) octets. The link control octet is used between sending and receiving link layers to coordinate their activities.

A destination address specifies which DNP3 device should process the data, and the source address identifies which DNP3 device sent the message. Having both destination and source addresses satisfies at least one requirement for peer-to-peer communications because the receiver knows where to direct its responses. Every DNP3 device must have a unique address within the collection of devices sending and receiving messages to and from each other. Three destination addresses are reserved by DNP3 to denote an all-call message; that is, all DNP3 devices should process the frame. Thirteen addresses are reserved for special needs in the future.



**Figure 4.5: DNP3 Layers [8]**

The data payload in the link frame contains a pair of CRC octets for every 16 data octets. This provides a high degree of assurance that communication errors can be detected. The maximum number of octets in the data payload is 250, not including CRC octets. (The longest link layer frame is 292 octets if all the CRC and header octets are counted).

One often hears the term “link layer confirmation” when DNP3 is discussed. A feature of DNP3's link layer is the ability of the transmitter of the frame to request the receiver to confirm that the frame arrived. Using this feature is optional, and it is often not employed. It provides an extra degree of assurance of reliable communications. If a

confirmation is not received, the link layer may retry the transmission. Some disadvantages are the extra time required for confirmation messages and waiting for multiple timeouts when retries are configured.

It is the responsibility of the transport layer to break long messages into smaller frames sized for the link layer to transmit, or when receiving, to reassemble frames into the longer messages. In DNP3 the transport layer is incorporated into the application layer. The transport layer requires only a single octet within the message to do its work. Therefore, since the link layer can handle only 250 data octets, and one of those is used for the transport function, then each link layer frame can hold as many as 249 application layer octets.

Application layer messages are broken into fragments. Fragment size is determined by the size of the receiving device's buffer. It normally falls between 2048 and 4096 bytes. A message that is larger than one fragment requires multiple fragments. Fragmenting messages is the responsibility of the application layer.

Note that an application layer fragment of size 2048 must be broken into 9 frames by the transport layer, and a fragment size of 4096 needs 17 frames. Interestingly, it has been learned by experience that communications are sometimes more successful for systems operating in high noise environments if the fragment size is significantly reduced.

The application layer works together with the transport and link layers to enable reliable communications. It provides standardized functions and data formatting with which the user layer above can interact. Before functions, data objects and variations can be discussed, the terms static, events and classes need to be covered.

In DNP3, the term static is used with data and refers to the current value. Thus static binary input data refers to the present on or off state of a bi-state device. Static analog input data contains the value of an analog value at the instant it is transmitted. DNP3 allows a request for some or all of the static data stored in a slave device.

DNP3 events are associated with something significant happening. Examples are state changes, values exceeding some threshold, snapshots of varying data, transient data and newly available information. An event occurs when a binary input changes from an "on" to an "off" state or when an analog value changes by more than its configured deadband limit. DNP3 provides the ability to report events with and without time stamps so that the client can generate a time sequence report.

The user layer can direct DNP3 to request events. Usually, a client is updated more rapidly if it mostly polls for events from the server and only occasionally asks for static data as an integrity measure. The reason updates are faster is because the number of events generated between server interrogations is small and, therefore, less data must be returned to the client.

DNP3 goes a step further by classifying events into three classes. When DNP3 was conceived, class 1 events were considered as having higher priority than class 2 events, and class 2 were higher than class 3 events. While that scheme can be still be configured, some DNP3 users have developed other strategies more favorable to their operation for assigning events into the classes. The user layer can request the application layer to poll for class 1, 2 or 3 events or any combination of them.

DNP3 has provisions for representing data in different formats. Examination of analog data formats is helpful to understand the flexibility of DNP3. Static, current value, analog data can be represented by variation numbers as follows:

- A 32-bit integer value with flag
- A 16-bit integer value with flag
- A 32-bit integer value
- A 16-bit integer value
- A 32-bit floating point value with flag
- A 64-bit floating point value with flag

The flag referred to is a single octet with bit fields indicating whether the source is on-line, value contains are start value, communications are lost with the source, the data is forced and the value is over range.

Not all DNP3 devices can transmit or interpret all six variations. DNP3 devices must be able to transmit the simplest variations so that any receiver can interpret the contents.

Event analog data can be represented by these variations:

- A 32-bit integer value with flag
- A 16-bit integer value with flag
- A 32-bit integer value with flag and event time
- A 16-bit integer value with flag and event time
- A 32-bit floating point value with flag
- A 64-bit floating point value with flag
- A 32-bit floating point value with flag and event time
- A 32-bit floating point value with flag and event time

The flag has the same bit fields as the static variations.

It looks like a variation one or two analog events cannot be differentiated from a variation one or two static analog value. DNP3 solves this predicament by assigning object



numbers. Static analog values are assigned as object 30, and event analog values are assigned as object 32. Static analog values, object 30, can be formatted in one of 6 variations, and event analog values, object 32, can be formatted in one of 8 variations.

When a DNP3 server transmits a message containing response data, the message identifies the object number and variation of every value within the message. Object and variation numbers are also assigned for counters, binary inputs, controls and analog outputs. In fact, all valid data types and formats in DNP3 are identified by object and variation numbers. Defining the allowable objects and variations helps DNP3 assure interoperability between devices. DNP3's basic documentation contains a library of valid objects and their variations.

The client's user layer formulates its request for data from the server by telling the application layer what function to perform, like reading, and specifying which objects it wants from the server. The request can specify how many objects it wants or it can specify specific objects or a range of objects from index number X through index number Y. The application layer then passes the request down through the transport layer to the link layer that, in turn, sends the message to the server. The link layer at the server checks the frames for errors and passes them up to the transport layer where the complete message is assembled in the server's application layer. The application layer then tells the user layer which objects and variations were requested.

Responses work similarly, in that, the server's user layer fetches the desired data and presents it to the application layer that formats the data into objects and variations. Data is then passed downward, across the communication channel and upward to the client's application layer. Here the data objects are presented to the user layer in a form that is native to the client's database.

One area that has not been covered yet is transmission of unsolicited messages. This is a mode of operating where the server spontaneously transmits a response, possibly containing data, without having received a specific request for the data. Not all servers have this capability, but those that do must be configured to operate in this mode. This mode is useful when the system has many slaves and the master requires notification as soon as possible after a change occurs. Rather than waiting for a master station polling cycle to get around to it, the slave simply transmits the change.

To configure a system for unsolicited messages, a few basics need to be considered. First, spontaneous transmissions should generally occur infrequently, otherwise, too much contention can occur, and controlling media access via master station polling would be better. The second basic issue is that the server should have some way of knowing whether it can transmit without stepping on someone else's message in progress. DNP3 leaves specification of algorithms to the system implementer.

One last area of discussion involves implementation levels. The DNP3 Users Group recognizes that supporting every feature of DNP3 is not necessary for every device. Some devices are limited in memory and speed and do not need specific features, while other

devices must have the more advanced features to accomplish their task. DNP3 organizes complexity into three levels. At the lowest level, level 1, only very basic functions must be provided and all others are optional. Level 2 handles more functions, objects and variations, and level 3 is even more sophisticated. As a result only certain combinations of request formats and response formats are required.

DNP3 is a protocol that fits well into the data acquisition world. It transports data as generic values, has a rich set of functions, and was designed to work in a wide area communications network. The standardized approach and public availability make DNP3 a protocol to be the standard for SCADA applications.

## 5.0 Deploying SCADA Systems

There are many different ways in which SCADA systems can be implemented. Before a SCADA or any other system is rolled out, you need to determine what function the system will perform. Depending on whether you are a utility company or a telecommunications provider, you have a number of options in creating your systems. There may be a need to employ different methods that are complimentary to each other.

The way in which SCADA systems are connected can range from fiber optic cable to the use of satellite systems. The following sections will present some of the common ways in which SCADA systems are deployed. We will also look at their advantages and disadvantages.

### 5.1 Twisted-Pair Metallic Cable

Twisted-pair telecommunications cable is the most popular medium used by utilities and has existed in its present form for many years. The cables are essentially the same as those used by the Telephone Company and contain a number of pairs of conductor.

Aerial cables would be more appropriate for installation in the utility's service area since the Utility may own a large number of distribution poles from which the cables could be suspended. The smallest aerial cables can be self-supporting, whereas large aerial cables have to be attached to supporting wires (messengers) by lashing wire. Table 5.1 shows the Twisted-Pair Cable advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"><li>• No licensing, fewer approvals</li><li>• Existing pole Infrastructure</li><li>• Economical for short distances</li><li>• Relatively high channel capacity (up to 1.54 MHz) for short distances</li></ul>	<ul style="list-style-type: none"><li>• Right-of-way clearance required for buried cable</li><li>• Subject to breakage</li><li>• Subject to water ingress</li><li>• Subject to ground potential rise due to power faults and lightning</li><li>• Failures may be difficult to pinpoint</li><li>• Inflexible Network Configuration</li></ul>

**Table 5.1: Twisted-Pair Advantages/Disadvantages [8]**

### 5.2 Coaxial Metallic Cable

Coaxial cable is constructed of a center copper conductor, polyvinyl chloride (PVC) insulation, a braided or extruded copper shield surrounding the center conductor and PVC insulation, and a plastic jacket cover. Coaxial cable can transmit high frequency signals up to several MHz with low attenuation compared to twisted pair wires used for telephone service. Methods of installation used for existing systems in Europe and the USA are underground, direct burial, overhead, and on existing power line structures.

Services usually supported are voice, data, and interoffice trunking. Table 5.2 shows the Coaxial Cable advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• No licensing, fewer approvals</li> <li>• Existing pole Infrastructure</li> <li>• Economical for short distances</li> <li>• Higher channel capacity than Twisted-Pair Metallic</li> <li>• More immune to Radio Frequency (RF) noise interference the Twisted Pair Metallic</li> </ul>	<ul style="list-style-type: none"> <li>• Right-of-way clearance required for buried cable</li> <li>• Subject to breakage</li> <li>• Subject to water ingress</li> <li>• Subject to ground potential rise due to power faults and lightning</li> <li>• Failures may be difficult to pinpoint</li> <li>• Inflexible Network Configuration</li> </ul>

**Table 5.2: Coaxial Cable Advantages/Disadvantages [8]**

### 5.3 Fiber Optic Cable

Fiber optic technology has improved considerably since its inception in 1970. The technology has improved to the point where commercially available fibers have losses less than 0.3 dB/km. Losses of this magnitude, as well as the development of suitable lasers and optical detectors, allow designers to consider fiber optic technologies for systems of 140 km or more without repeaters.

Optical fibers consist of an inner core and cladding of silica glass and a plastic jacket that physically protects the fiber. Two types of fibers are usually considered: multi-mode graded index and single-mode step index fiber. Single-mode fiber supports higher signaling speeds than the multi-mode fiber due to its smaller diameter and mode of light propagation. Communication services usually supported by optical fiber include voice, data (low speed), SCADA, protective relaying, telemetering, video conferencing, high-speed data, and telephone switched tie trunks. Optical fiber cables have similar characteristics to twisted-pair communications cables in that aluminum tape or steel-wire armors and polyethylene outer jackets can protect them. However, the inner core is constructed to accommodate the mechanical characteristics of the fibers. Typically, the fibers are placed loosely in semi-rigid tubes, which take the mechanical stress. Special types of fiber optic cables have been developed for the power industry. One type of fiber cable is the Optical Power Ground Wire (OPGW) that is an optical fiber core within the ground or shield wire suspended above transmission lines. Another type of optical fiber cable is the All-Dielectric Self-Supporting (ADSS) cable that is a long-span of all dielectric cables designed to be fastened to high voltage transmission line towers underneath the power conductors. A Wrapped Optical Cable (WOC) is also available that is usually wrapped around the phase conductor or existing ground/earth wire of the transmission or distribution line. In the Utility's case, aerial fiber optic cable can be fastened to the distribution poles under the power lines. Table 5.3 shows the Fiber Optic Cable advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Immune to electromagnetic interference</li> <li>• Immune to ground potential rise</li> <li>• High channel capacity</li> <li>• Low operating cost</li> <li>• No licensing requirement</li> </ul>	<ul style="list-style-type: none"> <li>• Novel technology, i.e. new skills must be learned</li> <li>• Expensive test equipment</li> <li>• Inflexible network configuration</li> <li>• Cable subject to breakage and water ingress</li> </ul>

**Table 5.3: Fiber Optic Cable Advantages/Disadvantages [8]**

The cost per meter of fiber optic systems is expected to continually decrease. The cost of single mode fiber optic cables is now less than multimode fiber optic cable because of the increasing demand for single mode fiber. Conversely, the multimode fiber optic has limited distance and bandwidth characteristics.

The fiber optic terminal equipment is simpler and generally less expensive than microwave equipment. Optical transmitters can be either light emitting diodes (LEDs) or laser diodes. They operate at 850, 1310, or 1550 nm wavelengths, depending on the application. Many optical terminals have been developed for the telephone industry for large numbers of channels. There are now a number of products specifically designed for power utilities. These are low capacity terminals that feature surge withstand capabilities and special channel units for tele-protection signaling.

Parameters that influence the choice of the type of optical cable to be used are:

- Overhead cable can be OPGW, ADSS, or WOC
- Underground cable can be duct cable (light, medium, or heavy duty), ADSS for use in a duct, or direct burial cable with armor jacket

#### **5.4 Power Line Carrier**

Power Line Carrier (PLC) was one of the first reliable communications media available to electric utilities for critical communications channels that could not be subjected to the intolerance and unreliability of leased (common carrier) telephone circuits. PLC uses the power transmission lines to transmit radio frequency signals in the range of 30 kHz to 500 kHz. The physical security of this communications is very high since the power line carrier equipment is located within the substations. PLC systems are used to provide voice, telemetry, SCADA, and relaying communications on portions of the 220/230 kV, 110/115 kV, or 66 kV interconnected power transmission network.

Digital PLC technology is a relatively new technology. Power lines and their associated networks are not designed for communications use. They are hostile environments that make the accurate propagation of communication signals difficult. Two of the biggest problems faced in using power lines for communications are excessive noise levels and

cable attenuation. Noise levels are often excessive, and cable attenuation at the frequencies of interest is often very large.

The cost of PLC will probably increase at a greater rate than inflation because of decreasing demand. Communication transmission capacity of Single Side Band (SSB) PLC cannot be increased without purchasing a second or third PLC Radio Frequency (RF) channel at the same cost as original terminal equipment. Some cost can be saved by sharing dual frequency Traps, Line Tuning Units and coupling equipment. Digital PLC can be increased from one channel to three channels within the same RF bandwidth. Table 5.4 shows the advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Located where the circuits are required</li> <li>• Equipment installed in utility owned land or structures</li> <li>• Economically attractive for low numbers of channels extending over long distances</li> <li>• Digital PLC has capacity for three to four channels (e.g., two voice and one high speed data)</li> <li>• Analog PLC has capacity for two channels (one voice and one “speech plus” low speed data)</li> </ul>	<ul style="list-style-type: none"> <li>• Not independent of the power distribution system</li> <li>• Carrier frequencies often not protected on a primary basis</li> <li>• Inherently few channels available</li> <li>• Expensive on a per channel basis compared to microwave (normally, over four channels)</li> <li>• Will not propagate through open disconnects</li> </ul>

**Table 5.4: Power Line Carrier Advantages/Disadvantages [8]**

## 5.5 Satellites

The use of satellites has been investigated for a number of years. The satellites are positioned in geo-stationary orbits above the earth’s equator and thus offer continuous coverage over a particular area of the earth. Satellites contain a number of radio transponders which receive and retransmit frequencies to ground stations within its “footprint,” or coverage, on the earth’s surface. A network facility on the ground tracks and controls the satellite. Earth stations are comprised of an antenna pointing at the satellite, a radio transceiver with a low-noise amplifier, and baseband equipment. Satellites use both the C-band and the Ku-band. Very Small Aperture Terminal (VSAT) technology has advanced to the point where a much smaller antenna (down to about one meter) can be used for Ku-band communications. This has resulted in the Ku-band being preferred for sites with modest communications requirements. VSAT technology is advancing steadily, and the capital costs have dropped substantially. Continual time-of-use charges must be considered in the use of satellite communications. Developments in

this area should be investigated when making a decision on the use of this technology. Table 5.5 shows the Satellite system advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Wide area coverage</li> <li>• Easy Access to remote sites</li> <li>• Costs independent of distance</li> <li>• Low error rates</li>   <li>• Adaptable to changing network patterns</li> <li>• No right-of-way necessary, earth stations located at premises</li> </ul>	<ul style="list-style-type: none"> <li>• Total dependency on a remote facility</li> <li>• Less control over transmission</li> <li>• Transmission time delay</li> <li>• Reduced transmission during solar equinox</li> <li>• Continual leasing costs</li> </ul>

**Table 5.5: Satellite Advantages/Disadvantages [8]**

### 5.6 Leased Telephone Lines

Leased telephone circuits have long been used to meet communications needs. Most organizations use standard telephones connected to the Public Switched Network (PSN) for office communications and for routine voice traffic to stations. Leased dedicated circuits are used for dedicated communication requirements, such as telemetry and SCADA. Wideband channels may be available for high speed data signaling. Circuit characteristics can often be conditioned for many other uses, including voice and various types of low and medium speed data. Table 5.6 shows the Leased Circuit advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Small Capital Outlay</li> <li>• Maintained circuit quality</li> <li>• No communications expertise required</li> <li>• Adaptable to changing traffic patterns</li> </ul>	<ul style="list-style-type: none"> <li>• Repair and maintenance is not controlled by the lessee</li> <li>• Circuits may not be available at some sites</li> <li>• Metallic links require protection against ground potential rise</li> <li>• Continual leasing costs</li> </ul>

**Table 5.6: Leased Circuits Advantages/Disadvantages [8]**

### 5.7 Very High Frequency Radio

The Very High Frequency (VHF) band extends from 30 to 300 MHz and is usually used by utilities for mobile radio, although point-to-point links have been implemented in this band. Advances in data transmission on mobile radios have been made, particularly for joint voice and data use, such as in taxi and police dispatching systems. Such systems

could be used for maintenance vehicle dispatching. SCADA systems can use adapted VHF radios for communications; however a SCADA system would need exclusive use of the frequencies. Frequency assignments in this band are usually reserved for mobile services. Table 5.7 shows the VHF Radio advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Frequency assignments available</li> <li>• Propagation over non-line-of-sight paths</li> <li>• Low cost radios compared to microwave</li>   <li>• Less stringent waveguide and antenna requirements</li> <li>• Not dependent on power lines and common carriers</li> <li>• Greater field strength coverage patterns than UHF band</li> </ul>	<ul style="list-style-type: none"> <li>• Low channel capacity</li> <li>• Low digital data bit rate</li> <li>• Limited transmission techniques available</li> </ul>

**Table 5.7: VHF Radio Advantages/Disadvantages [8]**

## **5.8 Ultra High Frequency Radio**

The Ultra High Frequency (UHF) band extends from 300 to 3000 MHz. The bands typically considered for UHF radio are in the 400 MHz and 900 MHz range.

Most of the suitable radio products for SCADA applications available in the U.S. operate in the 900 MHz frequency range. In the U.S., the Federal Communications Commission (FCC) regulates the use of radio frequencies and has designated the 928 to 952 MHz range specifically for use by utilities for data communication applications. These UHF systems can be Point-To-Point (PTP), Point-To-Multipoint (PTM), Trunked Mobile Radio, or spread spectrum systems. The PTM systems are also referred to as Multiple Address Radio Systems (MARS). Spread spectrum systems are the basis for many wireless applications including 802.11 a/b/g networks. These types of UHF systems are described in the following subsections.

### **5.8.1 Point-to-Point**

Point-to-point communications is usually used for SCADA communications from a master station or dispatch center to individual substations. Radios used in the lower frequencies of the UHF band can be expected to have greater ranges, particularly for non-line-of-sight paths. Fewer studies have been carried out on path performance of fixed point-to-point links operating in these bands, compared to studies on line-of-sight microwave paths or on mobile radio coverage. Path analysis tends to use methods adapted from one of these areas of study and may give significantly different results. The best method to determine propagation losses is to make actual path measurements with



suitable test equipment or modified radios. Table 5.8 shows the Point-To-Point UHF radio system advantages and disadvantages.

<b>Advantages</b>	<b>Disadvantages</b>
<ul style="list-style-type: none"> <li>• Frequency assignments available</li> <li>• Propagation possible over non-line-of-sight paths</li> <li>• Low cost radios compared to microwave</li> <li>• Less stringent waveguide and antenna requirements</li> <li>• Not dependent on power lines and common carriers</li> </ul>	<ul style="list-style-type: none"> <li>• Low channel capacity</li> <li>• Low digital data bit rate</li> <li>• Limited transmission techniques available</li> </ul>

**Table 5.8: Point-to-Point UHF Radio Advantages/Disadvantages [8]**

### **5.8.2 Multiple Address Radio Systems**

A Multiple Address Radio System (MARS) Radio System generally consists of one Master Station (usually Hot Standby, full duplex) transmitting over an omni directional, gain antenna in a 360 radiation pattern to fixed station remotes or slaves (usually Non Standby, half duplex) that receive the signals via a directional, gain antenna. The 400/900 MHz MARS Radio is a single channel system that communicates with each of its remotes or slaves in sequence. Services usually supported by MARS are SCADA, Telemetry/Data Reporting, and voice (on a limited basis).

The security of a MARS system is high between stations, but is vulnerable at terminal stations in regard to the antenna and the terminal RF transmission lines. If security is a potential problem, the RF transmission lines can be placed in conduit, and the antennas can be ruggedized. The components of a MARS system have a long Mean Time Between Failure (MTBF) and friendly user maintenance features. The MARS system is usually configured for data transmission at 300 to 9600 baud, but can be used for voice transmission during radio system maintenance by locking the data signal out while voice is being transmitted.

The channel bandwidth allowed by the FCC is 12.5 kHz, which limits the expansion and upgrade capability of the MARS systems. Table 5.9 shows MARS advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• Frequency assignments available</li> <li>• Propagation possible over non-line-of-sight paths</li> <li>• Low cost radios compared to microwave</li> <li>• Less stringent waveguide and antenna requirements</li>   <li>• Not dependent on power lines and common carriers</li> <li>• Lower cost than Point-to-Point media</li> </ul>	<ul style="list-style-type: none"> <li>• Low channel capacity</li> <li>• Low digital data bit rate</li>   <li>• Limited transmission techniques available</li> <li>• Multi-point operation restricts data speed compared to Point-to-Point UHF or dedicated paths between stations</li> </ul>

**Table 5.9: MARS UHF Radio Advantages/Disadvantages [8]**

### 5.8.3 Spread Spectrum Radio

Low power spread spectrum radios<sup>3</sup> are allowed to operate in the 902–928 MHz band, 2.4, and 5.3 GHz band without licenses. This has prompted the development of packet-type radio networks for data systems, which are appropriate for Digital Multiplex System (DMS) applications, such as Distribution Automation (e.g., utilities). There are also systems offered in the 450–470 MHz band by a number of manufacturers. Each band can provide suitable signaling rates and characteristics for DMS communications, although the 900 MHz systems appear to have more advanced features at this time. Table 5.10 shows the Spread Spectrum Radio System advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• No radio frequency license required</li>   <li>• Low cost equipment</li> </ul>	<ul style="list-style-type: none"> <li>• Subject to interference from co-channel transmitters</li> <li>• No primary license status</li> <li>• Limited path lengths because of restrictions on Radio Frequency (RF) power output</li> </ul>

**Table 5.10: Spread Spectrum Radio Advantages/Disadvantages [8]**

## 5.9 Microwave Radio

Microwave radio is a term used to describe UHF radio systems operating at frequencies above 1 GHz, although multi-channel radio systems operating below 1 GHz are sometimes referred to as microwave systems. These systems have high channel capacities

---

<sup>3</sup> In accordance with Part 15 of the FCC Rules and Regulations

and data rates, and they are available in either analog or digital transmission technologies. Analog transmission was the first microwave technology available. It is the most mature method of transmission. There have been a number of developments, which have affected the traditional balance between digital and analog technologies. On the analog side, direct-to-baseband analog channel units have been developed to ease the addition of channels to existing multiplexer equipment and to reduce the complexity of modifying the channel plan. On the digital side, products such as digital cross-connects and direct first order hierarchical level access to Private Branch Exchange (PBXs) have reduced costs further and added flexibility. There is also a growing demand for circuits with very high data rates, which can be transported much easier on the digital systems. New protocols and standards are being introduced for utility data communications that are more easily accommodated by digital carrier systems. Therefore, even for light communication traffic routes, digital is judged to be the more appropriate technology for new installations. Services usually supported by microwave communications include voice, data (low speed and high speed), SCADA, compressed video, protective relaying, telemetry, frame relay, Broadband Integrated Services Digital Network (B-ISDN), and fractional T1.

In the lower part of the frequency range, microwave radios are designed in both point-to-point and point-to-multipoint configurations. The radios use similar technologies but are configured, operated and controlled differently. Point-to-point radio systems have dedicated transceivers and directional antennas at each end of a link. Point-to-multipoint radio systems have a common master transceiver with a non-directional antenna at the hub of a number of radial links. Point-to-point radios carry a fixed number of channels continuously. The equipment to which the channel interfaces are connected determines channel usage. For instance, they can be fixed, full-time data circuits interconnecting computer systems or telephone exchanges with usage determined by voice traffic. Channels are operational even if the circuits are idle.

Point-to-multipoint radios operate like a local area network with a number of shared channels, which are used on a demand basis. Point-to-multipoint radios can operate in several modes:

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)

FDMA is more suitable for analog radios because they have narrower bandwidths. TDMA and CDMA are more suitable for digital radios. Point-to-multipoint radios are more appropriate if network topology is in a star or tree configuration in which a number of terminal nodes have direct radio paths to a single central node and channel usage is not continuous. For linear configurations and continuous traffic, or bulk transmission over long distances, point-to-point radio is more appropriate. Table 5.11 shows the Microwave Radio advantages and disadvantages.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>• High Channel Capacity</li> <li>• Transports high data rates</li> <li>• Circuits added at low unit cost</li> <li>• Independent from power lines and common carriers</li> <li>• Future standardized high-speed networks</li> <li>• Not vulnerable to “backhoe fading”</li> <li>• Low right-of-way costs</li> <li>• Simpler installation than cable technology</li> </ul>	<ul style="list-style-type: none"> <li>• Line of sight clearance required</li> <li>• Specialized test equipment and training required</li> <li>• Frequency assignments sometimes unavailable in urban areas</li> <li>• More expensive site development</li> <li>• Limited capacity</li> </ul>

**Table 5.11: Microwave Radio Advantages/Disadvantages [8]**

New digital equipment requires very little maintenance compared to older analog systems. Many are overlaying the older analog microwave routes with fiber optic cable or new digital microwave equipment to supplement the older analog microwave system. Microwave communications are usually very secure physically since most microwave terminal and repeater equipment is located on utility premises.

## 6.0 Security and Vulnerability of SCADA Systems

SCADA systems have evolved in recent years and are now based on open standards and COTS products. Most SCADA software and hardware vendors have embraced Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet communications, and many have encapsulated their proprietary protocols in TCP/IP packets. While all of this evolution towards more open-based standards has made it easier for the industry to integrate various diverse systems together, it has also increased the risks of less technical personnel gaining access and control of these industrial networks. On October 1, 2003 Robert F. Dacey, Director, Information Security Issues at the General Accounting Office (GAO) eluded to this and other issues in his testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform. He said:

*“For several years, security risks have been reported in control systems, upon which many of the nation’s critical infrastructures rely to monitor and control sensitive processes and physical functions. In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of risks specific to control systems, including the (1) adoption of standardized technologies with known vulnerabilities, (2) connectivity of control systems to other networks, (3) constraints on the use of existing security technologies and practices, (4) insecure remote connections, and (5) widespread availability of technical information about control systems”. [9]*

There are many tools and techniques that could be used to address these threats, and flexibility of security configurations is a key design consideration. There is no one magic solution for industry. Each entity must determine what their goals are and arrive at a cost effective solution to these issues.

### 6.1 Attacks Against SCADA Systems

In today’s corporate environment, internal networks are used for all corporate communications, including SCADA. SCADA systems are therefore vulnerable to many of the same threats as any TCP/IP-based system. SCADA Administrators and Industrial Systems Analysts are often deceived into thinking that since their industrial networks are on separate systems from the corporate network, they are safe from outside attacks. PLCs and RTUs are usually polled by other 3rd party vendor-specific networks and protocols like RS-232, RS-485, MODBUS<sup>4</sup>, and DNP, and are usually done over phone lines, leased private frame relay circuits, satellite systems, licensed and spread spectrum radios, and other token-ring bus topology systems. This often gives the SCADA System Administrators a false sense of security since they assume that these end devices are protected by these non-corporate network connections.

---

<sup>4</sup> MODBUS Protocol is a messaging structure developed by Modicon in 1979, used to establish master-slave/client-server communication between intelligent devices more info at [www.modbus.org](http://www.modbus.org)

Security in an industrial network can be compromised in many places along the system and is most easily compromised at the SCADA host or control room level. SCADA computers logging data out to some back-office database repositories must be on the same physical network as the back-end database systems, or have a path to access these database systems. This means that there is a path back to the SCADA systems and eventually the end devices through their corporate network. Once the corporate network is compromised, then any IP-based device or computer system can be accessed. These connections are open 24x7 to allow full-time logging, which provides an opportunity to attack the SCADA host system with any of the following attacks:

- Use a Denial of Service (DoS) attack to crash the SCADA server leading to shut down condition (System Downtime and Loss of Operations)
- Delete system files on the SCADA server (System Downtime and Loss of Operations)
- Plant a Trojan and take complete control of system (Gain complete control of system and be able to issue any commands available to Operators)
- Log keystrokes from Operators and obtain usernames and passwords (Preparation for future take down)
- Log any company-sensitive operational data for personal or competition usage (Loss of Corporate Competitive Advantage)
- Change data points or deceive Operators into thinking control process is out of control and must be shut down (Downtime and Loss of Corporate Data)
- Modify any logged data in remote database system (Loss of Corporate Data)
- Use SCADA Server as a launching point to defame and compromise other system components within corporate network. (IP Spoofing)

The impact of these and other SCADA Security Risks is summarized in Table 6.1.

**Table 6.1: SCADA Attack Matrix [10]**

<b>Description of Attack</b>	<b>Type of Attack</b>	<b>Attack Motive</b>	<b>Impact to Victim</b>	<b>Impact Rating (1 = largest immediate impact 5 = least immediate impact)</b>	<b>Items Needed for Attack</b>	<b>Estimated Time to Implement Once System is Compromised</b>
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down	2	Ability to flood the server with TCP/IP calls, the IP Address of SCADA Server, and the path to the server	5 min.
Delete System Files (Low-level format on all local drives)	System Shutdown	Wish to take down server and cause immediate shutdown situation	Critical Server and SCADA files are lost and operations can no longer monitor process or control plant or facility	4	IP Address of SCADA Server, path to server, and permission to delete files permission can be escalated used other tools)	15 min.
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.	1	IP Address of SCADA Server, path to server, and either Trojan or back door installed. (Can also use PCAnywhere, Terminal Services, SMS, or other system admin services.)	1 hr.
Log Keystrokes, Usernames, Passwords, System Setpoints, and any Operational Information	Information Mining	Gain Information for future attacks or satisfy curiosity	Lower immediate impact, but information gained can be used for future attacks.	4	IP Address of SCADA Server, path to server, and software or mechanism for logging the keystroke activities.	15 min.

**Table 6.1: SCADA Attack Matrix [10]**

<b>Description of Attack</b>	<b>Type of Attack</b>	<b>Attack Motive</b>	<b>Impact to Victim</b>	<b>Impact Rating (1 = largest immediate impact 5 = least immediate impact)</b>	<b>Items Needed for Attack</b>	<b>Estimated Time to Implement Once System is Compromised</b>
Change Data Points or Change Setpoint(s) in SCADA System	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	2	IP Address of SCADA Server, access to these servers, and some knowledge of SCADA software system inner workings	45 min.
Log any Operational or Corporate data for personal gain or sell to competition or hold as ransom	Information Mining	Try to steal corporate data and either sell to other companies or hold for ransom amount	Low environmental or immediate damage, but can damage corporate image if attacker builds attention to the fact that this system was compromised	4	IP Addresses of SCADA and database servers. (Would not even need IP addresses if protocol sniffer/logger used to sniff TCP/IP traffic.)	30 min.
Modify Data points on SCADA graphics to deceive Operators that system is out of control and must ESD (Emergency Shut Down)	System Shutdown	Cause danger to the facility or company by staging a false alarm shutdown of the plant or facility	Operations can no longer trust the SCADA System, and the attacker has deceived the Operator into thinking that there was an emergency condition in the plant	2	IP Addresses of SCADA servers, and access to them through the company network	45 min.



**Table 6.1: SCADA Attack Matrix [10]**

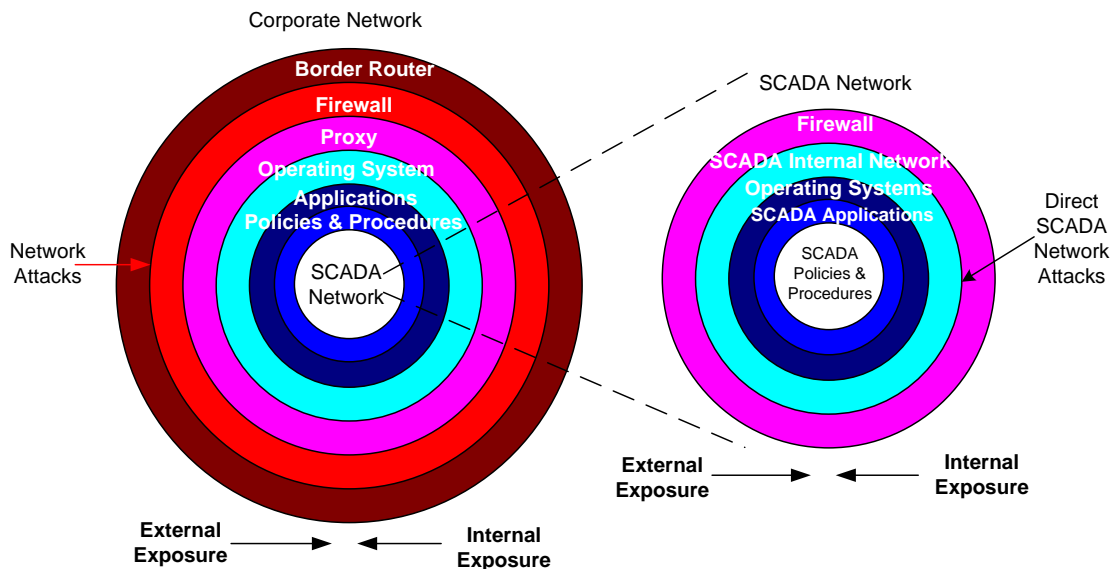
<b>Description of Attack</b>	<b>Type of Attack</b>	<b>Attack Motive</b>	<b>Impact to Victim</b>	<b>Impact Rating (1 = largest immediate impact 5 = least immediate impact)</b>	<b>Items Needed for Attack</b>	<b>Estimated Time to Implement Once System is Compromised</b>
Capture, Modify, or Delete Data Logged in Operational Database SQL Server, PI Historian, Oracle, Sybase, etc.)	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	3	IP Address of SCADA Server, path to database server, and knowledge of SCADA software structure	45 min.
Locate Maintenance Database and modify or delete information regarding calibration and reliability tests for industrial equipment	Information Tampering	Desire to steal, modify, or delete corporate data.	Less immediate danger, but corporate information data warehouse would be comprised	4	IP Addresses of database servers	30 min.

## 6.2 Developing a SCADA Security Strategy

For a company to protect its infrastructure, it should undertake the development of a security strategy that includes specific steps to protect any SCADA system. Such a strategy may include the following approach.

Developing an appropriate SCADA security strategy involves analysis of multiple layers of both the corporate network and SCADA architectures including firewalls, proxy servers, operating systems, application system layers, communications, and policy and procedures. Strategies for SCADA Security should complement the security measures implemented to keep the corporate network secure

Figure 6.1 below illustrates the typical corporate network “ring of defenses” and its relationship with the SCADA network. Successful attacks can originate from either Internet paths through the corporate network to the SCADA network, or from internal attacks from within the corporate office. Alternatively, attacks can originate from within the SCADA network from either upstream (applications) or downstream (RTUs) paths. What is an appropriate configuration for one installation may not be cost effective for another. Flexibility and the employment of an integrated and coordinated set of layers are critical in the design of a security approach.



**Figure 6.1: Relationship Between Corporate and SCADA Networks [10]**

Most corporate networks employ a number of security countermeasures to protect their networks. Some of these and a brief description of their functions are as follows:

- **Border Router and Firewalls**—Firewalls, properly configured and coordinated, can protect passwords, IP addresses, files and more. However, without a hardened

operating system, hackers can directly penetrate private internal networks or create a Denial of Service condition.

- **Proxy Servers**—A Proxy server is an internet server that acts as a firewall, mediating traffic between a protected network and the internet. They are critical to re-create TCP/IP packets before passing them on to, or from, application layer resources such as Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). However, the employment of proxy servers will not eliminate the threat of application layer attacks.
- **Operating Systems**—Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated. This is due to the fact that operating systems are the core of every computer system and their design and operating characteristics are well known world wide. As a result, operating systems are a prime target for hackers. Further, in- place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.
- **Applications**—Application layer attacks; i.e., buffer overruns, worms, Trojan Horse programs and malicious Active-X<sup>5</sup> code, can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.
- **Policies and Procedures**—Policies and procedures constitute the foundation of security policy infrastructures. They include requiring users to select secure passwords that are not based on a dictionary word and contain at least one symbol, capital letter, and number, and should be over eight characters long. Users should not be allowed to use their spouse, child, or pet's name as their password.

The above list is common to all entities that have corporate networks. SCADA systems for the most part coexist on the same corporate network [10]. The following list suggests ways to help protect the SCADA network in conjunction with the corporate network:

- **SCADA Firewalls**—SCADA Systems and Industrial Automation Networks, like corporate network operating systems, can be compromised using similar hacking methods. Oftentimes, SCADA systems go down due to other internal software tools or employees who gain access into the SCADA systems, often without any intention to take down these systems. For these reasons, it is suggested that strong firewall protection to wall off your SCADA networking systems from both the internal corporate network and the Internet be implemented. This would provide at least two layers of firewalls between the SCADA networking systems and the Internet.
- **SCADA Internal Network Design**—SCADA networks should be segmented off into their own IP segment using smart switches and proper sub-masking techniques to protect the Industrial Automation environment from the other network traffic, such as file and print commands. Facilities using Wireless Ethernet and Wired Equivalent Protocol (WEP) should change the default name of the Service Set Identifier<sup>6</sup> (SSID).

---

<sup>5</sup> An architecture that lets a program interact with other programs over a network (such as the Internet)

<sup>6</sup> Differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID

This will at least require someone driving by with a wireless card to know the name of the SSID, and have the appropriate encryption key for the wireless network.

- **SCADA Server Operating Systems**—Simply installing a firewall or segmenting SCADA IP addresses will not ensure their SCADA Infrastructure is secure. An experienced hacker can often bypass firewalls with ease and can even use Address Resolution Protocol (ARP) trap utilities to steal Media Access Control (MAC) addresses. The hacker can also deploy IP spoofing techniques to maneuver through switched networks. Operating systems running the SCADA applications must also be maintained. SCADA applications on Windows NT, 2000, or XP are properly patched against the latest vulnerabilities, and that all of the default NULL NT accounts and administrator accounts have been removed or renamed. SCADA applications running in UNIX, LINUX, Novell, or any other Operating System (OS), must also be maintained as above. All operating systems have back doors and default access accounts that should be removed and cleaned off of these SCADA Servers.
- **SCADA Applications**—You must also address security within the SCADA application itself. Trojan horses and worms can be inserted to attack application systems, and they can be used to manipulate data or issue commands on the server. There have even been cases of Trojan horses being deployed that completely emulate the application. The operator or user thinks that he is clicking on a command to stop a pump or generate a graph of the plant, but he is actually clicking on buttons disguised to look like the SCADA screen, and these buttons start batch files that delete the entire hard drive, or send out pre-derived packets on the SCADA system that turn all outputs to ON or “1” state. Trojan horses and viruses can also be planted through an email opened by another computer in the plant, and then it is silently copied over to adjacent SCADA servers, where they wait until a specified time to run. Many times plant control rooms will have corporate computers with the Internet and email active on them within the same physical room, and network switches as SCADA computers. Methodologies to mitigate against these types of situations are: the use of anti-virus software running on the computer where the SCADA application resides; systems administrators disabling installation of any unauthorized software unless the user has administrator access; and Policies and Procedures applicable to SCADA systems, which are addressed below.
- **SCADA Policies and Procedures**—SCADA policies and procedures associated with remote vendor and supervisory access, password management, etc. can significantly impact the vulnerabilities of the SCADA facilities within the SCADA network. Properly developed Policies and Procedures that are enforced will greatly improve the security posture of the SCADA system.

In summary, these multiple “rings of defense” must be configured in a complementary and organized manner, and the planning process should involve a cross-team with senior staff support from operations, facility engineering, and Information Technology (IT). The SCADA Security team should first analyze the current risks and threat at each of the rings of defense, and then initiate a work plan and project to reduce the security risk, while remembering to avoid any major impacts to operations.

## **7.0 SCADA Standards Organizations**

There are many organizations involved in the standardization of SCADA systems. This section details some of these organizations and the roles they play.

### **7.1 The Institute of Electrical and Electronics Engineers (IEEE)**

The IEEE Standards Association (IEEE-SA) is a membership organization that produces Electrical and IT-Related standards that are used internationally. The IEEE has been involved in standardizing technologies for many years. The following standards have been published by the IEEE with respect to SCADA systems:

- IEEE Std 999-1992 – IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications. This recommended practice applies to the use of serial digital transmissions by supervisory control and data acquisition (SCADA) systems having geographically dispersed terminals. These types of systems typically utilize dedicated communication channels, such as private microwave channels or leased telephone lines, which are limited to data rates of less than 10,000 b/s.
- IEEE Std 1379-2000 – IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation. This recommended practice presents a uniform set of guidelines for communications and interoperation of IEDs and RTUs in an electric utility substation. This recommended practice does not establish an underlying communication standard. Instead, it provides a specific limited subset of two existing communication protocols and encourages understanding and timely application.

### **7.2 American National Standards Institute**

The American National Standards Institute (ANSI) is a private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The Institute's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

The mission of The American National Standards Institute's Homeland Security Standards Panel (ANSI-HSSP) is to identify existing consensus standards, or, if none exists, assist the Department of Homeland Security (DHS) and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area.

Established by ANSI in February 2003, the ANSI-HSSP's scope is to catalog, promote, accelerate and coordinate the timely development of consensus standards within the

national and international voluntary standards systems intended to meet identified homeland security needs, and communicate the existence of such standards appropriately to governmental units and the private sector. The Panel will initially focus its activities on responding to the most immediate standards needs of DHS.

### **7.3 Electric Power Research Institute**

The Electric Power Research Institute (EPRI) was founded in 1973 as a non-profit energy research consortium for the benefit of utility members, their customers, and society. Their mission is to provide science and technology-based solutions of indispensable value to global energy customers by managing a far-reaching program of scientific research, technology development, and product implementation.

EPRI is the only science and technology consortium serving the entire energy industry—from energy conversion to end use—in every region of the world. With expertise in a wide spectrum of scientific research, technology development, and product application, they are able to offer solutions that cut across traditional boundaries, taking advantage of the latest advances in many fields. EPRI provides the knowledge, tools, and expertise you need to build competitive advantage, address environmental challenges, open up new business opportunities, and meet the needs of your energy customers.

The (EPRI) has developed The Utility Communications Architecture (UCA) to integrate communications for "real-time" utility operations for SCADA systems. The UCA is the only existing protocol that provides interoperability among different monitoring and control equipment and interconnectivity among databases for utility operations. The UCA Version 2 Specification has been recently published by the Institute of Electrical and Electronic Engineers (IEEE) Standards Board as Technical Report TR1550. EPRI takes great pride that the UCA technology has been published by the IEEE. In addition, UCA is in review by the International Electrotechnical Commission (IEC) to become the international standard for integrated utility operations. The new UCA Version 2 includes four parts that are published in two volumes, as follows:

- TR1550 Volume 1: Part 1: Introduction to UCA (TM) Version 2.0; Part 2: UCA (TM) Profiles; Part 3: UCA (TM) Common Application Service Models (CASM). And TR1550 Volume 2: Part 4: UCA (TM) Generic Object Models for Substation and Feeder Equipment (GOMSFE)

Part 1: Introduction. Gives an overview of the UCA Version 2. This document presents a background, philosophy, and applications of UCA to provide a basic understanding of UCA.

Part 2: Profiles. Presents the profiles and protocols for various communication media, including local area networks, radio, fiber optic, and telephone; including guidelines on the use of the Internet protocols in a UCA context.

Part 3: Common Applications Services Model (CASM). Describes models for device behavior from a UCA communications perspective; it also defines the language, services, semantics, and applications of UCA.

Part 4: Generic Object Models for Field Equipment (GOMSFE). Presents a detailed list of device object models for a wide range of substation and distribution field equipment, including breakers, relays, sectionalizers, capacitor controllers, remote terminal units (RTUs), and other intelligent electronic devices (IEDs).

## **7.4 International Electrotechnical Commission**

The International Electrotechnical Commission (IEC) Technical Committee 57 Working Group 03 (TC57 WG03) was chartered to develop protocol standards for telecontrol, teleprotection, and associated telecommunications for electric utility systems, and it has created IEC 60870-5, a group of five utility-specific protocol standards. IEC 60870-5 specifies a number of links, frame formats, and services that may be provided at each of three layers. IEC 60870-5 uses the concept of a three-layer enhanced performance architecture (EPA) reference model for efficiency of implementation in devices such as RTUs, meters, relays, etc. used in SCADA systems.

IEC 60870-5 specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer EPA reference model for efficient implementation within RTUs, meters, relays, and other IEDs. Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the OSI application layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set. Standard profiles are necessary for uniform application of the IEC 60870-5 standards. Such profiles have been and are being created. The Standard 101 Profile is described in detail following the description of the applicable standards.

- IEC 60870-5-1 (1990-02) specifies the basic requirements for services to be provided by the data link and physical layers for telecontrol applications. In particular, it specifies standards on coding, formatting, and synchronizing data frames of variable and fixed lengths that meet specified data integrity requirements.
- IEC-60870-5-2 (1992-04) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because some point-to-point topologies do not require either source or destination addressing.
- IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic standards that may be used to support a great variety of present and future telecontrol applications. This section of IEC 60870-5 describes the general structure of application data and basic rules to specify application data units without specifying details about information fields and their contents.

- IEC 60870-5-4 (1993-08) provides rules for defining information data elements and a common set of information elements, particularly digital and analog process variables that are frequently used in telecontrol applications.
- IEC 60870-5-5 (1995-06) defines basic application functions that perform standard procedures for telecontrol systems, which are procedures that reside beyond layer 7 (application layer) of the ISO reference model. These utilize standard services of the application layer. The specifications in IEC 60870-5-5 (1995-06) serve as basic standards for application profiles that are then created in detail for specific telecontrol tasks.

Each application profile will use a specific selection of the defined functions. Any basic application functions not found in a standards document but necessary for defining certain telecontrol applications should be specified within the profile. Examples of such telecontrol functions include station initialization, cyclic data transmission, data acquisition by polling, clock synchronization, and station configuration.

## **7.5 DNP3 Users Group**

The development of DNP3 was a comprehensive effort to achieve open, standards-based interoperability between substation computers, RTUs, IEDs (Intelligent Electronic Devices) and master stations (except inter-master station communications) for the electric utility industry for SCADA systems. Also important was the time frame; the need for a solution to meet today's requirements. As ambitious an undertaking as this was, the objective was achieved. Since the inception of DNP, the protocol has also become widely utilized in adjacent industries such as water/waste water, transportation, and the oil and gas industry.

DNP3 is based on the standards of the International Electrotechnical Commission (IEC) Technical Committee 57, Working Group 03, who have been working on an OSI 3 layer "Enhanced Performance Architecture" (EPA) protocol standard for telecontrol applications. DNP3 has been designed to be as close to compliant as possible to the standards, as they existed at time of development with the addition of functionality not identified in Europe but needed for current and future North American applications (e.g. limited transport layer functions to support 2K block transfers for IEDs, RF and fiber support). DNP3 has been selected as a Recommended Practice by the IEEE C.2 Task Force; RTU to IED Communications Protocol.

DNP3 was developed by Harris, Distributed Automation Products. In November 1993, responsibility for defining further DNP3 specifications and ownership of the DNP3 specifications was turned over to the DNP3 Users Group, a group composed of utilities and vendors who are utilizing the protocol.

DNP3 is an open and public protocol. In order to ensure interoperability, longevity and upgradeability of protocol, the DNP3 User Group has taken ownership of the protocol and assumes responsibility for its evolution. The DNP3 User Group Technical Committee



evaluates suggested modifications or additions to the protocol and then amends the protocol description as directed by the User Group members.

Complete documentation of the protocol is available to the public. The four core documents that define DNP3 are: Data Link Layer Protocol Description, Transport Functions, Application Layer Protocol Description, and Data Object Library (referred to as the "Basic 4 Document"). The User Group also has available to members the document "DNP3 Subset Definitions" which will help implementors identify protocol elements that should be implemented.

## 8.0 Observations and Conclusions

This TIB has presented an overview of SCADA system, relevant to the NCS in support of their NS/EP and CIP missions. SCADA systems have been used for years in the utilities industry with great success. Now more than ever, it is important that our critical infrastructures such as power grids, water processing systems, and the Public Switched Network (PSN), be monitored and protected. SCADA architectures, protocols, typical deployments, and security vulnerability concerns have been addressed. The following observations and conclusions are provided:

- Today's SCADA systems are able to take advantage of the evolution from mainframe based to client/server architectures. These systems use common communications protocols like Ethernet and TCP/IP to transmit data from the field to the central master control unit.
- SCADA protocols have also evolved from closed proprietary systems to an open system, allowing designers to choose equipment that can help them monitor their unique system using equipment from variety of vendors
- SCADA systems are widely used to monitor and control U.S. critical infrastructure utilities such as Electrical Power Plants and Water Distribution Centers
- SCADA systems, like other computer systems, are subject to many common security attacks such as viruses, denial of service, and hijacking of the system
- Because SCADA systems use leased telephone lines, twisted pair cable, microwave radio, and spread spectrum techniques, they have many of the same security vulnerabilities
- While SCADA protocols are more open today, there is no clear consensus of which protocol is best. IEC 60870-5 series and DNP3 have many similarities but are not 100% compatible.
- UCA 2.0, developed by EPRI, has been published by the IEEE as a Technical Report and submitted to IEC for review. UCA is a new SCADA protocol that may replace both DNP3 and IEC 60870-5.

## 9.0 Recommendations

In their current state, SCADA systems may not be fully able to support the NS/EP and CIP missions of the NCS. Several issues need to be addressed, especially in the area of vulnerabilities associated with computer usage and the communications within SCADA systems. To facilitate SCADA systems' ability to support the NS/EP and CIP missions of the NCS, the following are recommended:

- NCS should monitor the development, and make contributions when appropriate, of IEC 60870-5, DNP3, and UCA 2.0
- Monitor and participate, as appropriate, in the IEEE standards process as it relates to SCADA systems, especially in security features or requirements with SCADA Standards
- NCS should participate in the ANSI-HSSP. This panel is looking into refining and creating standards critical to homeland security. They are looking at utilities in particular, which heavily utilize SCADA systems.
- NCS should look at commissioning additional studies that examine unconventional attacks, such as those using Electro Magnetic Pulse (EMP) weapons, against SCADA system supporting NS/EP and CIP
- NCS should pursue, with the developers of SCADA protocols, incorporation of security features internal to the protocol rather than external



## Appendix A - Acronyms

ADSS	All Dielectric Self Supporting
ADSU	Application Data Service Unit
ANSI	American National Standards Institute
ANSI-HSSP	American National Standards Institute - Homeland Security Standards Panel
ARP	Address Resolution Protocol
ASDU	Application Service Data Units
B-ISDN	Broadband Integrated Services Digital Network
CASM	Common Application Service Models
CCITT	International Telegraph and Telephone Consultative Committee
CDMA	Code Division Multiple Access
CMS	Central Monitoring Station
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DHS	Department of Homeland Security
DMS	Digital Multiplex System
DNP	Distributed Network Protocol
DNP3	Distributed Network Protocol Version 3
DoS	Denial of Service
E.O	Executive Order
EIA	Electronic Industries Association
EOP	Executive Office of the President
EP	Electrophotographic Engine
EPA	Enhanced Performance Architecture
EPRI	Electric Power Research Institute
ESD	Emergency Shut Down
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FT	Fixed radio Terminal
GHz	Gigahertz
GOMSFE	Generic Object Models for Substation and Feeder Equipment
HF	High Frequency
HMI	Human Machine Interface
HSSP	Homeland Security Standards Panel
HTTP	Hyper Text Transfer Protocol

I/O	Input/Output
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	ITU Telecommunications
LAN	Local Area Network
LED	Light Emitting Diodes
MAC	Medium Access Control
MARS	Multiple Address Radio Systems
MHz	Megahertz
MMI	Man Machine Interface
MTBF	Mean Time Between Failure
NCS	National Communications System
NE/EP	National Security/Emergency Preparedness
NS	National Security
NS/EP	National Security and Emergency Preparedness
NT	Network Termination
ODBC	Object Oriented Database Connectivity
OMNCS	Office of the Manager, NCS
OPGW	Optical Power Ground Wire
OS	Operating System
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PCL	Power Line Communication
PCS	Personal Communications Service
PI	Program Interruption
PLC	Programmable Logic Controller
PN	Public Network
PSN	Public Switched Network
PTM	Point to Multipoint
PTP	Point to Point
PVC	Polyvinyl Chloride
RF	Radio Frequency
RS	Radio Shack
RTU	Remote Terminal Unit

RTU/IED	Remote Terminal Unit/Intelligent Electronic Devices
SCADA	Supervisory Control and Data Acquisition
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSB	Single Side Band
SSID	Service Set Identifier
TA	Technical Assembly
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TETRA	Trans European Trucked Radio
TIB	Technical Information Bulletin
UART	Universal Asynchronous Receiver Transmitters
UCA	Utility Communications Architecture
UHF	Ultra High Frequency
VHF	Very High Frequency
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WEP	Wired Equivalent Protocol
WOC	Wrapped Optical Cable

## Appendix B - References

- [1] “Convergence Task Force Report,” President’s National Security Telecommunications Advisory Committee, Washington, DC, June 2001
- [2] J. Walrand and P. Varaiya, High Performance Communication Networks, Second Edition, San Francisco: Morgan Kaufmann Publishers, 2000
- [3] “Information Technology Progress Impact Task Force Report On Convergence,” President’s National Security Telecommunications Advisory Committee, Washington, DC, May 2000
- [4] Walski, Thomas M., et. al., Advanced Water Distribution Modeling and Management, Haestad Press, January 2003
- [5] *McClanahan, R.H.*, The Benefits of Networked SCADA Systems Utilizing IP-Enabled Networks, Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C5 - C5\_7
- [6] IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, IEEE Std 1379-2000 (Revision of IEEE Std 1379-1997), 21 September 2000
- [7] Curtis, Ken, A., DNP3 Protocol Primer, DNP Users Group, 1 June 2000
- [8] *Marihart, D.J.*, Communications Technology Guidelines for EMS/SCADA Systems, Power Delivery, IEEE Transactions on, Volume: 16, Issue: 2, April 2001 Pages: 181–188
- [9] “Critical Infrastructure Protection Challenges in Securing Control Systems”, General Accounting Office (GAO) Report, GAO-04-140T, October 1, 2003
- [10] Pollet, Jonathan, SCADA Security Strategy, Plant Data Technologies, August 8, 2002



## Appendix C - Bibliography

*McClanahan*, SCADA and IP: is network convergence really here?, Industry Applications Magazine, IEEE , Volume: 9 , Issue: 2 , March-April 2003 Pages:29 - 36

*Bin Qiu, Hoay Beng Gooi, Yilu Liu, Eng Kiat Chan*, Internet-based SCADA display system, Computer Applications in Power, IEEE , Volume: 15 , Issue: 1 , Jan. 2002 Pages:14 - 19

*Shyh-Jier Huang, Chih-Chieh Lin*, Application of ATM-based network for an integrated distribution SCADA-GIS system, Power Systems, IEEE Transactions on , Volume: 17, Issue: 1 , Feb. 2002 Pages:80 - 86

*Marihart, D.J.*, Communications technology guidelines for EMS/SCADA systems, Power Delivery, IEEE Transactions on , Volume: 16 , Issue: 2 , April 2001 Pages:181 - 188

*Qiu, B., Gooi, H.B.*, Web-based SCADA display systems (WSDS) for access via Internet Power Systems, IEEE Transactions on , Volume: 15 , Issue: 2 , May 2000 Pages:681 - 686

*Bruce, A.G.*, Reliability analysis of electric utility SCADA systems, Power Systems, IEEE Transactions on, Volume: 13, Issue: 3, Aug. 1998 Pages: 844 - 849

*Ghoshal, K.*, Distribution automation: SCADA integration is key, Computer Applications in Power, IEEE , Volume: 10 , Issue: 1 , Jan. 1997 Pages:31 - 35

*Marcuse, J., Menz, B., Payne, J.R.*, Servers in SCADA applications, Industry Applications, IEEE Transactions on , Volume: 33 , Issue: 5 , Sept.-Oct. 1997 Pages:1295 - 1299

*Luque, J., Gomez, I.*, The role of medium access control protocols in SCADA systems, Power Delivery, IEEE Transactions on , Volume: 11 , Issue: 3 , July 1996 Pages:1195 - 1200

*Luque, J., Gomez, I., Escudero, J.I.*, Determining the channel capacity in SCADA systems using polling protocols, Power Systems, IEEE Transactions on , Volume: 11, Issue: 2 , May 1996 Pages:917 - 922

*Sciacca, S.C., Block, W.R.*, Advanced SCADA concepts, Computer Applications in Power, IEEE , Volume: 8 , Issue: 1 , Jan. 1995 Pages:23 - 28

*Flowers, T., Houle, B., Refzer, J., Ramanathan, R.*, Routing SCADA data through an enterprise WAN, Computer Applications in Power, IEEE , Volume: 8 , Issue: 3 , July

1995 Pages:40 - 44

*Bernard, J.-P., Durocher, D.*, An expert system for fault diagnosis integrated in existing SCADA system, Power Systems, IEEE Transactions on , Volume: 9 , Issue: 1 , Feb. 1994 Pages:548 - 554

*Bruce, A., Lee, R.*, A framework for the specification of SCADA data links, Power Systems, IEEE Transactions on , Volume: 9 , Issue: 1 , Feb. 1994 Pages:560 - 564

*Ghoshal, K., Douglas, L.D.*, GUI display guidelines drive winning SCADA projects, Computer Applications in Power, IEEE , Volume: 7 , Issue: 2 , April 1994 Pages:39 - 42

*Gaushell, D.J., Block, W.R.*, SCADA communication techniques and standards, Computer Applications in Power, IEEE , Volume: 6 , Issue: 3 , July 1993 Pages:45 - 50

*Chan, E.-K., Ebenhoh, H.*, The implementation and evolution of a SCADA system for a large distribution network, Power Systems, IEEE Transactions on , Volume: 7 , Issue: 1, Feb. 1992 Pages:320 - 326

*Pollet, J.*, Developing a solid SCADA security strategy, Sensors for Industry Conference, 2002. 2nd ISA/IEEE, 19-21 Nov. 2002 Pages: 148 - 156

*Duo Li, Serizawa, Y., Mai Kiuchi*, Concept design for a Web-based supervisory control and data-acquisition (SCADA) system, Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES , Volume: 1 , 6-10 Oct. 2002 Pages:32 - 36 vol.1

*Hayashi, H., Takabayashi, Y., Tsuji, H., Oka, M.*, Rapidly increasing application of Intranet technologies for SCADA (supervisory control and data acquisition system), Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES, Volume: 1 , 6-10 Oct. 2002 Pages:22 - 25 vol.1

*Xiaodong Zhang, Yun Gao, Guangyuan Zhang, Guangguo Bi*, CDMA2000 cellular network based SCADA system, Power System Technology, 2002. Proceedings. PowerCon 2002. International Conference on, Volume: 2, 13-17 Oct. 2002 Pages: 1301 - 1306 vol.2

*Zhihao Ling, Jinshou Yu*, The design of SCADA based on industrial Ethernet, Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on, Volume: 4, 10-14 June 2002 Pages: 2786 - 2789 vol.4

*Alexander, R.L.*, Intelligent electronic device (IED) technology SCADA and 3Ø metering, Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C6 - C6\_3

*Dagle, J.E., Widergren, S.E., Johnson, J.M.*, Enhancing the security of supervisory control and data acquisition (SCADA) systems: the lifeblood of modern energy infrastructures, Power Engineering Society Winter Meeting, 2002. IEEE, Volume: 1, 27-31 Jan. 2002 Pages: 635 vol.1

*Qian Wang, Qingquan Qian*, Design and analysis of communication network for distributed SCADA system, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2062 - 2065 vol.3

*Wu Sitao, Qian Qingquan*, Using device driver software in SCADA systems, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2046 - 2049 vol.3

*Chen Qizhi, Qian Qinquan*, The research of UNIX platform for SCADA, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2041 - 2045 vol.3

*Ebata, Y., Hayashi, H., Hasegawa, Y., Komatsu, S., Suzuki, K.*, Development of the Intranet-based SCADA (supervisory control and data acquisition system) for power system, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 1656 - 1661 vol.3

*Chen Qizhi*, Optimization of a SCADA system based on client/serve mode, Power System Technology, 1998. Proceedings. POWERCON '98. 1998 International Conference on, Volume: 2, 18-21 Aug. 1998 Pages: 1237 - 1240 vol.2

*Medida, S., Sreekumar, N., Prasad, K.V.*, SCADA-EMS on the Internet, Energy Management and Power Delivery, 1998. Proceedings of EMPD '98. 1998 International Conference on, Volume: 2, 3-5 March 1998 Pages: 656 - 660 vol.2

*Zecevic, G.*, Web based interface to SCADA system, Power System Technology, 1998. Proceedings. POWERCON '98. 1998 International Conference on, Volume: 2, 18-21 Aug. 1998 Pages: 1218 - 1221 vol.2

*Marcuse, J., Menz, B., Payne, J.*, Servers in SCADA applications, Industry Applications Conference, 1995. Thirtieth IAS Annual Meeting, IAS '95., Conference Record of the 1995 IEEE , Volume: 3 , 8-12 Oct. 1995 Pages:2124 - 2129 vol.3

*Bruce, A.G., Lee, R.*, A framework for the specification of SCADA data links, Power Industry Computer Application Conference, 1993. Conference Proceedings , 4-7 May 1993 Pages:117 - 121

*McDonald, J.D.*, Developing and defining basic SCADA system concepts, Rural Electric Power Conference, 1993. Papers Presented at the 37th Annual Conference , 25-27 April 1993 Pages:B3/1 - B3/5

*Quarthey, B., Shaw, D., Waked, P.*, An application of PLC's as an RTU in SCADA systems, Petroleum and Chemical Industry Conference, 1992, Record of Conference Papers., Industry Applications Society 39th Annual , 28-30 Sept. 1992 Pages:271 - 274

*Hoge, D.J., Jensen, J.R.*, A comparison of protocol conversion methods for the retrofit of SCADA systems, Petroleum and Chemical Industry Conference, 1988, Record of Conference Papers., Industrial Applications Society 35th Annual , 12-14 Sept. 1988 Pages:245 - 248

IEEE recommended practice for master/remote supervisory control and data acquisition (SCADA) communications, IEEE Std 999-1992 , 12 Feb. 1993

*Blackman, J.M., Hissey, T.W.*, Impact of local and wide area networks on SCADA and SCADA/EMS systems, Advanced SCADA and Energy Management Systems, IEE Colloquium on , 6 Dec 1990 Pages:8/1 - 815

*Kwok-Hong Mak, Holland, B.L.*, Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking, Power Engineering Journal, Volume: 16 , Issue: 6, Dec. 2002 Pages:305 - 311

*Su, C.-L., Lu, C.-N., Lin, M.-C.*, Migration path study of a distribution SCADA system, Generation, Transmission and Distribution, IEE Proceedings- , Volume: 146 , Issue: 3, May 1999 Pages:313 - 317

*Cheung, R.W.-L., Yu-Fai Fung*, Wireless access to SCADA system, Advances in Power System Control, Operation and Management, 2000. APSCOM-00. 2000 International Conference on , Volume: 2 , 30 Oct-1 Nov, 2000 Pages:553 - 556

*Ball, R., Berresford, D.R., Crook, E., Squires, R.*, Interfacing between SCADA systems and substation communications networks, Developments in Power System Protection, 1993, Fifth International Conference on , 1993 Pages:9 - 12

*Slater, A.*, PC and SCADA based energy management techniques, Advanced SCADA and Energy Management Systems, IEE Colloquium on , 6 Dec 1990 Pages:4/1 - 4/2

*Lai, L.L.*, The impact of new technology on energy management systems and SCADA, Advanced SCADA and Energy Management Systems, IEE Colloquium on , 6 Dec 1990 Pages:1/1 - 1/3

IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, IEEE Std 1379-2000 (Revision of IEEE Std 1379-1997), 21 September 2000

*Curtis, Ken, A.*, DNP3 Protocol Primer, DNP Users Group, 1 June 2000

Fundamentals of Utilities Communication Architecture, Computer Applications in Power, IEEE , Volume: 14 , Issue: 3 , July 2001 Pages:15 - 21