Basics of Supervisory Control and Data Acquisition (SCADA) Systems

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.

Components of SCADA

SCADA systems consist of:

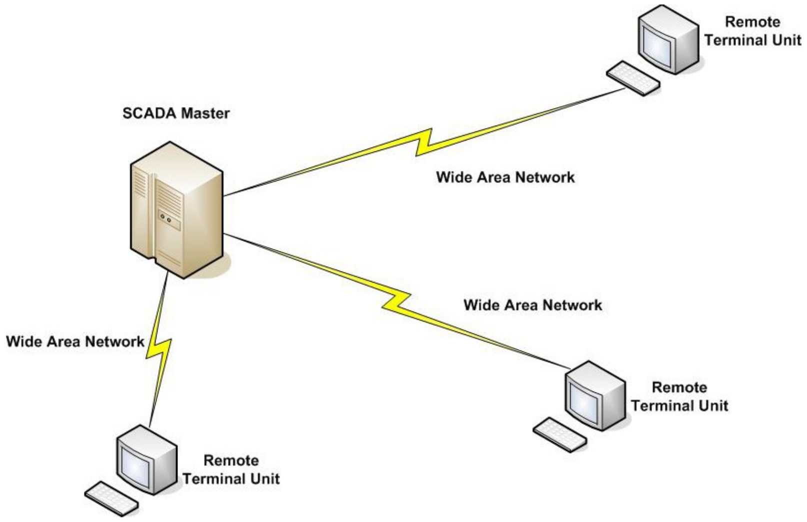
- One or more field data interface devices, usually RTUs, or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators
- A communications system used to transfer data between field data interface devices and control units and the computers in the SCADA central host. 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.

SCADA Architectures

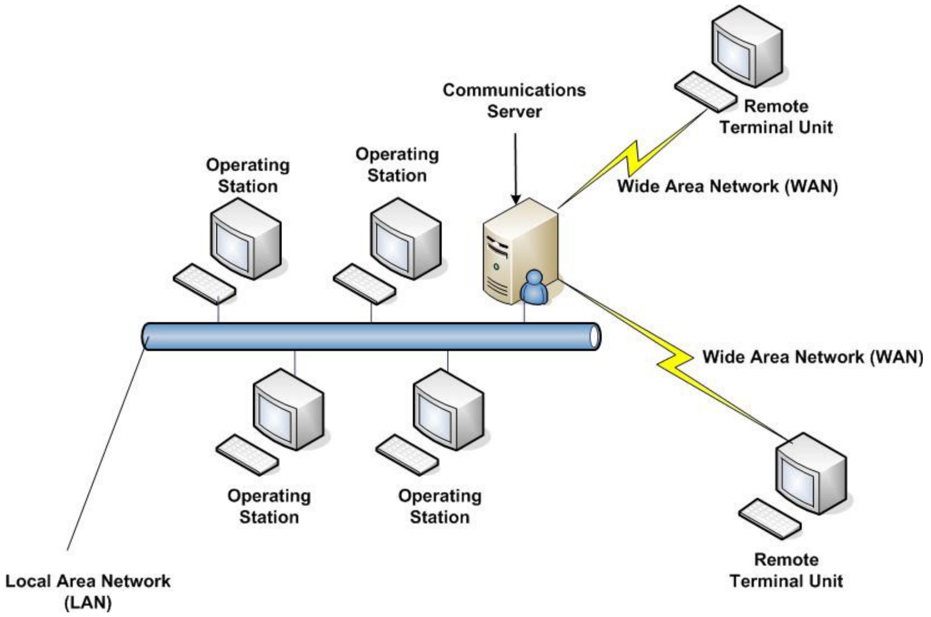
SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology. The following sections will provide a description of the following three generations of SCADA systems:

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



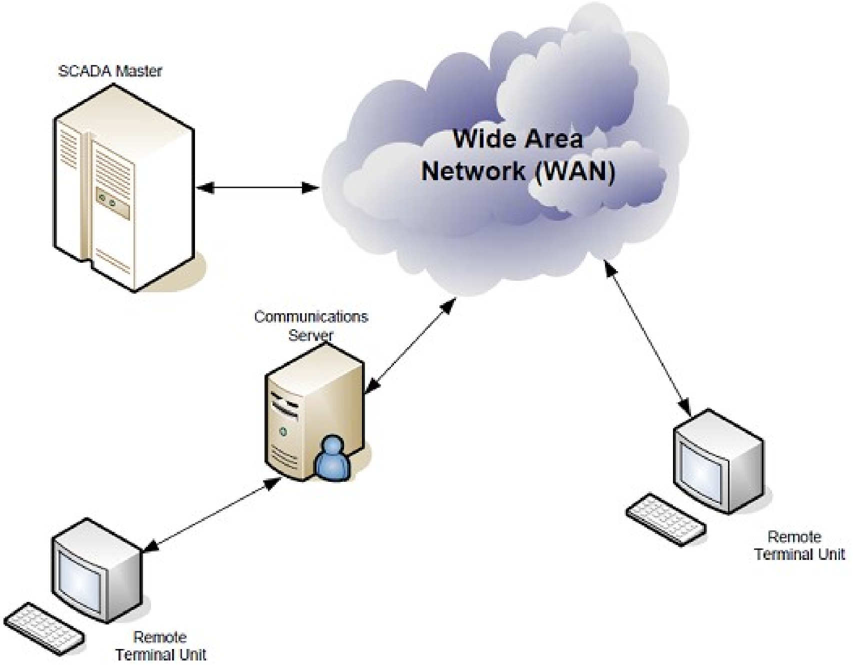
First Generation – Monolithic Architecture

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.



Second Generation – Distributed Architecture

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



Third Generation – Networked Architecture

The present (third) generation 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 multiple networked systems, sharing master station functions. There are RTUs utilizing protocols that are vendor-proprietary as before. But, 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.

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.

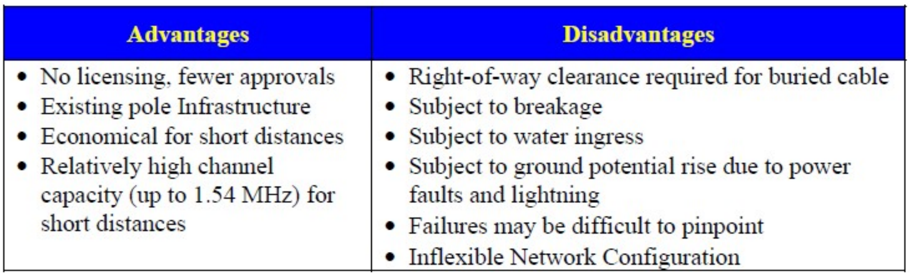
Each protocol consists of **two message sets or pairs**. One set forms the **master protocol**, containing the valid statements for master station initiation or response, and the other set is the **RTU protocol**, containing the valid statements an RTU can initiate and respond to. In most but not all 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).

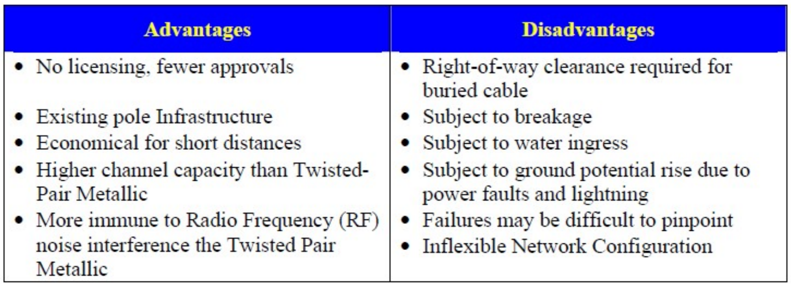
Deploying SCADA Systems

- **Twisted-Pair Metallic Cable**



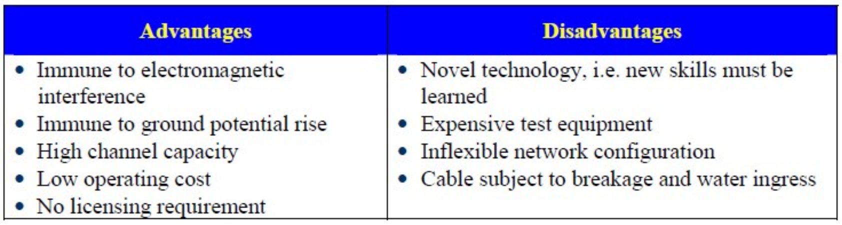
Advantages	Disadvantages
• No licensing, fewer approvals • Existing pole Infrastructure • Economical for short distances • Relatively high channel capacity (up to 1.54 MHz) for short distances	• Right-of-way clearance required for buried cable • Subject to breakage • Subject to water ingress • Subject to ground potential rise due to power faults and lightning • Failures may be difficult to pinpoint • Inflexible Network Configuration

- **Coaxial Metallic Cable**



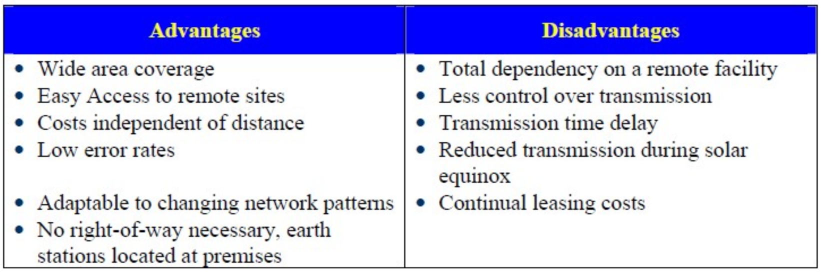
Advantages	Disadvantages
• No licensing, fewer approvals • Existing pole Infrastructure • Economical for short distances • Higher channel capacity than Twisted-Pair Metallic • More immune to Radio Frequency (RF) noise interference the Twisted Pair Metallic	• Right-of-way clearance required for buried cable • Subject to breakage • Subject to water ingress • Subject to ground potential rise due to power faults and lightning • Failures may be difficult to pinpoint • Inflexible Network Configuration

- **Fiber Optic Cable**



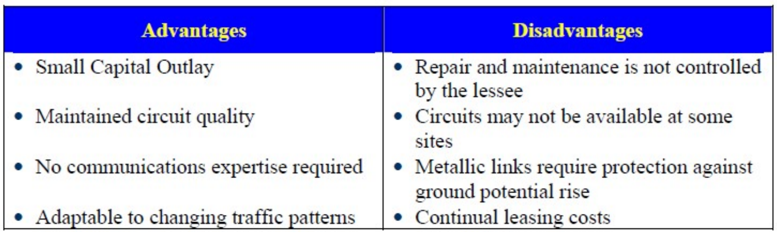
Advantages	Disadvantages
• Immune to electromagnetic interference • Immune to ground potential rise • High channel capacity • Low operating cost • No licensing requirement	• Novel technology, i.e. new skills must be learned • Expensive test equipment • Inflexible network configuration • Cable subject to breakage and water ingress

- **Satellites**



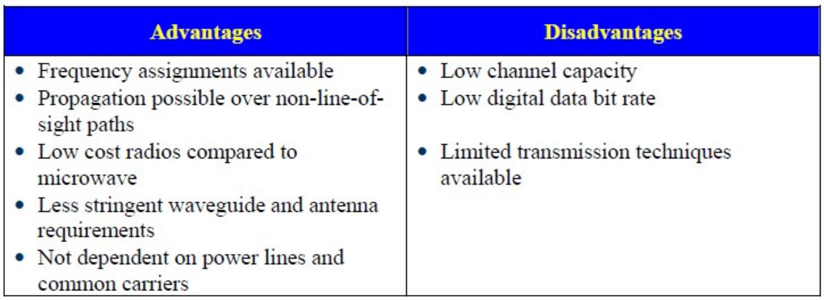
Advantages	Disadvantages
- Wide area coverage	- Total dependency on a remote facility
- Easy Access to remote sites	- Less control over transmission
- Costs independent of distance	- Transmission time delay
- Low error rates	- Reduced transmission during solar equinox
- Adaptable to changing network patterns	- Continual leasing costs
- No right-of-way necessary, earth stations located at premises	

- **Leased Telephone Lines**



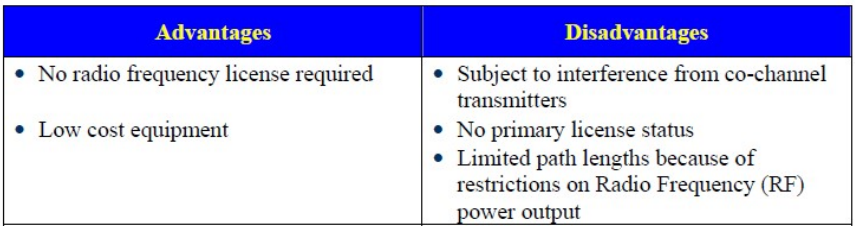
Advantages	Disadvantages
- Small Capital Outlay	- Repair and maintenance is not controlled by the lessee
- Maintained circuit quality	- Circuits may not be available at some sites
- No communications expertise required	- Metallic links require protection against ground potential rise
- Adaptable to changing traffic patterns	- Continual leasing costs

- **Ultra High Frequency Radio**



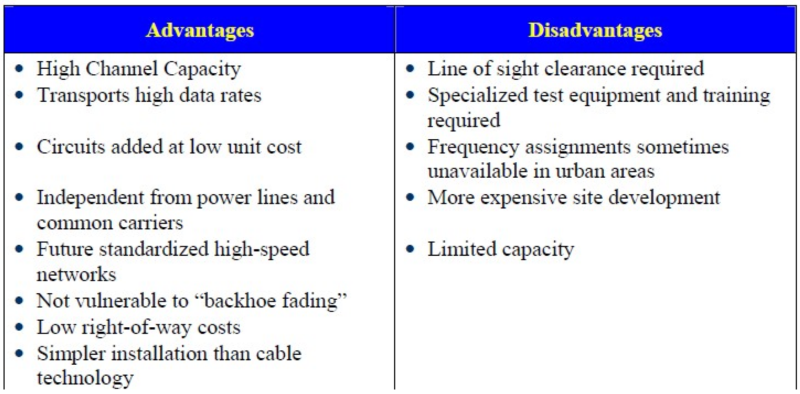
Advantages	Disadvantages
- Frequency assignments available	- Low channel capacity
- Propagation possible over non-line-of-sight paths	- Low digital data bit rate
- Low cost radios compared to microwave	- Limited transmission techniques available
- Less stringent waveguide and antenna requirements	
- Not dependent on power lines and common carriers	

- **Spread Spectrum Radio**



Advantages	Disadvantages
- No radio frequency license required	- Subject to interference from co-channel transmitters
- Low cost equipment	- No primary license status
	- Limited path lengths because of restrictions on Radio Frequency (RF) power output

- **Microwave Radio**



Advantages	Disadvantages
• High Channel Capacity	• Line of sight clearance required
• Transports high data rates	• Specialized test equipment and training required
• Circuits added at low unit cost	• Frequency assignments sometimes unavailable in urban areas
• Independent from power lines and common carriers	• More expensive site development
• Future standardized high-speed networks	• Limited capacity
• Not vulnerable to "backhoe fading"	
• Low right-of-way costs	
• Simpler installation than cable technology	

SCADA Security Risks

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, 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.

These connections provide 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)

Security Strategy

- **Proxy Servers and Firewalls**
- **Policies and Procedures** associated with remote vendor and supervisory access, password management
- **SCADA Server Operating System**
- **SCADA Applications**

In summary, these multiple "*rings of defense*" must be configured in a complementary and organized manner.

SCADA Standards Organizations

- The Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- Electric Power Research Institute (EPRI)
- International Electrotechnical Commission (IEC)
- DNP3 Users Group