COMMUNICATION NETWORK

General Overview of SCADA Communications

Without a properly designed communication network system, a SCADA system cannot exist. All supervisory control and data acquisition aspects of the SCADA system rely entirely on the communication system to provide a conduit for flow of data between the supervisory controls, the data acquisition units, and any controllers that may be linked to the system. The purpose of a communications network within a SCADA system is to connect the remote terminal units (RTUs) with the SCADA Master. Figure 1 below illustrates the communications network of SCADA equipment.

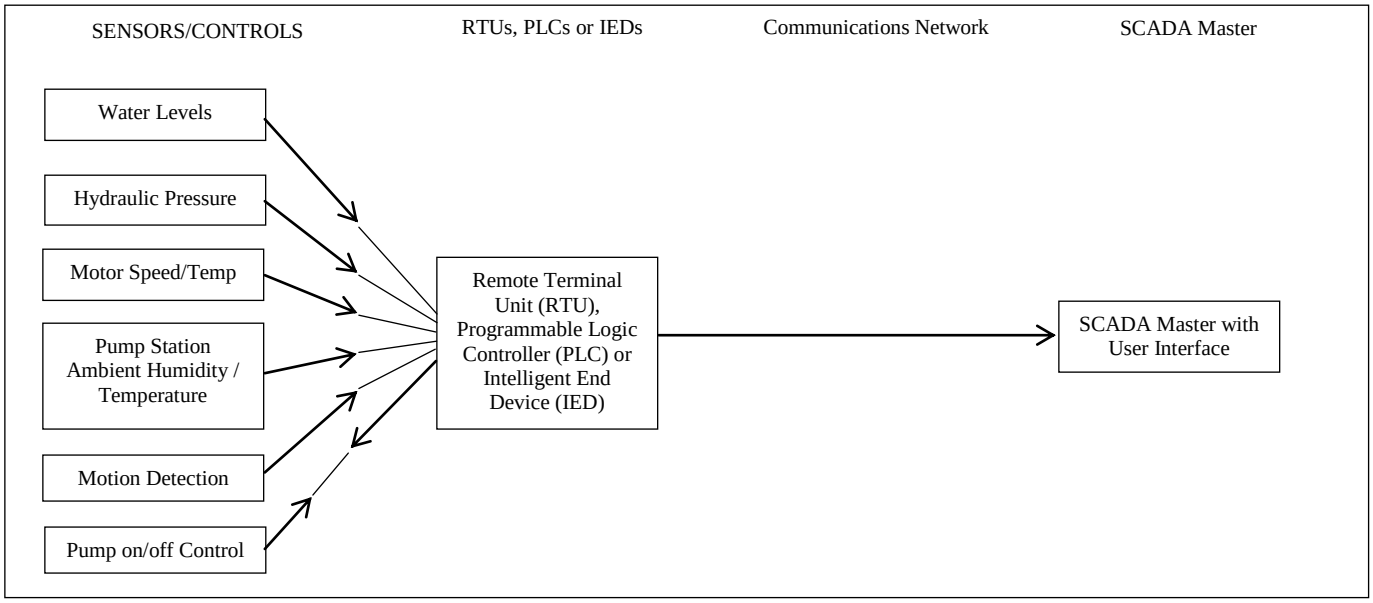

Figure 1. SCADA Components

Communications Network Options

The data can be transmitted through a variety of different communications platforms such as:

Ethernet - A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information

Telephone Line - A system that utilizes electrical signals in order to transmit data over a distance using a single pair of copper (traditionally) wires.

Optical Fiber Line- Similar to the traditional copper telephone lines, but differs by utilizing optical fibers made of glass or plastic and uses light to transmit the data, with is faster and has less losses as compared to copper wires.

Radio/Wireless - A system that uses radio transmitters and receivers to send data over short distances. Typically requires line of sight for best application.

Cellular - Based on the cellular phone technology to transmit data, regardless of distance, but dependent on cellular signal coverage.

Satellite - Similar to the cellular phone platform, but utilizing satellites instead of ground-based cellular towers.

Wi-Fi - A technology increasing in popularity that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed internet connections. Earlier generation Wi-Fi systems can be notoriously insecure; Wireless Equivalent Privacy [WEP] is relatively easy to compromise, so care must be taken when selecting Wi-Fi equipment to ensure that it supports robust security. WPA2 is present in almost all currently available equipment, and its use should be mandated.

Microwave – A system for providing long-range connectivity between two sites, utilizing either inexpensive public frequencies or FCC-licensed spectrum. Some microwave units are an extension of Wi-Fi – but for long range (20+ miles), others use proprietary protocols.

To meet security and performance specifications, it is important to consider the endpoint of each connection. Point-to-point connections (such as Ethernet, Fiber, and Microwave) typically terminate at a central system management facility. Cellular systems may provide an Internet connection requiring additional security, and phone-line systems must be protected against security breaches through the standard land-line, twisted-pair copper wire network.

It is also important to consider the privacy offered by a solution; wireless solutions in particular need to pay attention to the possibility of a nearby device eavesdropping on an otherwise secure conversation. This can have profound implications if private data such as passwords are included in the gathered data.

Finally, it is important to remember that these technologies are not mutually exclusive. A site can readily use a combination of Wi-Fi and Ethernet locally, and transmit the entirety of the site's data to a central point through fiber, microwave or other longer-range technology.

All of these communications methods fall under either hardwire or wireless category. Hardwire communication options include dedicated hardwire (i.e. Ethernet cable), fiber optic (i.e. light pipe), telephone wire (i.e. copper pair), or coaxial cable. Options for wireless data transmission include but are not limited to include satellite, radio, cellular, and Wi-Fi. Current industry trends suggest that wireless communication systems will continue to gain a larger market sector of the SCADA communication platforms, especially for large distributed networks such as water distribution systems where there is a need for a vast coverage area, perhaps in remote locations not readily accessible to existing hardwires. The same industry trends indicate that Ethernet is becoming the preferred communications standard for local area SCADAs, such as a water treatment plant. (Ritchie, 2011).

Wireless and hardwire options can be used alone or in tandem depending on the size and nature of the system. Factors to consider in selecting communication options include:

Coverage area of SCADA system. For example, is the SCADA only for the local water plant, or does it include an entire, widely dispersed distribution system, as well as the water plant?

If a system-wide SCADA, then consideration must be given to the size and terrain of the distribution system. For example, wireless may be a less expensive option, but the communications system would require adequate line of sight between the radio transmitters/receivers.

Local availability of infrastructure and its proximity to the system feature that will require a SCADA sensor is also relevant. For example, if an there is an existing telephone line to a particular site where a sensor needs to be installed, then that telephone line may be the best option.

Growth of the community could affect the SCADA system performance and future expandability as well as the ability to upgrade the system easily and budget for the system.

Some of the more significant advantages and disadvantages are summarized in Table 1. Most modern SCADA systems use a variety of communication options within one system to meet their needs. Typically, there is not a one size fits all solution and SCADA communications should be tailor made to fit a utility's needs.

Communications Network Features and Considerations

When selecting a communications system for plant operations, it is common to use only hardwire to connect remote equipment to the SCADA Master given the short distances involved. When using hardwired lines to communicate with remote sites in the distribution system, distance, reliability and time responses are all limiting factors in the design process. New construction of hardwire communication networks are not practical when trying to connect to distant system components, such as a pump station on the other side town. In situations where it is not economically feasible to run an independent hardwire for each remote site, one may elect to tap into existing infrastructure or elect to use a form of wireless communication. If a utility elects to use pre-existing infrastructure several options are available including dial-up or leased telephone lines or fiber networks. The type of platform selected often depends on the bandwidth required to perform remote operations such as pumping, or the polling frequency (e.g. how often do you need to collect data).

Inaccessible sites or lack of "wire" type of infrastructure may necessitate the use of wireless communications systems, but regardless of terrain, distance, or accessibility, current trends suggest a growing affinity to use wireless options to replace hardwire systems. Wireless communication provides utilities with the following benefits versus traditional hardwire systems: scalability, deployment speed, reduced network and construction costs, and reduced maintenance and repair of hard wires. The scalability (or ability to quickly expand as the system grows) of a wireless network is a great advantage over wired systems. Increasing SCADA system coverage can be achieved without running wire or other costly labor items and can be installed in a relatively short period of time which offers savings over hardwire systems. Wireless systems can also expand independent of existing infrastructure to meet the needs of a growing community. The advantages of wireless can be seen in Figure 2.2.3-A. Consider the image in this figure spread out over a twenty square mile area and the relative costs of a wireless system versus a hardwire system. Now consider the replacement costs after 20 years of technological innovation. The ability to upgrade remote sites on an individual basis versus system wide is a clear advantage and provides a degree of assurance as land lines become phased out. Existing

hardwire systems may also be supplemented with wireless systems on a per unit level as new operations come on-line. For cellular systems reliability and availability of service should be taken in to consideration.

Hardwired		
	Advantages	Disadvantages
Telephone Line	May already exist to site(s). Very mature technology.	May be monthly lease charge(s). Consider who is responsible for fixing problems on the line and if it is a third party, what is their track record for repair responses. Typically slow and limited data transmission.
Ethernet	Good application for local site, such as a water treatment plant.	Limited application range. Cannot be utilized over distances greater than 1000' without boosting signal. Can be prone to lightning damage without significant protection measures.
Fiber Optic	Best direct connection with the fastest data transmission. Large bandwidth allows for video applications (i.e. security cameras) to part of the SCADA system.	May be significant monthly lease charge(s). If the fiber does not already exist, the capital costs for the initial project could have a very high. Fiber is also typically very expensive to repair.
Coaxial Cable	May already exist to the site(s). Very mature technology. Better data bandwidth than a telephone line.	May be monthly lease charge(s). Depending on the setting, this type of hardwire is less common than a telephone line.
Wireless		
	Advantages	Disadvantages
UHF and VHF Voice Radio	Generally very low maintenance and can usually be repaired by a local radio shop.	FCC license required, along with periodic fees and renewals.
900Mhz spread spectrum and 2.4Ghz Data Radio	No FCC license necessary and transmit data at a higher rate.	Requires line of sight for best application. Some 900Mhz require FCC license.
Wi-Fi	Potentially very good option for a local site application, such as a water treatment plant.	Very limited ranges (typically 300 ft or less), and the signal can be significantly diminished by structures. Wi-Fi requires careful security assessment.
Microwave	Potentially very good option for linking sites with good elevation, such as water towers.	Requires expert assistance with installation. Some frequencies require FCC licensing.
Cellular	Quickly gaining in popularity, especially as pricing continues to decline and for areas that may not have strong radio signals or line-of-sight conditions.	The area for coverage should have good, consistent cellular coverage.
Satellite	Good application where there is no, or unreliable cell coverage, such as extreme terrains, very remote locations, etc.	May become a viable option in the future, but is currently not cost-effective except in the most extreme cases.

Table 1 – Differences between hard-wired and wireless communication systems.

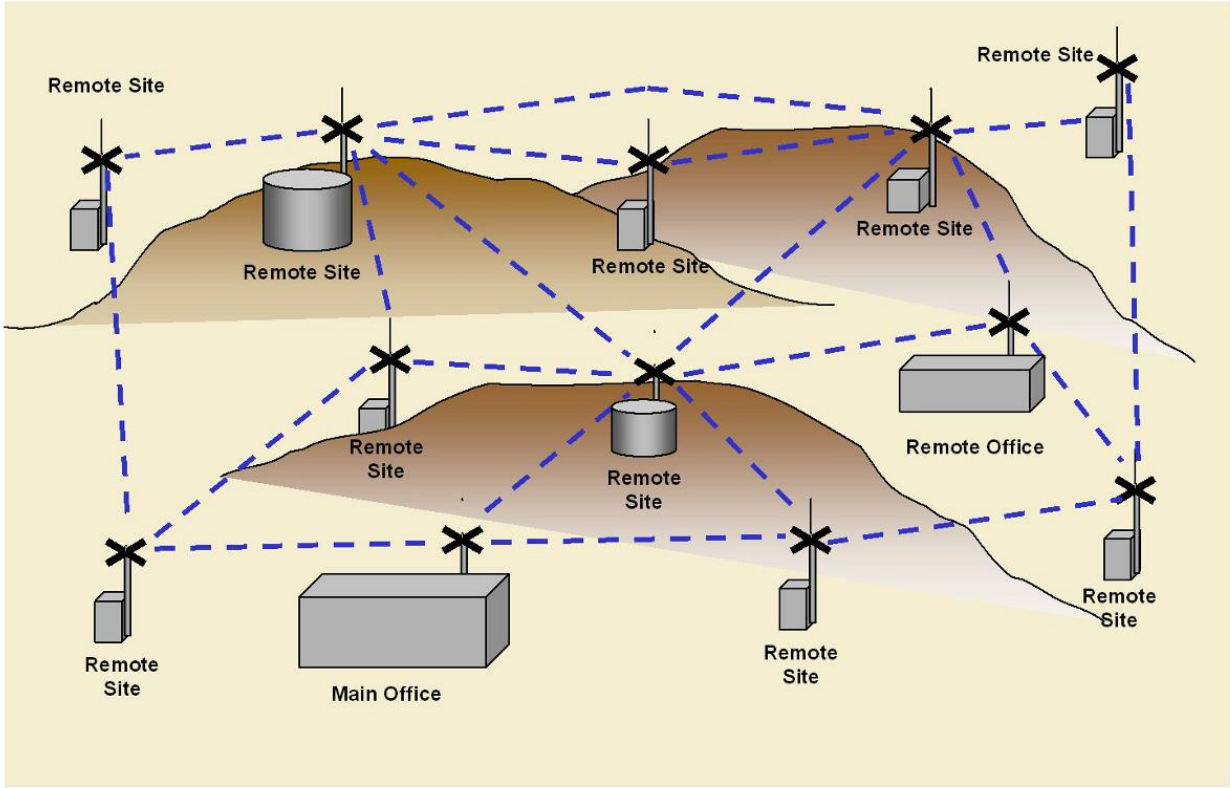

Figure 2. Typical SCADA Communication Network Configuration

Communication Security

Security is an important consideration when designing a SCADA network. Many existing SCADA systems have been found wanting in this regard, leaving essential systems vulnerable to outside influence.

Security should be considered on three levels:

- **Perimeter Security**, limiting access to systems and network equipment from unauthorized sources.
- **Interior Security**, requiring at the very least a login to access important infrastructure.
- **Transport Security**, ensuring that it is difficult to illicitly access a network segment in an attempt to gain control.

Additionally, a cohesive security plan requires the following components:

- **Authentication**, answering the question "who are you?" This is typically handled with a login requirement (user's name and password), although more secure systems are possible. Ideally, a system should be compatible with a centralized login security system, preventing the need to visit each device in order to revoke authorization whenever personnel changes.

- **Authorization**, answering the question "what are you allowed to do?" This dove-tails with authentication. Again, an ideal system will centralize this authority permitting rapid revocation of authorization in the event of personnel changes or a security breach.
- **Accounting**, answering the question "who did what?" In essence, this is an audit-trail, allowing you to see which user performed what operation, and when they did it. This can be an essential element of understanding an incident after it occurs, or catching it as it begins.