SCADA SYSTEMS

Class # 3070

Ian Metcalfe
ClearSCADA Sales
Control Microsystems
90 Madison St, #600
Denver, CO 80206

Introduction

The definition of SCADA is 'Supervisory Control and Data Acquisition'. The major function of SCADA is for acquiring data from remote devices such as valves, pumps, transmitters etc. and providing an overall control remotely from a SCADA Host software platform. This provides process control locally so that these devices turn on and off at the right time, supporting your control strategy and a remote method of capturing data and event (alarms) for monitoring these processes. SCADA Host platforms also provide functions for graphical displays, alarming, trending and historical storage of data.

Historically, SCADA products have been produced that are generic with a 'one shoe fits all' approach to various markets. As SCADA has matured to provide specific solutions to specific SCADA markets it has provided solutions for wide area network SCADA systems that rely on tenuous communication links. These types of SCADA systems are used extensively throughout the Oil & Gas market due to the fact that assets are spread over large geographical areas.

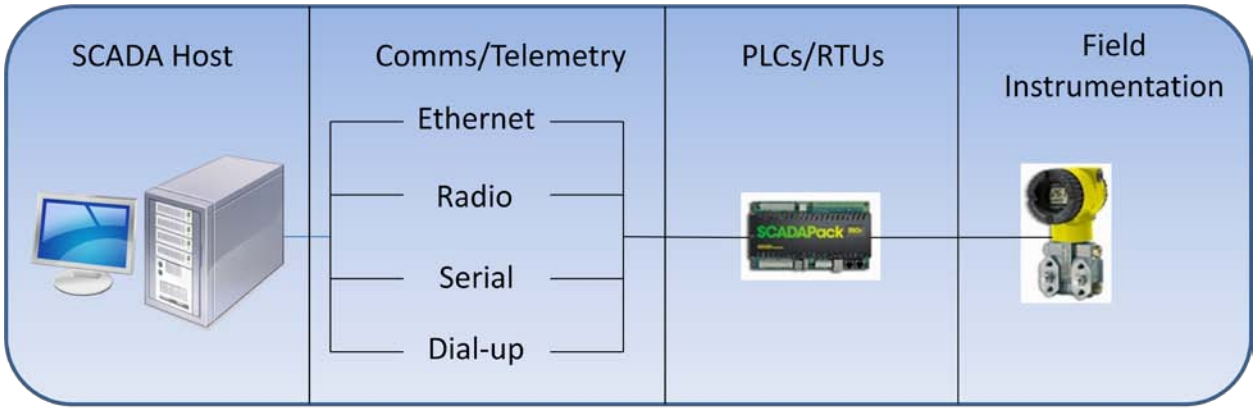

Figure 1: SCADA System Overview

Looking at the overall structure of a SCADA system, there are four distinct levels within SCADA, these being;

i. Field instrumentation,
ii. PLCs and / or RTUs,
iii. Communications networks and
iv. SCADA host software.

We will discuss each of these levels in detail describing their function and how this has changed over the past 30 years and the impact of security requirements and regulatory compliance.

Field Instrumentation

"You can't control what you don't measure" is an old adage, so instrumentation is a key component for a safe and optimized control system. Traditionally, pumps and valves would have been manually controlled i.e. an operator would start/stop pumps locally and valves would have been opened/closed by hand. Slowly, over time these instruments would have had feedback sensors fitted such as limit switches providing connectivity for these wired devices into a local PLC or RTU so that this data could be relayed to the SCADA host software.

	Early instrumentation	Feedback sensors	Add actuators
Pro	Cheap to install	Central View	Central control
Con	Expensive to operate	Still expensive to operate	Higher Technical Requirements

Figure 2: Progress of instrumentation

Although today's instrumentation requires more technical knowledge and ability to design, install and maintain, this is mitigated by the reduced cost in automating processes and higher technical skills by personnel. Today most field devices such as valves have actuators fitted so a PLC or RTU can control the device rather than require manual manipulation. This capability means the control system can react quicker to optimize production or shutdown under abnormal events.

In terms of regulatory compliance, instrumentation for the oil & gas industry has had to comply with hazardous class, division and group classifications. The requirement is that the instrument has to be designed for the location or area that it has been placed, for example, due to the existence of explosive vapors during normal operating conditions or during abnormal conditions.

In many cases the instrument is also required to exist in harsh environments. Many types of instrumentation are design for these extremes of hot and cold. If the instrumentation is not design for these temperatures an artificial environment within a cabinet or some sort of building is required, this comes at an extra cost not just in initial design but also for ongoing maintenance.

Instrumentation has to comply with any EMC standards. EMC standards are electromagnetic compatibility ensuring an electrical device does not have any undesirable effects upon its environment or other electrical devices within its environment.

PLCs and RTUs

Programmable Logic Controllers (PLCs) and Remote Telemetry Units (RTUs) used to be distinctly different devices but over time they are almost the same, this has been a convergence of technology as manufacturers of these devices expanded their capabilities to meet market demands.

If we go back 30 years, an RTU was a 'dumb' telemetry box for connecting field instruments. The RTU would 'relay' the data from the instruments to the SCADA host without any processing or control but had well developed communication interfaces or telemetry. In the 1990's control programming was added to the RTU so now it operated more like a PLC. The PLCs on the other hand could always do the control program but lacked the communications interfaces and data logging capability and this has been added to some extent over the past 10 years.

A further development of devices in the field is to offer a specific application that would incorporate a number of instruments and devices with an RTU/PLC, incorporating technology sets to provide an 'off the shelf' approach to common process requirements, e.g. gas well production that includes elements of monitoring, flow measurement and control that would extend as an asset into the SCADA Host.

In terms of environmental and regulatory compliance PLCs and RTUs have the same type of requirements as instrumentation as they operate in the same environment. Traditionally PLCs have not been as environmentally compliant as RTUs. This is mainly due to the fact that PLCs were designed to operate in areas where the environment conditioned to some degree, such as factory floors.

Communications Networks

The communication network is necessary to relay the data from the remote RTU/PLCs which is out in the field or along the pipeline to the SCADA host located at the field office or central control center. With assets distributed

over a large geographical area, communications is the glue or the linking part of a SCADA system and is essential to its operation. How well a SCADA system can manage communication to remote assets is fundamental to how successful the SCADA system is.

20 years ago the communication network would have been leased lines or dial up modems which were very expensive to install and maintain but in the last 10-15 years many users switched to radio or satellite communications to reduce costs and eliminate the problematic cabling issues. More recently other communications types have been made available that include cellular communications and improved radio devices that can support greater communications rates and better diagnostics. However, the central issue that these communication medium are still prone to failure is a central issue to modern distributed SCADA systems.

At the same time as the communication medium changed so did the protocols. Protocols are electronic languages that PLC's and RTU's use to exchange data, either with other PLC's and RTU's or SCADA Host platforms. Traditionally, protocols have been proprietary and the product of a single manufacturer. As a development forward from this, many manufacturers gravitated to a single protocol, MODBUS, but added on proprietary elements to meet functionality requirements. For the Oil & Gas industry there are a number of variants of MODBUS, including but not limited to, ASCII MODBUS, RTU MODBUS, Enron MODBUS and TCP/IP MODBUS. For the Oil & Gas industry this provided a part standard for communications to retrieve flow or process data from a particular RTU or PLC.

This step development in using MODBUS variants was seen as an improvement but it still tied a customer to a particular manufacturer, this is still very much the case today. A good example of this would be how historical flow data is retrieved from a RTU/PLC to a SCADA Host Platform. However, the advancement of SCADA Host software and in some cases the sharing of protocol languages meant that many of the issues with proprietary element have been further resolved.

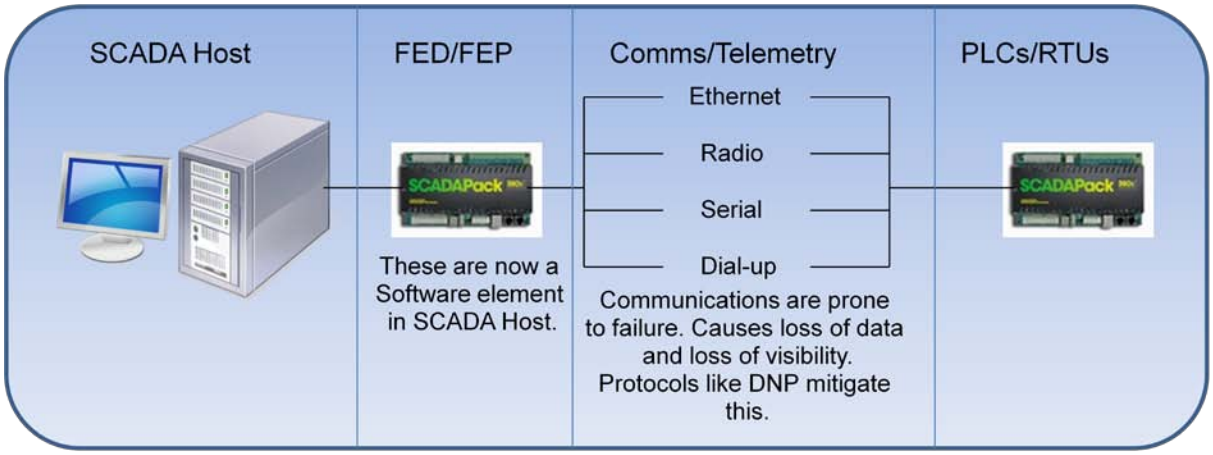

Figure 3: Wide Area Network SCADA

In more recent year protocols have started to appear that are truly non-proprietary, such as DNP (Distributed Network Protocol). These are protocols that have been created independent of any single manufacturer and are more of an industry standard in that many individuals and manufacturers have subscribed to these protocols and contributed to their development. However, these protocols have yet to develop significantly enough to have a broad appeal to the application process and regulation requirements for Oil & Gas markets. Consequently the oil and gas market is still heavily invested in MODBUS variants. As the benefit of these protocols becomes apparent to users in the Oil & Gas market it is expected that they will begin to be generally accepted and standard solutions provided for Oil & Gas market requirements.

Host Software

Traditionally, SCADA Host software has been a mechanism to view Graphical displays, alarms and trend. Control from SCADA Host Software Platforms only became available when control elements were available for remote instruments.These systems were isolated from the outside world and were only the tools of operator, technician and engineers with responsibility to monitor, maintain and engineer the processes and SCADA elements. With the

advancements in Information Technology (IT) this is no longer the case. Many different stake holders now require access and real time access to the data that SCADA Host software generates. Accounting, maintenance manager, material purchasing requirements are preformed or partly preformed from data derived from SCADA system.

Therefore there is a drive for SCADA Host Platform to be an Enterprise entity providing data to a number of different users and processes. This has required SCADA Host Software to adopt standards and mechanism to support interfacing to these systems. It also means that IT, traditionally separated from SCADA systems are now involved in helping maintaining networks, database interfacing and user access to data.

Many of the initial SCADA Host software products were developed specifically for the manufacturing environment where a SCADA system resided within a single building or complex, so did not posses many of the telemetry communication features required by SCADA system for geographically distributed SCADA assets.

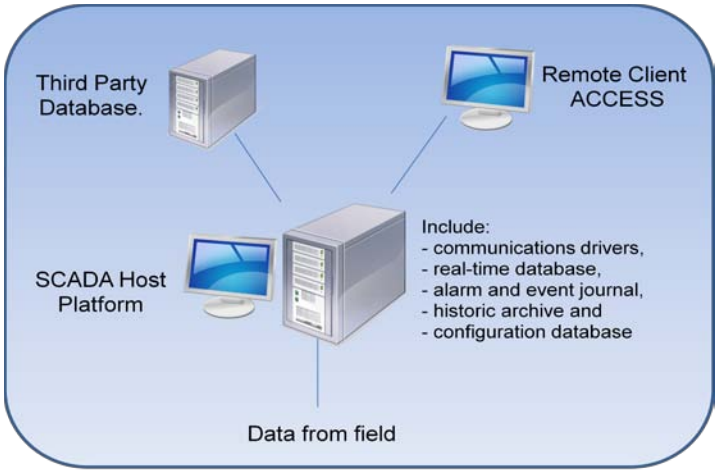

Figure 4: SCADA Host Platform

For communications with these types of initial SCADA Host platforms if was often required that a hybrid PLC or RTU called a Front End Driver (FED) or Front End Processor (FEP) be used to handled the communications with remote devices. This had a number of disadvantages as it required specialized programming external to the SCADA Host platform and provided a communications bottleneck. Although multiple FED or FEP devices resolved some of this, they were extra costs and difficulties in creating and maintaining them due to their specialized nature. Modern SCADA software that encapsulates telemetry functionality no longer require these types of hybrid PLCs for communications, they now use software programs called ‘drivers’ that are integrated into the SCADA Host Platform. Software drivers hold the different types of protocol electronic languages to communicate with remote devices such as RTUs and PLCs.

As the technology developed SCADA Host software platforms were able to take advantage of many new features. These included the development of integral databases that are specifically design for SCADA Host software requirements, they are able to handle thousands of changes a second for really large systems yet still conform to standard database interfacing such as Open Database Connectivity (ODBC) and Object linking and Embedding for Databases (OLE DB). These standards are required so that third party databases can access data from the SCADA Host software. Client access to the SCADA Host Platform remote from its location is another technology that has enabled users of SCADA Host Platform the ability to operate and monitor SCADA systems while on the move or at other locations.

There is a drive in terms of operational safety for SCADA Host Systems within the Oil & Gas industry. 49 CFR 195.446 Control Room Management regulations look at SCADA Host software and how it operates in terms of operations, maintenance and management. It also covers the actual SCADA system itself in terms of how integrated it is and the use of open Architecture and standards.

Security

Security for SCADA systems has in recent years become an important and hotly debated topic. Traditionally SCADA systems were isolated entities that were the realm of operators, engineers and Technicians. This has meant that SCADA Host platforms were not necessarily developed to have protected connections to public networks. This leaves many SCADA Host platforms open to attack as they do not have the tools necessary to protect themselves.

In terms of remote assets communicating back to a SCADA Host, this has been a problem for many years with attacks on SCADA system documented. However, it has only been in recent years that an open standard has been produced to provide secure encrypted and authenticated data exchanges between remote assets and a SCADA Host Platform.

Solutions to security for communicating to remote assets and security for SCADA host platform have very different requirements. Also, security has to be viewed overall not just in terms of the SCADA system itself. For example, if somebody wanted to disrupt production, they would not necessarily need to access the SCADA system to do this. If a site for a gas well head or a monitoring point on a gas pipeline is remote, it could be easily compromised by a trespasser. If the asset is important and critical other solution that may or may not form part of the SCADA system would have to be consider e.g. camera security.

A large number of unauthorized accesses to a SCADA system come not from or at the remote assets themselves but through the SCADA host platform or computers used to access the SCADA system for diagnostic or maintenance purposes. The recent attack using the Stuxnet virus was introduced via a thumb drive on a computer used to access a SCADA system.

There are a number of standard available that describe how to secure a SCADA system not just in terms of the technology employed but in terms of practices and procedures. This is very important as the security solution to SCADA is not a technological silver bullet, but a series of practices and procedure in conjunction with technological solutions. The practices and procedure would include items of training, SCADA Platform access and procedure to follow when SCADA security has been compromised, just to name a few. In modern SCADA systems IT departments are integral to implementing and maintaining SCADA security for an organization and should be included in setting up practices, procedure and implementing technology.

Summary

SCADA system have made use of the various technological advances to drive forward the proficiency of SCADA systems. From the introduction of Actuators and transducers at instrumentation levels that made monitoring of processes easier, more accurate and less costly to the introduction of open standards to make the interchange of data between a SCADA system and other processes within an organization.

The drive of modern SCADA systems is to:

- Provide Instrumentation and RTUs/PLCs for asset or process solutions that can be easily managed and provide operational benefits from the SCADA host down to instrumentation, not just in terms of controlling and retrieving data but in terms of engineering, implementing, operating and maintaining these assets.

- Develop and employ open standards to further ease the integration of assets within a SCADA system using best practices defined by open groups and not a single manufacturing entity. This will in turn reduce the cost of owning SCADA.

- Provide secure environments for SCADA systems and the assets or processes by not only providing technology solutions but by implementing a series of practices and procedure.