# SCADA Systems

March 2012 / White paper

by Schneider Electric
Telemetry & Remote SCADA Solutions

Make the most of your energy

Schneider Electric

# Summary

# Executive summary

This white paper discusses the various components found in a typical Remote SCADA System, the operational challenges inherent in these types of systems, and how various technological advances have been implemented to drive forward SCADA System proficiency.

# 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 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 events (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.

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, how SCADA has changed over the past 30 years and the impact of security requirements and regulatory compliance on SCADA system operations.

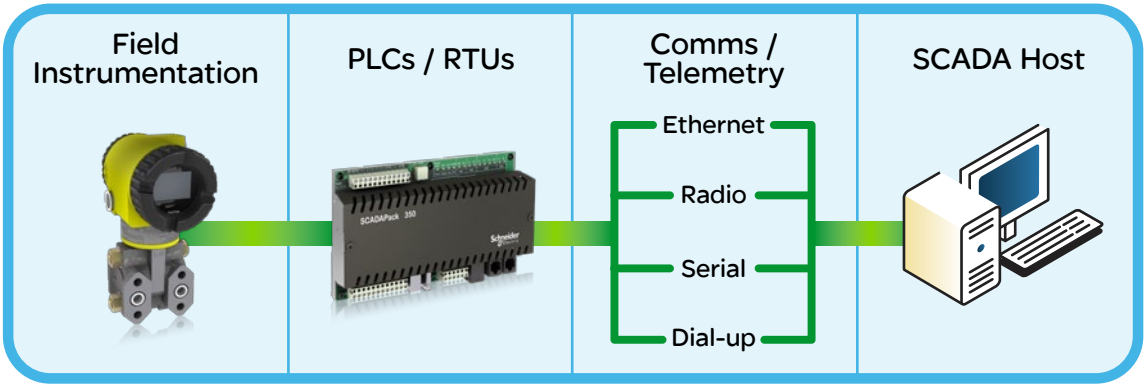


Figure 1:
SCADA System Overview

# Field Instrumentation

"You can't control what you don't measure" is an old adage, meaning that instrumentation is a key component of a safe and optimised control system. Traditionally, pumps and their corresponding operational values 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 been fitted with feedback sensors, such as limit switches, providing connectivity for these wired devices into a local PLC or RTU, to relay data to the SCADA host software.

| | Early instrumentation | Feedback sensors | Add Actuators |
|---|---|---|---|
| Pro | Installation is cost-effective | Central view | Central control |
| Con | Expensive to operate | Still expensive to operate | Higher technical requirements |

Figure 2:
Progress of Instrumentation

Although today's instrumentation technician requires more technical knowledge and the ability to design, install and maintain equipment, than in the past, this is mitigated by the reduced cost in automating processes and higher technical skills held by personnel. Today, most field devices such as valves have been fitted with actuators, enabling a PLC or RTU to control the device rather than relying on manual manipulation. This capability means the control system can react more quickly to optimise 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 must be designed for the location or area in which it has been placed, eg. an environment where the existence of explosive vapours during normal operating conditions, or during abnormal conditions, are known.

In many cases the instrument is also required to function in harsh environments. Many types of instrumentation are designed for extremes of hot and cold. If the instrumentation is not designed 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 must also comply with any EMC (electromagnetic compatibility) standards which may be in place, to ensure that 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 now 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 1990s control programming was added to the RTU so it operated more like a PLC. PLCs on the other hand could always do the control program but lacked communication interfaces and data logging capability, which has been added to some extent over the past decade.

A further development of devices in the field is to offer a specific application that could 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 in that they operate in the same environment. However, PLCs have traditionally not been as environmentally compliant as RTUs. This is mainly due to the fact that PLCs were designed to operate in areas, such as factory floors, where the environment was already conditioned to some degree.

# Remote Communications Networks

The remote communication network is necessary to relay data from remote RTU/PLCs, which are 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, communication is the glue or the linking part of a SCADA system and essential to its operation. How well a SCADA system can manage communication to remote assets is fundamental to how successful the SCADA system is.

Twenty 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 have switched to radio or satellite communications to reduce costs and eliminate the problematic cabling issues. More recently, other communication types have been made available that include cellular communications and improved radio devices that can support greater communication rates and better diagnostics. However, the fact that these types of communication media are still prone to failure is a major issue for modern, distributed SCADA systems.

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

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

In recent years, protocols have appeared that are truly non-proprietary, such as DNP (Distributed Network Protocol). These protocols have been created independently of any single manufacturer and are more of an industry standard; 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 benefits of these protocols become more apparent to users, it is expected that they will be more readily accepted and become a component of standard solutions provided specifically for oil and gas markets.

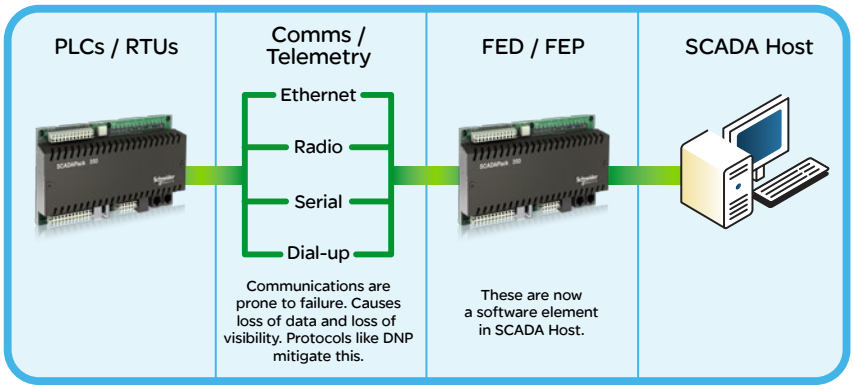


Figure 3:
Wide Area Network SCADA

# SCADA Host Software

Traditionally, SCADA Host software has been the mechanism to view graphical displays, alarms and trends. Control from the SCADA Host itself only became available when control elements for remote instruments were developed.These systems were isolated from the outside world and were the domain of operators, technicians and engineers. Their responsibility was to monitor, maintain and engineer processes and SCADA elements. With advancements in Information Technology (IT) this is no longer the case. Many different stake holders now require real time access to the data that the SCADA Host software generates. Accounting, maintenance management and material purchasing requirements are preformed or partly preformed from data derived from the SCADA system.

Consequently,  there is a drive for the SCADA Host to be an Enterprise entity providing data to a number of different users and processes. This has encouraged SCADA Host software development to adopt standards and mechanisms to support interfacing to these systems. It also means that IT, traditionally separated from SCADA systems, is now involved in helping to maintain networks, database interfacing and user access to data.

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

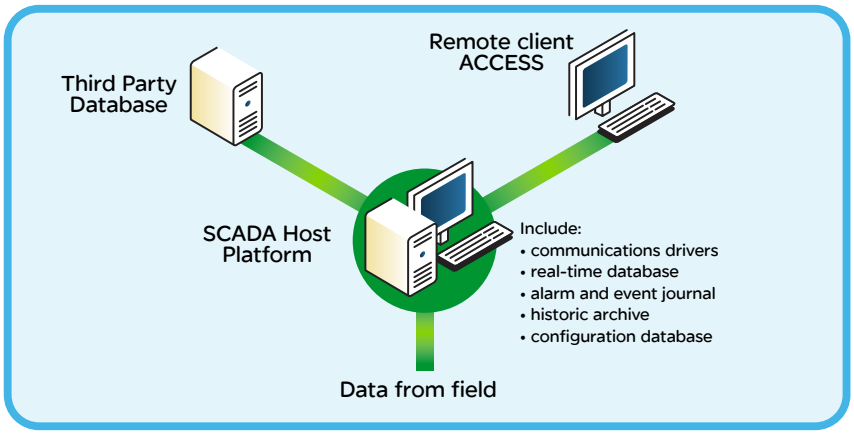


Figure 4:
SCADA Host Platform

These types of 1st-generation SCADA Hosts often required a hybrid PLC or RTU, called a Front End Driver (FED) or Front End Processor (FEP), to be used for handling communications with remote devices. This resulted in a number of disadvantages as it required specialised programming, external to the SCADA Host platform, and created a communications bottleneck. Although multiple FED or FEP devices resolved some of this, there were extra costs and difficulties in creating and maintaining them due to their specialised nature. Modern SCADA software that encapsulates telemetry functionality no longer requires these types of hybrid PLCs for communications. They now use software programs called 'drivers' that are integrated into the SCADA Host itself. Software drivers contain the different types of protocols to communicate with remote devices such as RTUs and PLCs.

As technology developed, SCADA Host software platforms were able to take advantage of many new features. These included the development of integral databases specifically designed for SCADA Host software requirements, being 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. Remote client access to the SCADA Host is another technology that has enabled users to operate and monitor SCADA systems while on the move between or at other locations.

There is a drive towards operational safety for SCADA Host systems within the oil and gas industry. 49 CFR 195.446 Control Room Management regulations look at SCADA Host software and how it functions in terms of operations, maintenance and management. It also covers the degree of integration of the SCADA system itself and its 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 left many SCADA host platforms open to attack as they did not have the tools necessary to protect themselves.

In terms of remote assets communicating back to a SCADA Host, security has been an issue for many years with numerous documented attacks on SCADA systems. However, it's 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 for remote asset and SCADA host communication security have very different requirements. Security has to also be viewed overall, and 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 gas wellhead site or a monitoring point on a gas pipeline is remotely situated, it could be easily compromised by a trespasser. If the asset is critically important, other solutions that may or may not form part of the SCADA system itself would have to be considered. e.g. camera surveillance security.

A large number of unauthorised accesses to a SCADA system come not from or at the remote assets themselves but through the SCADA Host or computers used to access the SCADA system for diagnostic or maintenance purposes. For example, 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 standards 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 since the security solution to SCADA is not a technological silver bullet, but a series of practices and procedures in conjunction with technological solutions. These practices and procedures would include items of training, SCADA Host access and procedures to follow when SCADA security has been compromised. In modern SCADA systems IT departments are integral to implementing and maintaining SCADA security for an organisation and should be included in setting up practices, procedures and implementing technologies.

# Conclusion

From the introduction of actuators and transducers (that made monitoring of processes easier, more accurate and less costly) at the instrumentation level to the introduction of open standards (to improve the interchange of data between a SCADA system and other processes within an organisation), SCADA systems have exploited the various technological advances to drive forward their proficiency.

The drive of modern SCADA systems is to:

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

Schneider Electric

**Telemetry & Remote SCADA Solutions**
48 Steacie Drive, Kanata, Ontario K2K 2A9 Canada
Direct Worldwide: 1 (613) 591-1943
Fax: 1 (613) 591-1022
Toll Free within North America: 1 (888) 267-2232
www.schneider-electric.com





Document Number TBUL00001-31

March 2012 tk