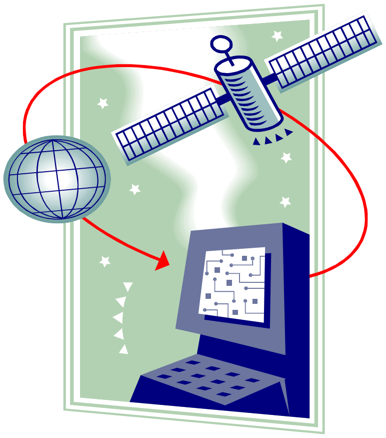
An Introduction to Internet-based SCADA



Donald I. Wallace

March 24, 2003

Table of Contents

Background

Equipment may be monitored and controlled remotely using supervisory control and data acquisition (SCADA) systems. SCADA systems comprise a remote terminal unit (RTU) connected to sensors and actuators mounted on the equipment; a long distance communications network such as leased telephone lines; and a central computer running programs that automatically collect sensor data and send commands to the RTU.

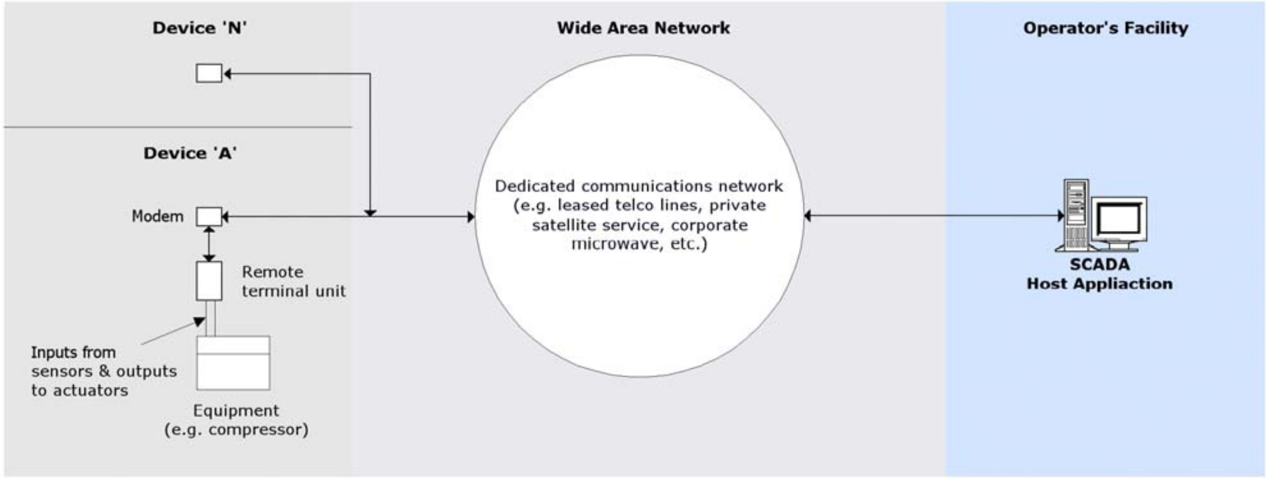

Device 'N'
Wide Area Network
Operator's Facility
Device 'A'
Modem
Remote terminal unit
Inputs from sensors & outputs to actuators
Equipment (e.g. compressor)
Dedicated communications network (e.g. leased telco lines, private satellite service, corporate microwave, etc.)
SCADA Host Appliaction

Figure 1: Traditional SCADA System

First Generation Systems

Early SCADA systems employed RTUs with little or no intelligence; they simply provided an interface to the equipment to collect the data from the sensors and a communications link to the host system. The host application organized and stored the data and then displayed it on a screen for operator evaluation and action. Control commands were entered by the operator and transmitted to the RTU for execution (e.g. a command may be issued to close a relay in the RTU, which in turn closes a relay on the equipment to shut it down).

Second Generation

More modern SCADA systems use RTUs with varying degrees of intelligence that allow much of the control strategy to be implemented locally. The host system is still updated, and the operator may override control instructions. In both cases, an average of about fifty RTUs may be connected to a single dedicated leased line arranged in a master/slave relationship, i.e. the host initiates all communications. This poll/response architecture results in significant redundant data traffic because each RTU responds to its poll with a full data set, irrespective of whether any changes have occurred or not.

Traditional SCADA host software is custom written (or highly customized) for each specific customer or application. The resulting code often requires significant effort to develop and maintain over the life of the system.

The Problem with Protocols

Communications protocols are a significant issue for all operational SCADA systems. A protocol is usually selected during early planning stages so that RTUs and host system software can be selected and/or developed around a common protocol. Today, this is often MODBUS protocol, but there are dozens to choose from because most manufacturers of measurement and control equipment use their own proprietary protocols. Expansion of an installed system is often restricted because all equipment added to the system must support the system's communications protocol, which perpetuates the "closed system" architecture and often makes it difficult and costly to incorporate new technology.

Benefits of Choosing the Internet

With the above in mind, it is fairly obvious that there are some benefits to using the Internet in such systems: elimination of dedicated line costs (or long distance charges when dial-up lines are used); Internet protocols eliminate the need for a poll/response architecture and thus reduce data traffic and thus improve responsiveness; and Internet protocols enable use of web tools in the development and maintenance of the host software thus reducing the cost and potentially the development schedule.

Another benefit is also realized: freedom from the constraints of a legacy SCADA protocol. In an Internet-based SCADA system, host software inherently handles Internet protocols (e.g. TCP/IP, UDP, HTTP, etc.) and Internet data formats (e.g. HTML, XML, etc.), so any manufacturer's RTU, flow computer or controller that supports Internet protocols may be connected to the system. The benefit of this interoperability is that the system user can select equipment based on appropriate factors such as functionality, price, performance, and quality, without being concerned about the communications protocol and whether or not it is compatible with the existing system.

The ultimate benefit of enabling IP addressing at the device level is that any browser (PC, cell phone, Palm, two-way pager, etc.) may be used from anywhere in the world to obtain data and take control.

Security

The open nature of the Internet requires careful consideration of data security measures when implementing Internet-based SCADA systems. Processes, procedures, and tools must be put in place to address availability, integrity, confidentiality, and protection against unauthorized users.

- Availability: System up time must be maintained at the highest levels through use of redundant servers. Firewall protection must be provided in the Gateway and servers along with automated monitoring to detect DNS attacks.

- Integrity: System must ensure data is not modified or corrupted through use of encrypted data signatures, authentication to restrict access, etc.

- Confidentiality: System must ensure restricted access to data through use of encryption, and to the system by employing authentication such as Secure Socket Layer.

- Protection against unauthorized users: Multi-layered password protection must be provided at all levels in the system.

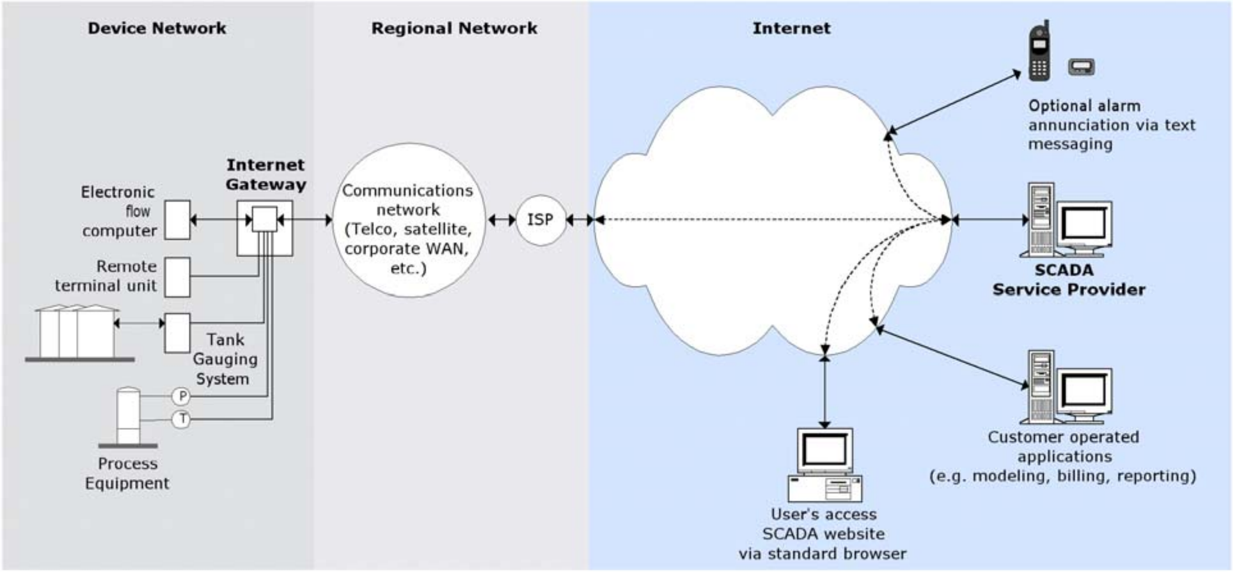

Device Network
Regional Network
Internet
Electronic flow computer
Internet Gateway
Remote terminal unit
Tank Gauging System
P
T
Process Equipment
Communications network (Telco, satellite, corporate WAN, etc.)
ISP
Optional alarm annunciation via text messaging
SCADA Service Provider
Customer operated applications (e.g. modeling, billing, reporting)
User's access SCADA website via standard browser

Figure 2: Internet SCADA Network

Interfacing Equipment to Internet-Based SCADA Systems

Unfortunately, few of the traditional SCADA equipment manufacturers have adopted Internet protocols, and of course, the installed base only supports proprietary protocols. The solution is to retrofit Internet protocol and data format capability through firmware upgrades either to the existing unit, or by adding a protocol/data format converter, often referred to as an Internet Gateway or Adaptor. In order to implement a flexible Internet SCADA solution that will support occasional connections as well as dedicated lines, the upgrade must include the ability to dial an ISP for connection to the Internet.

Scalability

Scaling an Internet-based SCADA system from a few to thousands of assets while maintaining near real-time performance requires a system architecture that enables data to be pushed from the remote equipment without host system polls. This approach has been implemented in systems supporting 20-second simultaneous updates from 3000 devices.

Data Presentation

As the acronym implies, the purpose of a SCADA system is to allow asset owners and operators to monitor and control remote assets, therefore the presentation of data is a critical component of any SCADA system. The use of Internet protocols and services to collect data makes it simple to use standard web browsers for data presentation.

The technology chosen for development of the web page user interface (UI) must support development of sites that are highly dynamic, incorporate animation, and provide a high level of usability. Standard web page technologies such as HTML, JavaScript, and Macromedia FLASH are ideal for the development of SCADA presentation pages.

Implementation Options

Implementation of an Internet-based SCADA system is a complex project that may be handled in one of three different ways: owner may purchase components and either act as integrator or hire one; contract for a turnkey SCADA installation; or contract for turnkey subscription-based SCADA services.

Experience indicates that complex SCADA projects are generally best handled by a single vendor acting as system architect with responsibility for the total solution.

An important alternative to this traditional approach is to simply contract for SCADA services on a subscription basis. For a monthly fee some vendors design the system, install field hardware if necessary, operate secure servers to host the data, and provide customers access to their data via a standard web browser.

A Simple_Example

The use of Internet-based SCADA systems to monitor and control gas production wells has been proven to improve production and lower maintenance costs. For example, a field operator installed proprietary gas flow computers at nine wells to record flow data and store it for collection once every twenty minutes via a SCADA subscription service.

The operator estimated that operational efficiencies achieved through use of the SCADA service resulted in production increases of 7% per year. The subscription service fee was $25 per month per well for a period of 36 months and the cost of field automation equipment was $30,000. Using a discount rate of 10% and $1.50 per mcf gas price, the project RoI was calculated to be in excess of 500%.

Conclusion

Internet-based, secure, real-time SCADA is now a reality, and offers many benefits:

- Provides corporate-wide solution that integrates new and legacy SCADA equipment
- Flexibility – choose equipment and systems based on price/performance rather than compatibility with installed base
- Scales quickly from a few sites to thousands
- Single solution is suitable for both local and enterprise-wide applications
- Subscription service contract option available
    - Reduces SCADA project risk – customer pays only upon commencement of service
    - No capital investment is required

About the author

Donald Wallace, a graduate of the University of East London, is a Professional Member of the British Computer Society (www.bcs.org). He is a past Director of the HART Foundation (www.hartcomm.org), an industry group formed to standardize sensor data communications, and he holds two patents for wide area telemetry (SCADA). He has over 30 years experience in the design, marketing, and sale of complex systems for industrial automation and data communications applications. He is currently Chief Operating Officer of M2M Data Corporation, a Denver, Colorado, company specializing in the provision of Internet-based SCADA services in oil & gas, power, and government markets.