EnergyPulse™
Insight, Analysis and Commentary on the Global Power Industry

U.S. Electric Power Reliability and Security -- Congress, We Don't Have to Wait

10.16.03 Donald Wallace, COO/VP Engineering and Operations, M2M Data Corporation

I decided to write this article after watching an early morning news show concerning homeland security during which a congressman stated that the Federal government must urgently fund new scientific research projects at our leading universities. He referred to the wealth of American talent available at our colleges to tackle the variety of problems faced in providing adequate protection of our homeland against terrorist threats.

My initial reaction was, "Typical political solution—fund new programs!" After a second of further consideration, I accepted the validity of the congressman's comments, but remained concerned and disappointed that he didn't even mention the more obvious and immediate solution: engage the energy, talent, and creativity of leading technology companies, large and small.

What Really Needs to be Done

A key component of any Homeland Security system must be the consistent and automatic monitoring and control of critical infrastructure such as power and natural gas distribution. One of the technologies needed to monitor and control critical infrastructure is called supervisory control and data acquisition, or SCADA, a system of monitoring and controlling equipment linked over long distances to a central computer. SCADA systems have been used for 30 years on pipelines, electric utility transmission systems, etc., however to allow homeland security personnel to fulfill their mission these existing systems must be integrated into a single centralized system.

Example: The recent blackout in the northeastern U.S. might have been averted or at least minimized if the data available from each of the dozens of SCADA systems currently used to control power generation and transmission had been available at a critical infrastructure-monitoring center.

. . . engage the energy, talent, and creativity of leading technology companies, large and small.

How We Do It

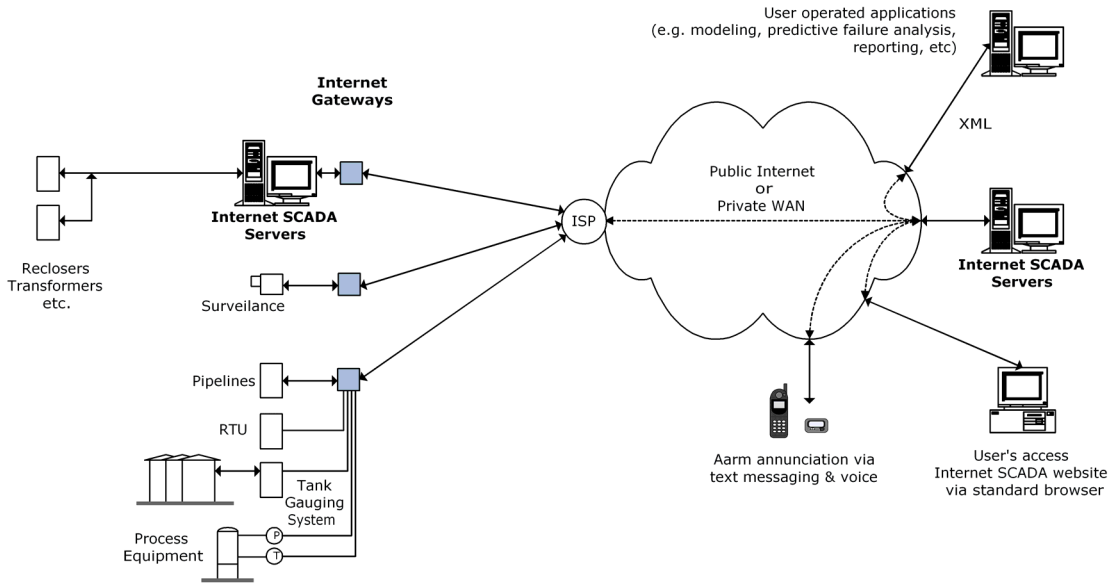
Over the past several years Internet technologies have enabled a new breed of SCADA systems to evolve. These open Internet-based SCADA systems provide access to real-time data from existing remote equipment and SCADA systems, therefore allowing the interconnection of these systems and equipment into a single integrated critical infrastructure monitoring system.

Internet-based SCADA makes this possible by using standards such as XML for data formatting, SQL databases for storage, and Web browsers for presentation, thus eliminating proprietary data formats and host software. It also eliminates or minimizes the cost and complexity of long distance communications because each piece of remote equipment is connected to a local Internet Service Provider (ISP) or private wide area network.

A critical infrastructure SCADA system must provide three key functions:

1. Collect data from and transmit control commands to existing SCADA servers,
2. Collect data from and transmit control commands to new and existing remote equipment such as recloser controllers and surveillance cameras, and
3. Provide access to aggregated data in a manner that allows rapid decision-making.

Figure 1 shows how the three categories of existing SCADA infrastructure (i.e. existing SCADA systems, standalone field equipment, and surveillance cameras) can be connected and integrated into an Internet SCADA system that meets all three functional requirements.



Dealing with Legacy Technology

Aggregating the necessary operational data into a nationwide critical infrastructure monitoring system offers some challenges. SCADA systems currently used by each operating entity (i.e. power generator or transmission and distribution company) are generally proprietary systems designed and built for the specific purpose of monitoring and controlling only the connected assets without consideration of sharing the data with other systems. These are not open systems of the type we now demand of ecommerce systems and as such, impose significant obstacles to any attempt at sharing data with other systems, including limited connectivity options, proprietary data formats, no facilities for data export or import, etc.

In cases where proprietary SCADA host software is Windows-based, it may be possible by working with the software vendor to provide open, standardized data export, however the longstanding proprietary nature of these systems makes this solution unlikely. The alternative is to install an Internet gateway that interfaces to the host software's proprietary data export utility (supported by most SCADA software). The Internet gateway converts the proprietary data format to an Internet standard such as XML and pushes the data to the Internet SCADA Servers.

Processes, procedures, and tools must be put in place to address availability, integrity, confidentiality, and protection against unauthorized users.

An Internet gateway may also be used to enable field equipment to communicate directly with the Internet SCADA servers. Once installed, it communicates with the equipment in the equipment's native protocol and converts the data to XML format, and then transmits the data to the Internet SCADA servers.

Another major issue is system security, which in this context means assurance that SCADA data is always available, is not tampered with, and is accessible to only authorized users. The open nature of the Internet requires careful consideration of data security measures when implementing Internet SCADA systems. A determined attacker must not be able to affect

the availability of the system or the integrity or confidentiality of the data.

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 Internet 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.

The Details

Open Standards

The Internet gateway must support Internet protocols and services, the only internationally recognized and supported network standards, specifically an IP address and at least parts of the TCP/IP stack – typically at least HTTPS, TCP/IP, UDP, and PPP. Once connected to the Internet, the Internet gateway pushes data to the Internet SCADA servers. In cases where the equipment incorporates an electronic controller, it may be possible to simply add similar functionality into the existing micro-controller. Therefore using an Internet gateway (or embedded protocols and services when available) permits the integration of data from disparate SCADA host software and remote equipment into a Internet SCADA server system that is based on open systems standards such SQL database, and XML data format. Once the data is available in the Internet SCADA system, it may be accessed from any standard web browser in any location.

Interoperability

The open architecture of an Internet SCADA system combined with appropriate field equipment makes it possible to develop a highly integrated nationwide centralized system. Integration of thousands of individual pieces of equipment and systems in a way that assures integrity requires standardization of data format and transmission protocol.

The preferred data format is Extensible Markup Language (XML). XML was developed to bring greater flexibility and interoperability to web applications. It is a meta-language for describing markup languages and therefore does not specify semantics or a tag set. In other words, XML provides a facility to define tags and structure. XML provides flexibility not available from HTML because the programmer has the freedom to create tag sets and semantics. The simpler alternative markup language, HTML has undergone continuous development to support new tags and style sheets. However, these changes are limited by the requirement to be backwards compatible, and to what the browser vendors are willing to support.

The preferred data transmission protocol is HTTPS because it is firewall friendly and allows web servers to be used to control data transmission. The alternatives, TCP/IP or UDP, require the cooperation of third party IT departments to open ports on servers and thereby introduce potential for cyber attack.

Scaling an Internet SCADA system from a few to hundreds of 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.

Scalability

Scaling an Internet SCADA system from a few to hundreds of 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. Internet protocols and services are ideal for a system architecture of this type. The scalability of commercially available databases and server hardware has been proven in thousands of ecommerce applications.
This approach has already been implemented in systems supporting simultaneous 20-second updates from 3000 devices.

Cost

The techniques, software, hardware, and networks required to accomplish the integration described above are all widely used on the public Internet and are low in cost and high in reliability. The only SCADA-specific hardware, the Internet gateway, is available from multiple vendors at a price of $300 or less.

The Pay-off

Once operational data has been aggregated and integrated into the Internet SCADA servers, it becomes relatively simple to develop Homeland Security applications in a way that is impossible with today's proprietary systems. Through the use of proven data mining and analysis techniques Internet SCADA can produce highly valuable information such as system-wide trending, failure predications, system condition reports, etc.

. . . let's worry less about new R&D funds for universities and put existing technology to work securing our homeland.

Internet SCADA is currently in use in oil and gas, electric utility, and government systems supporting real-time data acquisition, remote control, surveillance, and customized applications, so let's worry less about new R&D funds for universities and put existing technology to work securing our homeland.

About the author

Donald Wallace, a graduate of the University of East London, is a Professional Member of the British Computer Society. He is a past Director of the HART Foundation, an industry group formed to standardize sensor data communications and 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 Office and VP Engineering of M2M Data Corporation (www.m2mdatacorp.com), a Denver, Colorado company specializing in the provision of Internet-based SCADA services in oil and gas, power, and government.