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

# The Importance of Security in Internet-based SCADA Systems

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

The open nature of the Internet requires use of robust data security measures when implementing Internet-based SCADA systems.

## Risk Follows Promise

Many companies are considering using the Internet for supervisory control and data acquisition (SCADA) systems to provide access to remote equipment for monitoring and control purposes. Using the Internet makes it simple to use standard Web browsers for data presentation, thus eliminating the need for proprietary host software. It also eliminates the cost and complexity of long distance communications because each piece of remote equipment is connected to a local Internet Service Provider (ISP). However, the open nature of the Internet requires careful consideration be given to ensuring secure access to, and the integrity of data when implementing an Internet-based SCADA system.

In this context "security" means assurance that SCADA data is always available, is not tampered with, and is accessible to only authorized users.

## Security Philosophy

Ensuring that an Internet-based SCADA system meets the above criteria cannot be left to the simple installation of technology. Rather it is necessary to develop and implement processes and procedures that are continuously reviewed and updated to address newly identified vulnerabilities.

The Security Recommendation Guides outlined by the National Security Agency systems, which may be downloaded from www.nsa.gov, provide established policies and procedures to secure a wide variety of network infrastructure. Implementation of these guides is an ongoing process, which requires modification and continual changes as dictated by user applications.

## Specific Challenges

Internet-based SCADA systems provide challenges not found in typical IT infrastructure, in that a large part of the system is located in very remote locations—all of which have network access. Also, most system users access the SCADA servers from remotely located browsers. Both system features present wide area vulnerability that must receive specific attention.

## SCADA Security Goals

Data security processes and procedures must provide the following functionality.
Availability: System up time must be maintained at the highest level through use of redundant servers, network protection such as firewalls, etc.
Data 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 itself by employing user authentication, which may range from passwords to biometrics.

## Security Processes

In order to maintain effective SCADA security, processes must be reviewed regularly and updated as necessary to keep pace with new vulnerabilities. Appropriate processes are noted as follows:

### *Vulnerability Assessment*

All components of the SCADA system must be reviewed regularly including remote communications equipment, communications system components, as well as servers, firewalls, and other IT infrastructure.

### *System Design Review*

The initial SCADA system design must include data security assurance as an elemental issue. Selection of components and technologies such as firewalls, encryption techniques, etc. must receive appropriate attention by experts in the field. Once installed, the system design and technology must be reviewed regularly to ensure newly identified vulnerabilities are dealt with immediately.

### *Day-To-Day Operation*

The data security processes and techniques employed in a SCADA system require continuous attention. Once detected, breaches in security must be defined and corrective action must be identified and implemented. Much of the detection process can be automated, but corrective action will generally require the attention of an experienced security professional.

## Conclusion

It is possible to gain the benefits of using the Internet as the basis for a SCADA system and minimize security risks through use of appropriate processes and procedures implemented by security professionals.

---

*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.*