Creating a Reliable and Secure Advanced Distribution Management System

Executive summary

Advanced Distribution Management System (ADMS) solutions integrate supervisory control and data acquisition (SCADA) technology with other information management to enable greater automated control for more efficient distribution. This same functionality makes it an attractive target for cyber attacks that could wreak havoc on the electric grid, water pumping plant, or commodity pipeline. This paper discusses the security criteria for making SCADA systems secure and reliable. Compliance with these security attributes also facilitates auditing, system monitoring, certification, and user accreditation of the control system.

Schneider Electric

Summary

Executive summary

As public utilities strive to build an efficient distribution network, they are looking to automated solutions. One such solution is the advanced Distribution Management System (ADMS) that integrates SCADA, DMS and OMS technology, for optimum performance efficiency. Instead of operating with proprietary protocols on isolated networks, this approach applies open-system design – and makes security of the SCADA system paramount.

In the U.S., the National Institute of Standards and Technology (NIST) is leading the efforts toward establishment of security standards for SCADA networks that process unclassified information. The North American Electric Reliability Council (NERC), with oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada, enforces mandatory cyber security standards for the bulk power system in North America. Beyond North America, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) maintain the ISO/IEC 27001 Information Security Management System standard.

It is these standards that make possible the performance efficiency of an interoperable ADMS open system while actually improving the security of older, proprietary SCADA/DMS/OMS systems.

The NERC Critical Infrastructure Protection (CIP) guidelines establish best practices for the minimal level of security required for safe and secure operations of a modern ADMS solution. They fully describe the system's security objectives but leave to the user the choice of technology that best achieves these objectives for the user's network. These guidelines describe access control and event logging, personnel training, maintenance of the electronic security perimeter, incident reporting and response planning, and security auditing. The utility that implements an ADMS solution that complies with these guidelines is positioned not only for operational effectiveness and enterprise-wide efficiency but also security of operations. It is recommended that the ADMS solution vendor be actively involved in industry working groups, to support compliance with the latest developments.

An open-architecture, fully configurable ADMS system meeting NERC CIP guidelines will offer security at all operational levels, even as the network grows and software upgrades are applied.

Introduction

Today, public utilities are looking to optimize distribution performance through sophisticated Advanced Distribution Management System (ADMS) solutions that inherently integrate an advanced-technology SCADA with a DMS and Outage Management System (OMS) — a solution that enables a high-performance network model and automated control of a very large number of critical resource functions for efficient distribution. As such, SCADA/DMS/OMS technology can be an attractive lure for hackers, cyber-criminals and cyber-terrorists; the same supervisory control and data acquisition (SCADA) system functionality used to control and manage an information network could be used to blind an organization to attack, create confusion, provide false information, and prevent required actions — and wreak havoc on the electric grid, water pumping plant or oil pipeline.

The security of the SCADA employed in such a broad solution is paramount; a proprietary, non-adaptable monitoring and control system not designed for secure operation as part of a comprehensive technology solution is no longer an unacceptable option.

In this paper, we discuss the security criteria that make a SCADA system — and any network management solution incorporating the SCADA as a key component — a secure and reliable control system. Compliance with these security attributes also facilitates audit, system monitoring, certification and user accreditation of the control system.

Creating a Reliable and Secure Advanced Distribution Management System

The need for cyber security

In the past, SCADA/DMS/OMS systems ran proprietary protocols on isolated networks. While this eliminated a number of potential threats, it also limited the utility's access to its own information and increased the total cost of ownership of data management. New SCADA/DMS/OMS solutions embrace industry standards and open-system design, allowing connection to corporate networks that are, in turn, connected to the Internet. Access and information is shared with applications and authorized users across the entire enterprise — significantly increasing the threat and vulnerabilities that must be addressed through security controls.

Security standards and regulatory concerns

Leading industry groups and standards organizations have taken up the cyber security challenge and are creating guidelines, standards and certifications for the protection of critical IT systems. In many industries, compliance will be mandatory and will require a signed certification of compliance by a corporate officer.

United States

The terrorist attacks of September 11th dramatically increased the level of effort, funding and pace of developing and implementing certified security for U.S. industries relying on IT networks for core functionality. The critical infrastructure industries also have developed Information Sharing and Analysis Centers (ISACs) on the Internet, where industry members can securely share information dealing with threats and vulnerabilities.

The National Institute of Standards and Technology (NIST) is the U.S. government agency responsible for setting security standards for the protection of unclassified information and networks. NIST, in association with the National Security Agency (NSA), has formed a Process Control Security Requirements Forum to create security standards for SCADA networks. The Forum includes government security experts, SCADA vendors and significant participants from the industries that use SCADA systems.

- The Forum is following the ISO/IEC 15408 methodology and is writing Protection Profiles specific to SCADA networks. This methodology provides a security target that can be tested and certified by an independent third party. The first Protection Profiles will apply to the entire SCADA community, but industry specific Protection Profiles are likely to follow.

- In October 2002, NIST issued Special Publication 800-37, Guidelines for Security Certification and Accreditation of IT Systems. This document specifically mentions utility networks in Section 2.2.3, referring to "… utility distribution systems (for example, water and electric distribution systems)". The Guidelines define three security certification levels and the appropriate management, technical and operational security controls required to be certified at each level.

- In the spring of 2003, NIST issued Special Publication 800-53, Minimum Security Controls for Federal Information Technology Systems and Special Publication 800-53A, Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems.

These three NIST endeavors will result in standard processes that allow companies to certify and accredit their SCADA systems to the appropriate security level.

Electric providers in North America

Because of the highly inter-dependent nature of the electric grid, a vulnerability at one utility has the potential of cascading throughout the grid and causing a massive failure. Therefore, the security of the electric grid requires the cooperation and vigilance of all participants.

The North American Electric Reliability Council (NERC) is the regulatory authority established to evaluate reliability of the bulk power system in North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. Among its several functions, NERC has developed and enforces a set of mandatory cyber security standards as well as Security Guidelines for the Electricity Sector and a Vulnerability Assessment Methodology. It participates in education and training of industry personnel and provides the compliance checklist allowing each utility to complete self-certification.

International

Although the international security standards organizations have developed a number of standards that can be applied to IT systems, none relate specifically to SCADA. The Common Criteria, ISO/IEC 15408, is a very detailed standard that defines a methodology for actually testing and certifying system security at one of seven different security levels. This methodology, rigorous and expensive, has influenced many of the recent IT-specific standards. In 2003, the international Instrumentation, Systems, and Automation Society (ISA) developed a SCADA-specific security standard, the SP-99.

Published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001 is an Information Security Management System (ISMS) standard that is part of the growing ISO/IEC 27000 family of standards. It is officially named ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. As a formal specification, the ISO/IEC 27001 standard mandates specific requirements for achieving information security under explicit management control. Organizations that claim to have adopted ISO/IEC 27001 can, therefore, be formally audited and certified compliant with the standard.

More recently, the Working group for Smart Grid Information Security (WG SGIS), part of the Smart Grid coordination group, was established up by the European Standards Organizations (ESOs) to implement the standardization work requested by the European Commission mandate M/490 for standardization of Smart Grid implementation. The following documents and international standards are being analyzed for this group:

- EG2 Report: Report of the Task Force Smart Grid Expert Group 2 on “Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection.”

- ESO Joint Working Group Report: CEN/CENELEC/ETSI Joint Working Group on standards for Smart Grid Report (chapter 5.1.5 Smart Grid Information Security).

- NISTIR-7628: US non-prescriptive recommendations for Smart Grid Cyber Security.

- NERC/CIP: mandatory standards issued by NERC (North-American Electrical Reliability Corporation) to protect critical infrastructures.

- IEC 62351: IEC 62351 defines explicit security measures in the context of energy automation, such as for IP-based and serial protocols.

- ISO/IEC 27001: “Information technology – Security techniques – Information security management systems – Requirements.”

- ISO/IEC 27002: ISO/IEC 27002: “Information technology – Security techniques – Code of practice for information security management,” which identifies best practices recommendations for information security management.

An ADMS security strategy

The modern ADMS must provide the cost, performance and interoperability advantages of an open system, while actually improving the security offered by older, proprietary SCADA/DMS/OMS systems. System administrators can implement security standards that have passed a rigorous peer review, such as IPSec, SSL, Kerberos, and X.509 digital certificates. Not only does this standardization secure the system, eliminating the need to review a complex, proprietary security protocol makes security audit, certification and accreditation much easier, and, consequently, more practical and effective.

Built on open standards and component flexibility, the ADMS solution takes full advantage of the e-business era, elevates the integrated SCADA/DMS/OMS system to new levels of enterprise integration, and readies the utility for tomorrow's upgrades.

A key part of the architecture of such a flexible and extendable solution is the use of Windows Server™ integrated server software. This architecture provides numerous tools and security options that security administrators are deploying for their internal network operating system, and the resulting knowledge, experience and security components can be extended to secure the SCADA/DMS/OMS network and lower the total cost of ownership; see Figure 1. This security framework includes:

- Single sign-on to improve user experience
- Strong authentication (Kerberos, RSA keys) to eliminate most of the scope of security password problems
- Role-based access control for user authorization
- Highly granular Active Directory policy configuration, secured at installation
- Authentication-everywhere model
- Encrypted communications (IPSec, SSL) for data confidentiality
- Public key infrastructure (PKI) to automate security management (X.509 digital certificates)

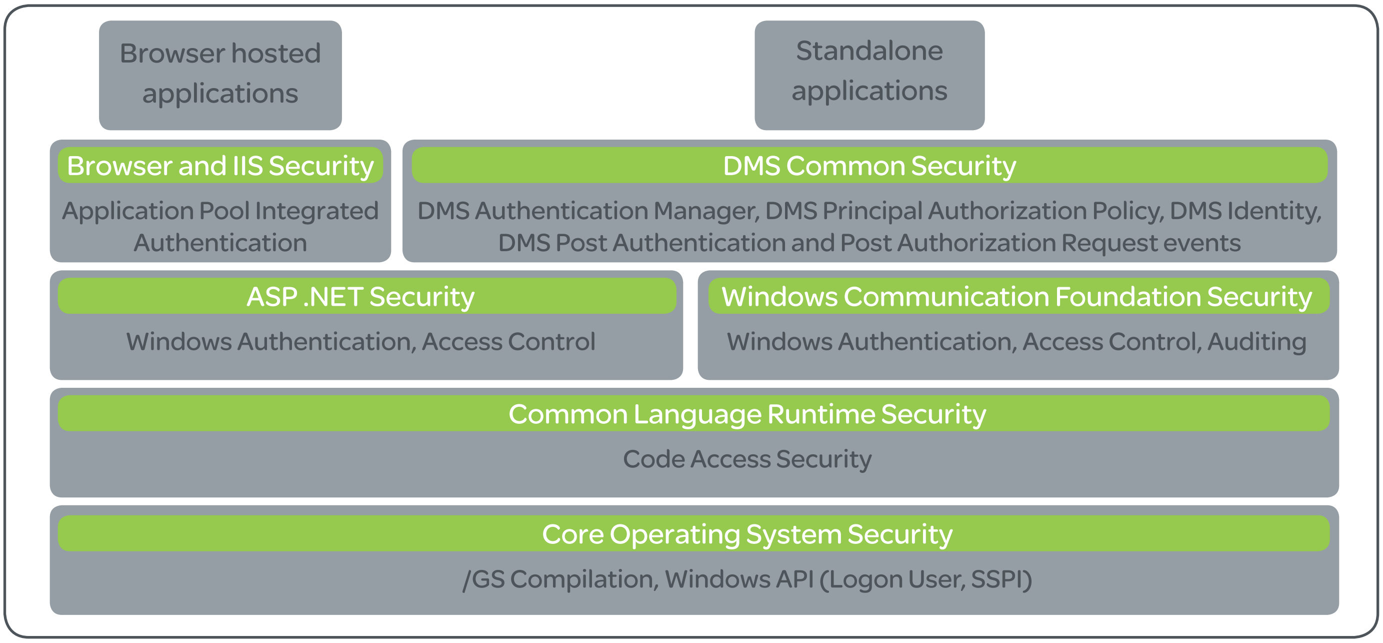
Browser hosted applications
Standalone applications
Browser and IIS Security
Application Pool Integrated Authentication
DMS Common Security
DMS Authentication Manager, DMS Principal Authorization Policy, DMS Identity, DMS Post Authentication and Post Authorization Request events
ASP .NET Security
Windows Authentication, Access Control
Windows Communication Foundation Security
Windows Authentication, Access Control, Auditing
Common Language Runtime Security
Code Access Security
Core Operating System Security
/GS Compilation, Windows API (Logon User, SSPI)

Figure 1. ADMS security framework.

NERC CIP

The NERC Critical Infrastructure Protection (CIP) guidelines, generally accepted by electric energy providers worldwide, describe how a modern ADMS solution must respond for safe and secure operation. First, let's clarify the main objectives of these guidelines —

- **What CIP does.** CIP provides general security guidance toward achieving the minimal level of security required for safe and secure operations.
- **What CIP does not do**. CIP does not prescribe or specify the technologies to be deployed to meet secure operational goals. It defines objectives, not how the user must achieve them. With the responsibility of meeting secure operations objectives, the user also has the choice of which technology will best serve its needs in meeting those objectives.

Brief description of CIP guidelines

The NERC CIP document addresses a broad range of Critical Cyber Asset (CCA) and Cyber Security issues; here, we very briefly review six of the CIP guidelines that apply to operation of control rooms and electric network field devices. The full text of the NERC CIP standard can be found at http://www.nerc.com.

CIP-003 Security Management Controls describes the development of a cyber-security policy and documentation of that policy in a way that it can be updated and that all staff is aware of the policy. It also discusses management of personnel who have access to the CCAs and identification of users with different privileges, roles and responsibilities.

CIP-004 Personnel and Training identifies the personnel training and awareness recommended for supporting security-related operations and procedures. It cites CCA user identification lists that are reviewed periodically and can be modified to change both users and user privileges.

CIP-005 Electronic Security Perimeter(s) deals with identification and protection of ESP access points and communications. While encryption is not identified specifically as a guideline for ESP access, CIP-005 does speak to:

- Security of dial-up access
- Access denied by default
- Enabling and disabling ports or functions deemed not needed
- Appropriate-use banner
- Monitoring, logging and warnings for user access or attempted access

CIP-006 Physical Security discusses physical accessibility to equipment, including:

- Mounting equipment in lockable enclosures
- Remote control of locks
- Access alarms indicating a door or gate is open
- Card keys, video cameras, etc.
- User logged in and failed login attempts

CIP-007 Systems Security Management deals with operating issues such as security patches, virus protection, vendor releases and event logging. References to device security reinforce CIP-005 concepts:

- Ability to enable or disable unused or unneeded ports and services — or compensating factor that will mitigate risk, such as physical security
- Security patches and firmware upgrades
- Anti-virus and malware protection — driven by the operating system

CIP-008 Incident Reporting and Response Planning relates to the managing and handling of reports and logs. While collecting and storing logs for historical reference is necessary, how that retention is done is determined by the hardware and the organization's capabilities.

NERC CIP alignment

Together, the CIP guidelines address eight different criteria related to a secure ADMS framework: User Controls, Access Control, Electronic Security Perimeter, System Logging, Personnel Termination/ Privilege Changes, Security Software Management, Alerts and Notifications, and Training. The following identifies the framework features that, working closely with the SCADA/DMS/OMS infrastructure, help meet these criteria and contribute to the ADMS security strategy described earlier.

User Controls. CIP-003, CIP-004 and CIP-007 identify characteristics of the permissions assigned to each user to perform certain functions within the system:

- Unique passwords for each user
- Role-based Access Controls
- Principle of Least Privilege (PoLP) architecture
- Granular audit capabilities
- Centralized user store
- Application restrictions available on a per-user basis and/or by console basis
- Administrative access not required for typical operations — only for maintenance and modification
- Passwords managed from a central location

Access Control. CIP-003, CIP-004 and CIP-005 describe these characteristics related to user authentication and account setup:

- Secure authentication (one or multi-factor)
- Separation of duties-based user model
- Highly configurable permissions structure
- No 'back doors' or maintenance channels
- All default user accounts documented and provided on request
- User access may be controlled based on time of shift or isolated to only specific workstations
- Strong passwords enforced by the operating system
- Password change policies enforced
- User-configurable banners available

Electronic Security Perimeter. CIP-003, CIP-005 and CIP-007 relate the issues to be considered for a valid security perimeter around the CCA:

- Monitoring and logging of all access
- Capable of integrating with off-the-shelf access control devices or VPNs to extend single-sign-on
- Encryption of communications with remote clients or sites
- Single-port communications through perimeter with external systems
- Software restrictions available for non-administrative users
- Communications inside the perimeter can be secured through signing end pervasive encryption
- Configurable port usage

System Logging. CIP-003, CIP-004, CIP-007 and CIP-008 all refer to this function as it relates to the audit requirements of the system:

- All access attempts securely logged through the operating system
- Individual privilege uses logged
- User account management and change control in place and logged
- Modifications to SCADA databases logged
- Ability to send logs to central server backup for aggregation purposes
- Configurable log lifetimes and log export capabilities

Personnel Termination/Privilege Changes. CIP-004 and CIP-007 speak to capabilities necessary regarding user accounts:

- User accounts can be revoked by administrator
- User accounts can be “downgraded” to lower authority

Security Software Management. CIP-007 cites the features needed for operating system patches and antivirus updates:

- Security patch management program in place
- OS multiple patch management technologies supported
- Anti-virus/anti-malware applications supported on all platforms and hosts
- Vendor security testing performed on realistic environments and system which accurately reflect real-world conditions

Alerts and Notifications. CIP-005, CIP-007 and CIP-008 all refer to the detection of failed attempts to access the system:

- Unauthorized logon attempts logged

Training. CIP-004 describes specific training tasks during implementation and subsequent maintenance of the system:

- Security concepts are covered in standard training courses
- Security controls are highlighted and their use is covered in standard training courses
- SCADA security-specific training is available for additional depth of knowledge

Solution characteristics

The utility looking to establish a robust, secure and reliable ADMS solution that will meet both current and future needs should target a system that —

Complies with NERC CIP and NISTIR 7628 guidelines

- **Access control and event logging** — A system based on the Windows® operating system or other platform with inherent access control capabilities prevents accidental or malicious acts from affecting the system. Only authorized personnel can access services; and all file access, permission usage and alterations to security policies are logged and can be tracked for auditing purposes. Host-based firewalls on every machine minimize the threat surface.

  Look for a system that locks down operator accounts to prevent any user access beyond the control room user interface, as well as the installation of unauthorized software. VPN connections allow users to securely access the system network from the insecure public and corporate infrastructure for management, maintenance and operations.

  Also, highly granular asset-based access control supports all operational requirements while limiting an operator's access to only those devices that fall under his or her jurisdiction.

- **Electronic Security Perimeter** — Network Model Promotion in an established ESP environment allows secure update without threatening the system's operational capacity. The process includes thoroughly identifying access points, monitoring transferred data and enforcing approval from an authorized entity located in the operational environment. This approach eliminates the possibility of automatic updates with respect to the established ESP.

- **Security Auditing** — Each system should be audited before deployment to assure every change in databases and network model is logged with user, timestamp and console annotations.

Reflects ongoing vendor engagement with industry working groups like the Cyber Security Coordination Task Group (SGIP) and Gridwise Alliance, to support compliance with the latest industry developments.

Represents commitment to product security

- **Business requirements and control system requirements** — IPSec encryption capability preserves data integrity and confidentiality for communications between servers and workstations without the need for altering operational procedures.

  Required ports open on servers should be screened from external access through the use of properly configured routers and network firewalls.

  The solution should remove all applications not required for the successful operation of the SCADA system.

- **Design and architect with future requirements in mind** — The solution must reflect a dedication to scalability and extensibility.

Offers out-of-the-box adaptable, secure systems

- **No back doors** — The system should easily accept any major authentication technology, such as biometrics, persistent smartcards and access tokens, and allow central access control at a user/machine policy level so that an administrator can make use of available tools.

- **No hard-coded passwords** — A system with full configurability allows strong, default password complexity, a configurable 'Failed Login' threshold and enforcement of password history. A feature such as Single-Sign-On authentication technology allows a user to access the system through a single complex password at the system platform level, allowing administrators to make use of greater password complexity.

- **Security lifecycle managemen**t — A support program that rapidly reviews, tests and approves security updates will maximize system security while minimizing the risk of upgrade-induced issues. The solution should be configurable for industry-leading anti-virus software packages.

Conclusion

The ‘security through obscurity’ argument supporting proprietary SCADA systems never was the option of choice of security professionals. In today’s Smart Grid environment requiring effective integration of SCADA with other information management systems, open-architecture technology designed with appropriate features is necessary not only for proper performance and enterprise efficiency, but also for the security necessary at all levels to assure the safety of critical infrastructure assets.