

Meeting IED Integration Cyber Security Challenges

Jacques Benoit
Manager Cybectec Product and Technology Training
Cooper Power Systems

Jacques.Benoit@cybectec.com

INTRODUCTION

Utilities are currently installing large numbers of modern Intelligent Electronic Devices (IED) in their substations, mostly to replace legacy protective relays, but also for metering and equipment monitoring. These devices provide valuable information that can be put to use to improve reliability and reduce operating costs. This is the promise of the Smart Grid.

To integrate IEDs, utilities are also deploying extensive communication networks. However, since the devices are now connected using modern communication technologies, there is a growing concern about the security of Supervisory Control and Data Acquisition systems (SCADA).

Traditionally, SCADA systems were considered secure by the simple fact that they used dedicated communication lines and obscure protocols. However, modern systems are being implemented using industry standard TCP/IP networks, wireless technologies, and standard protocols such as DNP3 or IEC 60870-5-104.

In the United States of America, the events of September 11, 2001 increased public awareness about the threat of terrorism. The August 2003 blackout demonstrated the vulnerability of the bulk power network in North America. To ensure the safe and reliable operation of the bulk power network, regulatory organisms such as the NERC (North American Electric Reliability Council) have thus stepped in and imposed cyber security measures. These measures currently target mostly transmission and generation utilities in North America. However, the matter is sufficiently important that international standard setting organizations such as IEC are now addressing cyber security issues for the power industry.

The Nature of the Risk

Cyber security is often associated with the Hollywood vision of terrorists or hackers taking control of a power system. While this type of threat is often exaggerated, the use of standard technologies exposes control systems to the same types of failures that are common in enterprise systems: misuse by unauthorized users, virus attacks, losses of availability.

Very few incidents have been publicly disclosed, but the following two illustrate the main vulnerabilities of control systems.

Maroochy Shire sewage spill. In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

Davis-Besse power plant. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

Root Causes

The two above-mentioned cyber security incidents directly result from the use of standard

networking technologies in the SCADA system. In the Maroochy Shire incident, the disgruntled employee used the wireless capability of his laptop to connect to the SCADA system, and operate it while sitting in his car parked in front of the facility.

In the nuclear reactor incident, the network was infected via a contractor's laptop contaminated by the Slammer worm plugging into one of the plant's systems.

Some analysts believe that these incidents will become increasingly difficult to prevent because in many SCADA systems the sole protection is a firewall designed to provide an impenetrable outer perimeter. However, traditional barriers are no longer effective because there are simply too many connections to the outside world. In a recent survey, the ARC Advisory Group asked control engineers about the types of connections that their automation networks had to the outside world. This is what it found¹:

- 47.5% - Company Intranet/Business Network
- 42.5% - Direct Internet Connections
- 35% - Direct Dial-up Modems
- 20% - Wireless Modems
- 17.5% - No Connection
- 8.0% - Other Connections

Protecting a SCADA system requires much more than a firewall. A complete set of measures and controls must be implemented.

As we will see throughout our discussion, some of the measures that are effective in the world of IT cannot easily be applied in the world of SCADA. Ultimately, a "defense in depth" strategy will need to be applied where each system component is an active participant in the security of the whole.

INFORMATION SECURITY CONCEPTS

Information security is a well established discipline whose goal is to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The core concepts of Information Security are Confidentiality, Integrity and Availability, generally referred to as the CIA triad.

Confidentiality consists of ensuring that the desired resource is only accessible to the desired person or system, under the desired conditions. Measures must be taken to prevent unauthorized

disclosure of systems and information. Some of the key principles of confidentiality are: Identity, Authentication and Authorization.

Integrity consists of ensuring that the desired resource contains accurate information and performs precisely as intended. Measures must prevent unauthorized modification of systems and information, whether intentional or unintentional. Non-repudiation is another aspect of integrity. Measures must be taken to tie an action to an actor, and prevent an actor from denying (repudiating) an action.

Availability consists of ensuring that resources are accessible when needed by an authorized party. Measures must be taken to prevent the disruption of service and productivity.

There is an important difference in the application of these practices in the world of IT systems and that of SCADA systems. The main focus of traditional IT is to ensure the confidentiality and the integrity of the data using rigorous access control and data encryption. In control systems, the main focus is ensuring the availability and the integrity of the data.

Enterprise security protects the data residing in the servers from attack. In a SCADA system, the purpose of security is to protect the ability of the facility to safely and securely operate, regardless of what may befall the rest of the network.²

This difference in philosophy is making the adoption of security technologies very difficult as security experts from the world of IT, often with no understanding of SCADA systems, are being assigned the responsibility of securing these systems.

NERC CIP

The North American Electric Reliability Corporation's (NERC) ensures the reliability of the bulk power system in North America. The NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards have already been adopted and utilities are under a strict timeline to implement them.

CIP-002 Critical Cyber-Assets – Requires utilities to define critical assets in general and critical cyber-assets in particular. Utilities must also implement a complete security policy that will protect these assets from different types of potential attacks.

Critical assets support the reliable operation of the Bulk Electric System:

- Control centers
- Transmission substations
- Generation resources
- Blackstart generators and substations in the electrical path of transmission lines used for initial system restoration
- Load shedding systems under a common control system capable of shedding 300 MW or more
- Special Protection Systems

Critical cyber-assets are defined as being cyber-assets that are directly or indirectly accessible via routable protocols (networks) or via dial-up mechanisms (modems).

CIP-003 Security Management Controls – Utilities must have a master plan to manage all security related aspects of all critical assets, as defined in part CIP-002-1.

CIP-004 Personnel and Training – All persons having access to critical assets shall be assessed for risk, properly trained to be aware of the risks, and familiar with the security policies that have been put in place.

CIP-005-1 Electronic Security – Requires that every critical cyber asset shall reside within an Electronic Security Perimeter that –

- Provides electronic access control
- Enables only ports and services required for operations and for monitoring
- Secures dialup access
- Monitors and logs access at access points
- Where technically feasible, monitors, detects and alerts for attempts at, or actual unauthorized accesses

Of all the NERC CIP sub-standards, Electronic Security is the one that most directly challenges the substation integration and automation systems that are being deployed.

CIP-006 Physical Security – Utilities must define, implement, document and manage physical

security perimeters around all critical assets, physical access control mechanisms at all physical access points, processes and tools to monitor accesses to the perimeter.

CIP-007 Systems Security Management – requires that utilities implement an overall System Security Management Program. Elements of compliance include account and password management, security patch management, access log management, test procedures, access reviews, integrity software, identification and documentation of vulnerabilities, change control and configuration management, backup and recovery tools, status monitoring tools, etc.

CIP-008 Incident Response Planning – requires that utilities establish mechanisms for dealing with security related incidents. Incidents must be monitored, classified, logged and reported. Actions must be taken to prevent similar incidents in the future. Roles and responsibilities related to these issues must be defined within the organization.

Some analysts consider that compliance with this requirement could be quite expensive and requires the hiring of full-time security analysts, or the use of external MSSP (Managed Security Service Provider) services.

CIP-009 Recovery Plans – requires that utilities have appropriate recovery plans for all critical cyber-assets and shall exercise these plans at least annually. Such plans must be defined, documented, tested, maintained up to date, and communicated to all personnel responsible for the operation of the critical cyber assets.

NERC CIP Implementation Timeline

NERC CIP specifies a detailed timeline for each standard and for each participant in the operation of the Bulk Power System. Typically, a transmission operator needed to be substantially compliant by June 2008, fully compliant by June 2009, and auditably compliant by June 2010.

Challenges to NERC CIP

The intent of the NERC CIP standards is to provide utilities with guidelines to be used to implement their System Security Management Program. In this aspect, NERC CIP is similar to the ISO 9001 standards. Utilities are expected to

define their own plan and compliance will be audited by NERC. Since the standards do not go into technical details, compliance to the intent of the standards is expected.

While NERC CIP was approved by the Federal Energy Regulatory Commission (FERC), it is being challenged by many, including the congressional committee on Homeland Security. The United States Congress is primarily concerned with the limitations which exclude critical assets from the risk methodology, and the lack of technical specifications. Congress believes that the reliability of the nation's bulk power system would be better protected by a standard that incorporates the additional security measures of NIST Special Publication 800-53 as applied to industrial control systems.³

NIST 800-53

The Federal Information Security Management Act (FISMA) imposes a mandatory set of processes that must be followed for all information systems used or operated by a U.S. federal government agency or by a contractor or other organization on behalf of a federal agency. These processes must follow a combination of Federal Information Processing Standards (FIPS) documents, the special publications SP-800 series issued by the National Institute of Standards and Technology (NIST), and other legislation pertinent to federal information systems, such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act.

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. NIST 800-53 defines precise guidelines to implement the following:

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection

- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Implementing NIST 800-53 in the power industry would be much more complex than NERC CIP. However, it is felt by many that the bulk power system is of such importance that significant measures must be taken to protect it.

IMPLEMENTING CYBER SECURITY

Response to NERC CIP has been varied. The timeline is quite short and larger utilities must already be significantly compliant in order to meet the 2010 deadline. In order to meet some of the requirements, utilities must be able to demonstrate that they have collected one year of data.

As we mentioned above, there remain some gray areas in the definition of critical cyber assets and we have seen utilities consider reverting to serial communications in order to be exempted. Others are simply waiting for the results of the first audits and will develop their plans accordingly. Since non-compliance can be fined up to one-million U.S. dollars per day, this could be a costly attitude.

Industry was quick to react and offer NERC CIP compliance solutions. We will discuss some of these solutions that focus on the following aspects of the overall System Security Management Program:

- Protecting the data path between remote devices and SCADA.
- Protecting remote maintenance access to devices.
- Change control and configuration management, backup and recovery tools.
- Monitoring, logging and reporting.

Protecting the Data Path

Traditionally, the main requirement of the SCADA to RTU data path has been to provide high availability, error free communications, with very low latency. Since communications generally

used a dedicated link, security was either a low priority requirement, or not considered at all.

With modern communications based on standard networking technologies such as TCP/IP, remote devices become vulnerable to a variety of attacks.

The IT field has developed solutions that are already being applied to the field of SCADA. Firewalls protect the borders of the network by blocking all ports and services that are not required by authorized services. Virtual Private Networks (VPN) are used to create secure communication channels between networks. In a VPN, both ends authenticate themselves and negotiate a key that will be used to encrypt data exchanges.

While the VPN protects the data path, it does not protect the application itself. If a network on one end of the VPN is compromised, the VPN will still allow the data to flow to the other end.

Control center protocols such as DNP3 or IEC 60870-5-101/104 do not implement any authentication mechanism. The remote device assumes that any request it receives has been emitted by "the" control center. This makes them vulnerable to attacks. As we will discuss later, work is being done to add authentication to these protocols. However, it will be some time before secure versions of these protocols become widely available and used.

Encryption technology is also used to protect the data path. One well known relay manufacturer offers encryption devices that are installed at both ends of the communication channel. There are a number of drawbacks to these "bump in the wire" devices. Since the data itself is encrypted, it can no longer be processed by intermediate devices such as data concentrators. Adding an encryption device at both ends of a communication link can rapidly become quite expensive and the encryption keys will need to be managed.

Encryption solutions remain a good approach to securing the data path. However, encryption is calculation intensive and introduces latency that will need to be taken into account when the system is designed. Furthermore, most networking devices were designed for the corporate IT world and do not meet substation environmental and electrical requirements.

Protecting Remote Maintenance Access To Devices

Many utilities are now using systems to provide remote maintenance access to IEDs in the field or the substation, using the TCP/IP network or dialup modems. This is exactly the type of application that NERC CIP is trying to regulate by requiring utilities to implement a System Security Management Program.

One fundamental requirement of NERC CIP is controlling access to IEDs and ensuring accountability. Access to critical cyber assets should be limited to authorized personnel only. Detailed logs must be maintained in order to be able to establish who did what, when. If an employee is terminated, access must be removed within 24 hours.

Typical IEDs do not implement true authentication and authorization. Passwords are used to control access to different levels of functionality such as reading data, modifying settings, and changing security. With such simple security schemes, it is not possible to identify the individual that performed a control function or changed a setting. The only way to remove access to a single individual is to change the passwords in all devices.

Multiple solutions are now available to provide secure access to IEDs. Access control can be implemented at the substation level, at the enterprise level, or both. Substation gateway devices and data concentrators can be used as an electronic perimeter to protect connected devices. Such gateway devices perform authentication and limit IED access to authorized users only. As long as the only access to the IED is through a gateway device, the IED password can even be removed.

Most vendor solutions integrate with corporate authentication systems such as Microsoft Active Directory and can even support two factor authentication through RSA SecurID. When this is the case, users log on to their computer using their standard corporate login and the remote access system manages IED access according to the identity of the user.

More sophisticated remote access systems can even perform automatic device login and command filtering. The user does not need to know the device password; the system does the device login and establishes a secure

communication path between the user and the device.

Change Control and Configuration Management, Backup and Recovery Tools

Maintaining up to date system drawings and documentation is a key component to good engineering practices. However, with the introduction of computers and IEDs, engineers are often challenged by the task of maintaining up to date records of device configuration and settings.

NERC CIP requires that utilities implement a configuration management system so that in the case of a component failure, a replacement device can easily be put in service with the same settings.

Document or software version control systems are quite commonly used in larger organizations. However, automated device configuration management systems are currently very rare, if not inexistent.

At least one vendor is planning on releasing a system to automate the process of managing device configuration changes. The system will scan connected devices, detect any change in the configuration, notify an administrator, and provide the capability to store the device configuration in a database as a backup.

Software patch management is another challenging NERC CIP requirement. In a corporate IT system, software patches are often installed automatically at night. However, this is not possible for a SCADA system without risking the loss of the whole system.

Monitoring, Logging and Reporting

Logs are a good tool to monitor the correct operation of a system. They also provide the capability of diagnosing problems and identifying their root causes. Since most IEDs provide limited logging capabilities, or none at all, the security management system must provide this logging capability, either by retrieving and consolidating device logs, or by doing the logging itself. However, analyzing logs is a humanly impossible task and requires automated tools. Numerous vendors provide such tools as this requirement is quite common in the IT field.

NERC CIP also requires extensive reports. Utilities must be able to provide an inventory of their cyber assets, authorized users, access permissions by users, access logs, and more. Again, many tools are available for this task.

Since NERC CIP requires enterprise-wide commitment and executive level support, utilities are often assigning responsibility of their cyber security program to the IT group, already familiar with these requirements, causing a culture clash with the engineering team.

SECURING CONTROL CENTER PROTOCOLS

As we have already discussed, networking technology can be used to secure the data path, but additional measures need to be taken to protect the application itself. Standard protocols are vulnerable to such simple attacks as replay, where known good commands are recorded and replayed at an importunate moment.

To secure data communications, the TC 57 Technical Working Group of IEC has developed the IEC 62351 set of standards. These standards apply to the protocols most commonly used in industry such as IEC 61870, IEC 61850 and DNP3:

- IEC 62351 Power System Control and Associated Communications - Data and Communication Security
- IEC 62351-1: Data and Communication Security – Introduction
- IEC 62351-2: Data and Communication Security – Glossary of Terms
- IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP
- IEC 62351-4: Data and Communication Security – Profiles Including MMS
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 Profiles
- IEC 62351-7: Data and Communication Security – Security Through Network and System Management

IEC 62351-3 provides security for protocols that use TCP/IP. It specifies the use of Transport Layer Security (TLS), previously known as Secure Socket Layer (SSL) to ensure authentication, confidentiality, and integrity.

IEC 62351-5 provides different solutions for serial protocols and devices that cannot support the computation requirements of encryption. Without encryption, it cannot guarantee the confidentiality of the data.

IEC 62351-6 provides a mechanism to digitally sign messages in order to provide authentication for peer-to-peer multicast protocols such as GOOSE. These messages need to be transmitted within 4 milliseconds and encryption or other security measures which affect transmission rates are not acceptable.

Finally, IEC 62351-7 defines Management Information Base (MIBs) that are specific for the power industry, to handle network and system management through SNMP-based capabilities.

CONCLUSION

SCADA systems and IEDs are key elements in the operation of the bulk power system. In order to reap the benefits promised by the Smart Grid, these systems will need to be made much more secure.

Security is now part of the design of any serious information system. For instance, information security provides us with the confidence necessary to trust our personal savings to banking system computers easily accessed through thousands of ATMs throughout the world.

Similarly, we need to develop the measures necessary to ensure that modern communications technology can continue to be used to retrieve the data provided by the thousands of IEDs that utilities are installing.

The field of SCADA security is still in its infancy. Regulatory bodies will need to develop measures that meet the requirement of experts in both the fields of security and process control. This will be a challenging task as there are very few domain experts, and the required mindsets are very different.

² Assuring Industrial Control System (ICS) Cyber Security, Joe Weiss PE, CISM, white-paper posted on ControlGlobal.com, September 2008

³ CRITICAL INFRASTRUCTURE PROTECTION – Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, United States Government Accountability Office (GAO), GAO-07-1036, September 2007

¹ WOLVES AT THE DOOR(S) OF THE HOUSE OF STRAW – The need for inherently secure control systems, Eric Byres, CONTROL Magazine, December 2007.