Security Issues for Smart Grid Networks

John A. Sturm – PhD Candidate, Indiana State University
March 3, 2011

ABSTRACT

The following paper is a survey and summary of research on the security needs for Smart Grid utility networks. In addition the paper includes a recommendation on possible security methods & protocols. "Continued existence of modern society is dependent on its industry and infrastructure and its ability to control electrical, chemical and mechanical transformations of materials and energy to produce desired results" as stated by the National Institute of Standards & Technology (NIST, 2004) in its study of the vulnerabilities and needs for industrial process control security. NIST has been soliciting input from the Process Control Industry and manufacturers on the appropriate security standards for over ten years and issued their first System Protection Profile (SPP) for ICS in 2004 (NIST, 2004) with help from the Instrumentation, Systems and Automation Society (ISA). However, the real concern is whether the security analysis and projected standards can address a "moving target". In the past industrial control systems were highly proprietary and one manufacturer (Fisher/Emerson, Foxboro, Honeywell, etc.) would typically provide a fixed, "turn-key" system for an entire factory and take care of all the systems & network integration issues from sensors to supervisory controllers. However, the industry has become both more "open" and more fragmented as new control network standards have appeared such as FOUNDATION Fieldbus and the OPC Foundation (developer of the OPC Unified Architecture – OPC UA). As a result there are more options in the design process and more flexibility to use "open" networks like the Internet Protocol (IP). The NIST SPP security analysis process depends on identifying a fixed, System Target of Evaluation (STOE) for the security analysis and it is critical that the STOE cover all possible vulnerabilities so there are no new, exposed "seams" that permit entry for a cyber attack.

1. INTRODUCTION

More and more systems are using the Internet for remote communications to tie distributed sensors to Supervisory Control and Data Acquisition (SCADA) systems. The internet protocol (IP) is readily available and provides low cost communications. However, the original Internet that evolved from the Arpanet had little security and over the years many security mechanisms have been added to IP to improve security such as IPSEC and SSL.

In the IEEE article by Kathy Kowalenko and Joseph Weiss on The Cyberhacker's Next Victim: Industrial Infrastructures (Kowalenko, 2010), she described that the systems most vulnerable to attack might be the control systems for critical facilities such as power and water-treatment plants, oil refineries, and mass transit systems. Per Joseph Weiss, author of two IEEE Expert Now eLearning online tutorials on how to protect the systems against cyber attack, he described that, "The relative obscurity of industrial control systems has generally protected them, but not anymore", Weiss says. "That's because the systems are no longer isolated. Intentional and unintentional cyber incidents are bound to increase", according to Weiss, "and protecting computers alone is not enough".

The problem is that security must be defined for each connection and is not automatically provided by the Internet Service Providers (ISPs) or telecommunication companies (TELCOs). In addition, Weiss described that "Authenticity (assuming that whatever or whoever is accessing a system has a right to be there) and system integrity (intruders cannot get in) are generally assumed, not assured," per the IEEE report. "Furthermore, confidentially requirements—which assure the information is accessible only to those authorized to have access—are often unknown or ignored" (Kowalenko, 2010). "What's even worse is that many control networks depend on outside sources—networks tied to networks tied to networks. These secondary networks cannot be trusted, as they are generally not secure." In addition Weiss has documented more than 170 cyber incidents against industrial control systems worldwide (Kowalenko, 2010).

2. SUMMARY ON DEVELOPMENT OF UTILITY NETWORK SECURITY STANDARDS

The ISA & NIST regularly track and report on the development of security for factory automation and utilities. According to Charley Robinson, manager of Standards and Technology at ISA (Robinson, 2010), "The ISA99-84 joint working group's initial work has focused on developing a security assurance level methodology for cyber security, similar to that of the current safety integrity levels (SIL) defined in ISA84. The plan is to define & develop processes for identifying intentional and systematic threats that can expose process hazards." In addition Robinson stated, the ISA99 work has also been recognized within the Framework and Roadmap for Smart

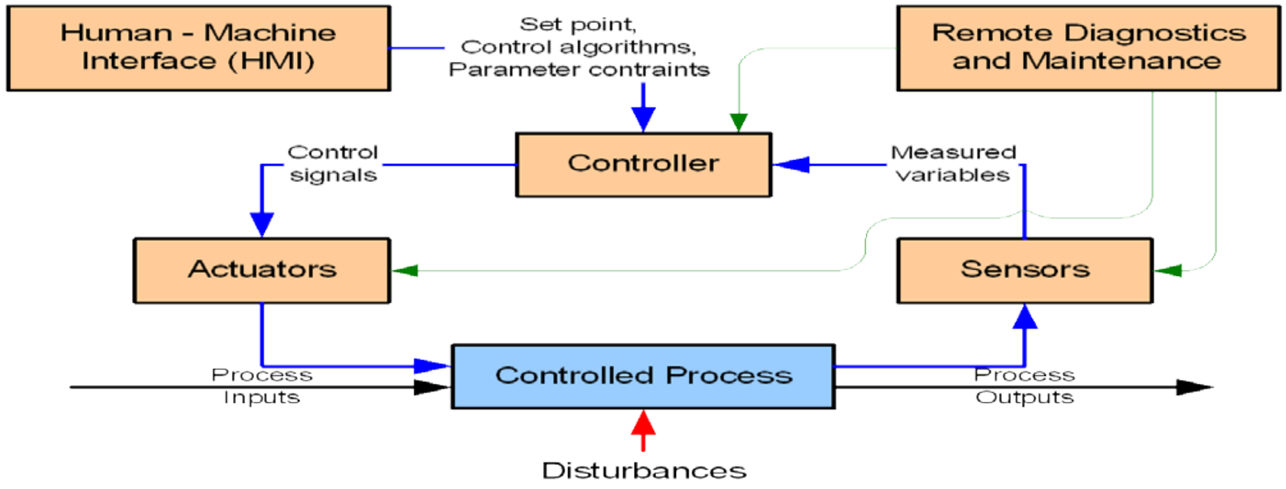

Figure 1. Generic Industrial Control System (NIST, 2004)

Grid Interoperability Standards (ANSI/ISA-99.02.01, 2009) released by the U.S. National Institute of Standards and Technology in August, 2010 (NIST, 2010). NIST's intent is to identify existing and draft standards vital to the success of the highly publicized Smart Grid program. All ISA99 published and draft documents are being made readily available for access by U.S. state utility commissions, the Federal Energy Regulatory Commission, and the National Association of Regulatory Utility Commissioners, who will be reviewing the content of all identified standards for regulatory purposes."

The typical supervisory control system is illustrated in Figure 1. Per NIST (2004), "An industrial control system consists of classes of components for the direct control of a process (the controller(s), actuators and sensors) a human machine interface and capabilities for remote diagnostics and maintenance. Although not represented in the diagram, there are also human elements such as operators and non-technical elements such as operating procedures."

The NIST System Protection Profile (SPP) focuses on that portion of the control system & communications relevant to the security analysis as the System Target of Evaluation (STOE), such as the area illustrated in Figure 2. Per the NIST (2004) SPP analysis, "This section describes the security subsystem of the industrial control system. The security subsystem includes both the information technology based components and the non-information technology based elements implemented via policies and operating procedures." In addition, "Particular attention is given to the interaction and dependencies between the security subsystem and the overall industrial control system. The STOE focuses on protecting data confidentiality, data integrity and system availability without interfering with safety system functions. Data integrity centers on protecting data flows to and from the controller and the other ICS components or subsystems. The STOE is also intended to protect system availability to assure continuity of operations" (NIST, 2004).

It is interesting that the boundary shown in Figure 2 excludes the corporate network (Intranet) and also excludes the Internet. In fact many SCADA systems utilize the Internet as the means for remote communications so the boundary illustrated in Figure 2 needs to be expanded to encompass the entire control system network. Otherwise the security recommendations would be compromised if the company SCADA systems used the Internet for remote communications and it was not part of the security STOE for analysis and policy management.

In fact NIST realized that many security vulnerabilities occur at the "seams" between systems and inserted the following guidance in the last section of the NIST System Protection Profile - Industrial Control Systems (NIST, page 146), "There are additional types of users in a distributed system, and their roles and responsibilities extend beyond the traditional user and administrator categories required user documentation. . . . One of these users may be external systems that are considered outside the STOE."

Most importantly the NIST (2004) SPP analysis stated, "the critical issue is that if there is a component that interfaces with the STOE but for whatever reason the component is not part of the STOE, then it is necessary to":
a) Define the interfaces between the STOE and the external component;
b) Define the security properties, if any, that are provided by or that are provided across the interfaces,

c) Define how the STOE and external component will authenticate themselves to each other;
d) Define the secure method by which the STOE and the external component will communicate such that a security policy is enforced;
e) Define the security agreement between the parties with responsibility for operating the STOE and the external component to establish the business rules that govern how that interface is to be used and maintained over time.
f) Define the security relevant configuration parameters that allow implementation, integration, and enforcement of system security policies.

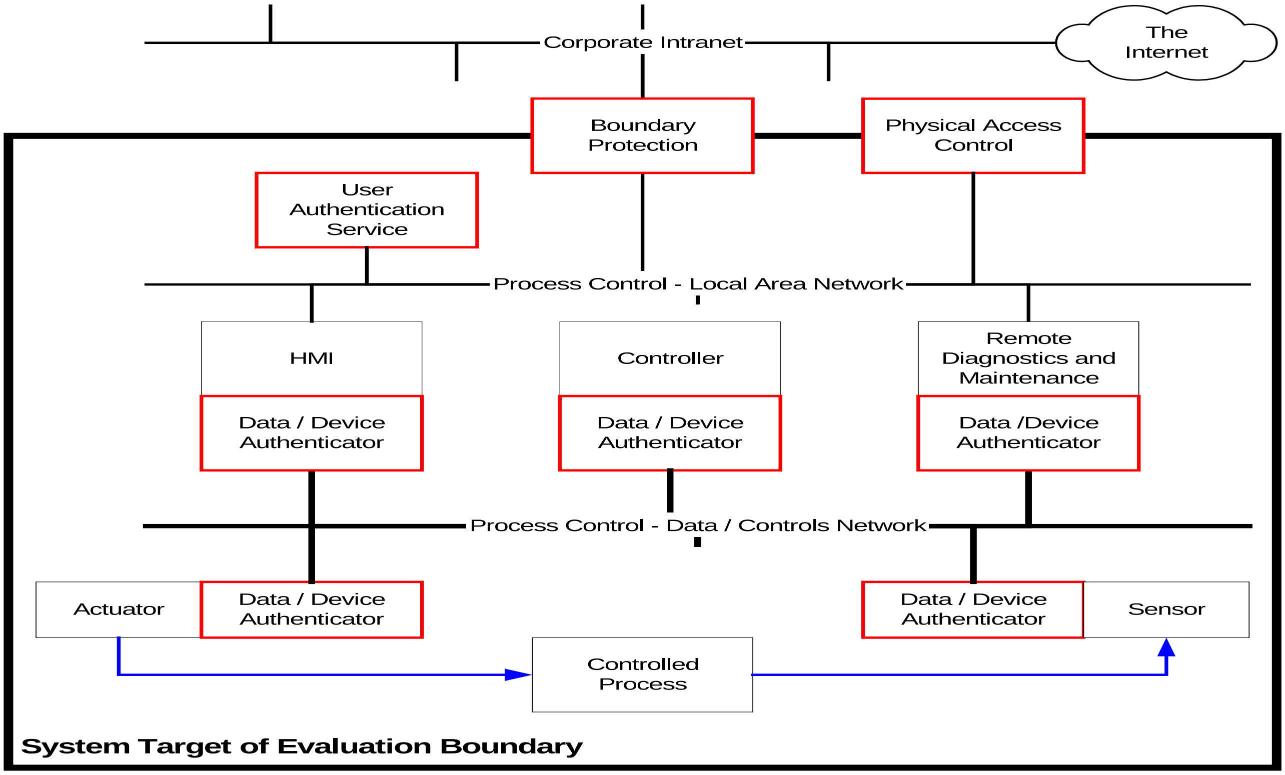
Corporate Intranet
The Internet
Boundary Protection
Physical Access Control
User Authentication Service
Process Control - Local Area Network
HMI
Controller
Remote Diagnostics and Maintenance
Data / Device Authenticator
Data / Device Authenticator
Data /Device Authenticator
Process Control - Data / Controls Network
Actuator
Data / Device Authenticator
Data / Device Authenticator
Sensor
Controlled Process
System Target of Evaluation Boundary

Figure 2. The NIST System Target of Evaluation (STOE) used for security analysis of Industrial Control Systems (NIST, 2004).

The steps recommended above basically enable the gap or seam in the security boundary to be stitched together with sufficient policy enforcement to protect against a cyber attack from penetrating the interface between the STOE and the remote system. As mentioned, current process control systems are moving away from proprietary networks (HART, Modbus, etc.) to more open systems such as Foundation Fieldbus, OPC UA and ultimately to the Internet Protocol (IP). Thus process control parameters are often transmitted outside the expected bounds illustrated in Figure 2 and are sometimes overlooked as a critical part of a control network.

The NIST SPP Security Analysis (NIST, 2004) includes a detailed list of security and Information Assurance (IA) attributes for analysis and reporting. The detailed security and IA attributes include consideration of software, hardware, systems and management policy issues as part of the scope of the System Target of Evaluation (STOE) for security analysis (NIST, 2004).

The following list from the System Protection Profile analysis indicates the scope of the System Target of Evaluation (STOE) for utility control systems (NIST, 2004):

- Authentication
- Confidentiality
- Integrity
- Availability
- Boundary Protection
- Access control
- Backup / Recovery
- Audit
- Monitoring
- Non-interference with safety critical functions
- Self Verification
- Emergency power
- Security Plans, Policies & Procedures

3. SURVEY OF EMERGING PROCESS CONTROL AUTOMATION NETWORK PROTOCOLS AND SECURITY IMPLICATIONS

As described earlier, the Process Control Industry is currently in a state of transition from proprietary protocols to an open architecture. Three of the major emerging open technologies and networks for utility & industrial control include:

- Foundation Fieldbus,
- OPC Unified Architecture (OPC UA), and the
- Secure Mobile Architecture (SMA), Industrial Ethernet and WIFI & WiMAX

FOUNDATION Fieldbus is an open technology, allowing automation and MIS devices to be interconnected on a common plant-wide or remote SCADA network using High Speed Ethernet (HSE) (Glanzer, 2005). Furthermore, per David Glanzer, "this open network architecture enables control devices from different manufacturers to interoperate on the same control network without the need for custom programming." Again the concern is that multiple "ad-hoc control systems" can be added at any time without a full control system SPP review to analyze security vulnerabilities. In addition to the standard IEEE 802 Ethernet model, HSE employs standard Internet protocols, including TCP/IP, UDP and SNMP. "The use of standard Ethernet/Internet protocols, coupled with COTS Ethernet cable, switches and routers, allows HSE networks of any size or topology to be built" (Glanzer, 2005).

The ease of implementation and broad flexibility of new emerging networks like Fieldbus and OPC UA means that security reviews should be scheduled on a regular basis in order to view and incorporate new changes into a company's overall security policies. Otherwise, one small control network modification can open a convenient "backdoor" for cyber attack.

As a result of the utility and industrial migration to open networks, more systems from different vendors can be integrated to build complex control systems. The customer pressure for open standards and flexibility to reduce cost is understandable; however, the customer needs to realize that they are taking more responsibility for the overall security systems design. How many process control industry customers have the support staff to conduct the NIST recommended security evaluations and STOE analysis? OPC UA offers significant security capabilities but they need to be designed and implemented as part of the overarching company's security policy management. Boeing offers a good example of a company migrating to new technology and also making the investment in security for "defense-in-depth" against cyber attack (Gurtov, 2008).

As mentioned, Industrial Ethernet (IE) has become one of the most important standards for factory automation. It provides the network backbone that carries control information and data for improved process control and greater efficiency. For industrial plants, the importance of the information technology & Ethernet cabling infrastructure is similar to that of other fundamental building utilities such as heating, lighting and main power supplies. Interruptions to service can have serious impact; and "poor quality of service due to lack of planning, use of inappropriate components, incorrect installation, poor administration or inadequate support can threaten an organization's effectiveness" per the IAONAs Guidelines (2003). In addition, the organization and layout of the Ethernet cabling also aids security by providing restricted access for "packet sniffers" and subsequent eavesdropping on packet transactions.

Per the Guidelines (2003), there are four phases in the successful installation of Industrial Ethernet (IE) in plants and Boeing serves as a good example. These are:
1. Design - the selection of IE components and their configuration;
2. Specification - the detailed requirement for the cabling, its accommodation and associated building services addressing specific environment(s) identified within the premises together with the quality assurance requirements to be applied;
3. Implementation - the physical installation in accordance with the requirements of the specification;
4. Operation - the management of connectivity and the maintenance of transmission performance during the life of the network.

For security planning and enforcement, it would be reasonable to add a fifth phase in the successful installation of information technology in industrial plants, namely:

5. Information Assurance & Security - identify all computing, SCADA field devices, and robotic systems as described by the Secure Mobile Architecture (SMA) as part of the System Target of Evaluation (STOE) for security analysis.

The Factory Network Planning Strategy (road map) and guidance should incorporate the complexity of the countless IP-addressable devices being deployed and developed. In the following plant view (Figure 3) from the IAONAs Guidelines (2003), there are numerous interconnected assembly areas that need to function in synchronization.

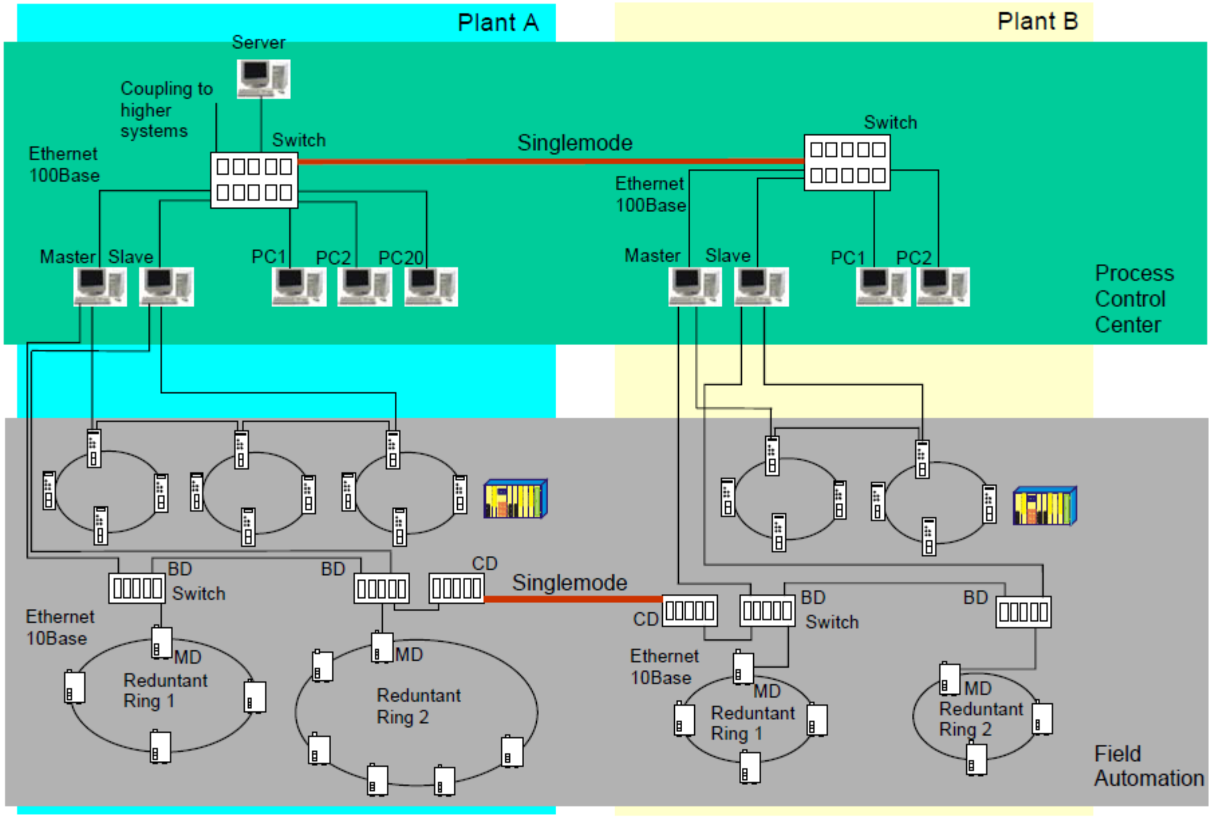

Figure 3. Practical example for Industrial Ethernet per IAONAs Guidelines (2003).

Secure Mobile Architecture (SMA)

The Boeing Aircraft assembly plant in Seattle is an example of the new Secure Mobile Architecture (SMA) and Host Identity Protocol (HIP) that assign unique Host Identity Tags (HIT) to all computers and field devices such as transmitters, repeaters, bridges and operator terminals (Paine, 2007). The OpenGroup published the SMA architecture and the components include (Gurtov, 2008):

- Industrial Ethernet
- Host Identity Protocol (HIP)
- Public Key Infrastructure (PKI)
- Network Directory Service (NDS)
- Location Enabled Network Service (LENS)

In the SMA Architecture cryptographic identities are associated with each and every packet. As IP-based devices move around the factory floor, the IP address changes are transparent to applications and connections since the Host Identity Tags (HIT) stay fixed with each field device (Paine, 2007). The SMA architecture significantly improves the Enterprise network architecture and security by providing (Paine, 2007):

- Improved flexibility and agility
- Network-enforced, end-to-end security
- Centralized access control with delegated authority
- Reduced operational cost and complexity
- Uniform internal/external access method

In summary, Boeing has used Industrial Ethernet to integrate many types of Host Computers, Field Devices, and even 802.11 WIFI Wireless Access Points with remote SCADA networks under the Secure Mobile Architecture (Gurtov, 2008). The SMA/HIP Endbox (FactoryNet) and HIP Bridge enable legacy Ethernet equipment to use SMA in the factory (FactoryNet) for secure communications from any point to any other point. The architecture provides a secure handoff using the End-to-End HIP-Enabled Security Associations (SAs) (Paine, 2007). Likewise a secure mobile handoff is possible using SMA & HIP over wireless 802.11 WIFI or WIMAX channels. The security issues previously identified by NIST in Table 1: Authentication, Confidentiality, Integrity, Availability, Boundary Protection, Access control, Backup / Recovery, Auditing, Monitoring, Non-interference with safety critical functions, Self Verification, Emergency power, Security Plans, and Policies & Procedures are being addressed at a core system-level so security is built-in and not patched on after the design is complete.

4. CONCLUSIONS

In summary, “the overall security concern for an ICS typically originates from malicious threat agents attempting to disrupt an industrial process such as to interfere with it specified operation (e.g. to create a power outage) or to negatively impact on the environment and/or personnel safety (e.g. exploding a fuel tank or destabilizing chemical process to free noxious gases)” per NIST (2004). NIST has also provided a security analysis approach called the System Protection Profile to identify and address the risks with appropriate security policies. The key part of the analysis is to define the security boundaries (the STOE) and realize that new control system technology (i.e. Fieldbus, OPC UA, IP-based communications, etc.) have made the boundaries very dynamic. Security analysis needs to be based on active security analysis through continuous network monitoring to detect and “firewall” unauthorized taps.

REFERENCES:

AGA. (2006). AGA Report No. 12 - Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan. Retrieved March 1, 2010, from http://www.aga.org/NR/rdonlyres/B797B50B-616B-46A4-9E0F-5DC877563A0F/0/0603AGAREPORT12.PDF

ANSI/ISA-99.02.01(2009). Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, ISA, January 2009. Retrieved March 1, 2011, at http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

Emerson Process Management. (November 3, 2009). Emerson introduces FOUNDATION™ Fieldbus Interfaces for remote oil, gas and water applications. Retrieved March 1, 2010, from http://www2.emersonprocess.com/en-US/news/pr/Pages/911-ROC-fieldbus.aspx

Glanzer, D. (2005). FOUNDATION Fieldbus HSE: An Open, High Speed Solution. Retrieved March 1, 2010, from http://www.fieldbus.org/images/stories/enduserresources/technicalreferences/documents/HSE%20Brazil%20articlefinal.pdf

Fieldbus Foundation ISA (2010). ISA standards and related information. Retrieved March 1, 2010, from www.isa.org/standards

Gurtov, A. (2008). Host Identity Protocol (HIP): Towards the Secure Mobile Internet.
Chippenham, England: John Wiley & Sons Ltd.

IAONAs. (2003). Industrial Ethernet - Planning and Installation Guide. Version 4.0, October 2003. Published by IAONA e.V., Joint Technical Working Group (JTWG) Wiring Infrastructure. Retrieved March 1, 2010, from http://www.iaona-eu.com

Kowalenko, K. and Weiss, J. (14 April 2010). FEATURE STORY - The Cyberhacker's Next Victim: Industrial Infrastructures. THE INSTITUTE - IEEE Home » Featured This Month » Article, Retrieved March 1, 2010, from http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2201&article=tionline/legacy/inst2010/apr10/featuretechnology.xml&

Nikander, P. and Sarela, M. (2004). Applying Host Identity Protocol to Tactical Networks.
Helsinki University of Technology and Ericsson Research IP Networks

NIST (2010). National Institute of Standards and Technology Interagency Report (NISTIR) 7628, vol. 1 Guidelines for Smart Grid Cyber Security:
Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. The Smart Grid Interoperability Panel – Cyber Security Working Group Retrieved March 1, 2011, from http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

NIST (2004). System Protection Profile - Industrial Control Systems Version 1.0. Retrieved March 1, 2010, from http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc

Paine, R. (2007). Secure Mobile Architecture SMA Basics for IEEE 802.21 May 2007 Secure Mobile Architecture (SMA) Demo Team, Published by Boeing Aircraft, Math & Computing Technologies. Retrieved March 1, 2011, at http://www.ieee802.org/21/doctree/2007_Meeting_Docs/2007-05_meeting_docs/21-07-0212-00-000-NGI_SMA_21_Secure_Multi-Network_Handoff.ppt

Robinson, C. (February, 2010). ISA99: Charting a security standards roadmap into a risky new decade. ISA | InTech, Retrieved March 1, 2010, from http://www.isa.org/InTechTemplate.cfm?Section=Standards_Update1&template=/ContentManagement/ContentDisplay.cfm&ContentID=81089RESOURCES

Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats.
Highland Park, New Jersey: Momentum Press.