U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Visualization & Controls Program Peer Review

Control Systems Security
Project Summaries

Arlington, Virginia
October 18, 2006

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

VISUALIZATION AND CONTROLS PROGRAM PEER REVIEW, SESSION B

WEDNESDAY, OCTOBER 18, 2006

PROGRAM MANAGER – HANK KENCHINGTON

Table of Contents

SCADA/EMS Cyber Security Assessments (INL) 1

Cyber Security Assessment of Inter-Control Center Communications Protocol Implementations (SNL, INL, PNNL) 1

SCADA Authentication Protocol (PNNL) 2

Security Modeling of Wide Area Monitoring Systems (PNNL) 2

Development of Virtual Control Systems Environment Tool (SNL) 3

Cyber Security Assessment of Advanced Metering Infrastructure (SNL) 3

Open Architecture, Interoperable Design for Control Systems (SNL) 4

AGA-12 Cyber Security Assessment Performance Testing (PNNL) 4

AGA-12 Cyber Security Assessment Cryptographic Analysis (SNL) 5

Security Metrics for Control Systems (SNL) 5

Trustworthy Cyber Infrastructure for the Power Grid 5

VISUALIZATION AND CONTROLS PROGRAM PEER REVIEW
CONTROL SYSTEMS SECURITY: PROJECT SUMMARIES

SCADA/EMS Cyber Security Assessments

Principal Investigator: Bob Hill, Idaho National Laboratory (INL) – Robert.Hill@inl.gov

With mounting evidence suggesting an increased probability that malicious attacks may be launched against energy control systems, there is a critical need to understand specific cyber vulnerabilities and corresponding mitigation strategies. This need is being addressed by SCADA/ Energy Management System (EMS) Cyber Security Assessments conducted at the National SCADA Test Bed (NSTB) facility at INL and at on-site field installations of control systems. The systems assessed are typically new products on the market, since these are the products for which vendors can best justify business expenditures for enhanced security. Control system assessments at INL are conducted in an environment that includes the key equipment and characteristics of an actual installation. This environment provides typical data flow and component response without the risk of interrupting normal operations of a production system. Subsequent on-site assessments help to determine whether the vulnerabilities identified in a laboratory setting are relevant in actual installations.

Upon completion, assessment results are documented and provided to the system developers. Findings from each assessment are also added to a cumulative *lessons learned* document that compiles findings across system types. Control system developers can use this information as the basis for hardening their next-generation systems and for developing patches applicable to legacy systems. Through presentations at vendor User Group Meetings and selective sharing of assessment reports, results and mitigation strategies are also provided to customers to improve their understanding of potential vulnerabilities in their specific systems and to inform them of good practices that can help address those vulnerabilities. These outcomes support several of the milestones identified in the ***Roadmap to Secure Control Systems in the Energy Sector***, including developing baseline methodologies for conducting self-assessments, identifying best practices for control systems security, determining how to establish secure connectivity between business and control networks, and helping vendors develop control systems with built-in, end-to-end security.

Cyber Security Assessment of Inter-Control Center Communications Protocol Implementations

Principal Investigator: John Michalski, Sandia National Laboratories (SNL) – jtmicha@sandia.gov

The Inter-Control Center Communications Protocol (ICCP) task responds to the ***Roadmap to Secure Control Systems in the Energy Sector*** strategies to "Measure and Assess Security Posture" and "Develop and Integrate Protective Measures." This two-fold task consists of (1) identifying abnormal data sets that can disrupt standard ICCP client-to-server communications and (2) providing utility support in the integration and operation of secure ICCP. The ICCP work package is therefore described as two separate components: "Standard ICCP" and "Secure ICCP."

The **Standard ICCP** subtask examines the current form of ICCP, the primary protocol used to communicate status and value data, commands, and general text information between EMS control centers. This task will determine whether vulnerabilities exist that might be exploited to

either corrupt data or gain entry into the SCADA/EMS. Once exploitable vulnerabilities are found, the effectiveness of existing mitigation techniques will be tested.

The **Secure ICCP** subtask investigates security enhancements of the new ICCP protocol, its impacts when implemented in control systems, and how identified inter-dependencies of the communication process impact the operation and security of dependent ICCP applications. This investigation will provide industrial users insight into the use of this protocol and how identified interdependencies impact the operation and security of dependent applications.

SCADA Authentication Protocol

Principal Investigator: Mark Hadley, Pacific Northwest National Laboratory (PNNL) – Mark.Hadley@pnl.gov

This task will continue development of a novel SCADA communications authenticator technology developed by the Pacific Northwest National Laboratory (PNNL) and funded by the U.S. Navy. The Secure SCADA Communications Protocol (SSCP) "wraps" original, serial SCADA communication traffic with a unique identifier and an authenticator. The SSCP then uses a unique identifier in the wrapper to ensure the communication is valid, and can detect and prevent various attack scenarios—including man in the middle, injected traffic, or message replay. The SSCP is envisioned to be available as an embedded software solution running on the SCADA master or input/output server, as a bump-in-the-wire industrial computer, or as a small micro-controller dongle. The authenticator technology directly supports the ***Roadmap to Secure Control Systems in the Energy Sector*** milestone targeting widespread implementation of methods for secure communication between remote-access devices and control centers.

In terms of the DOD *technology readiness level* definitions, the SSCP has currently achieved level 7 (i.e., system prototype demonstration in an operational environment). The goal for this project will be to move the SSCP toward technology readiness (level 8), where the technology has been proven to work in its final form and under expected conditions. Comprehensive testing will be performed to confirm that the technology will fulfill its technical objectives when deployed under a variety of expected conditions in the field. The goal is to facilitate earlier industry adoption of a novel security technology that is well suited for securing control systems used by energy infrastructures.

Security Modeling of Wide Area Monitoring Systems

Principal Investigator: Jeff Dagle, PNNL – Jeff.Dagle@pnl.gov

Wide area measurement systems (WAMS) incorporate the advanced measurement technologies, information tools, and operational infrastructure that facilitate our understanding and management of increasingly complex, large power systems. This task will evaluate the security of typical WAMS to identify cyber vulnerabilities and provide guidance to mitigate those identified vulnerabilities and to improve system security. This work supports the ***Roadmap to Secure Control Systems in the Energy Sector*** research and development priority to develop automated security state and response support systems.

Independent system operators and transmission utilities on the North American electrical grid are adopting WAMS technology and have applied it to monitoring applications in support of planning and operations. In the near future, they will make the transition from using WAMS for monitoring-only functions to using it with wide area control and advanced decision support tools

in support of real-time operations. This task will provide a common framework for evaluating security implications and for generating information that industry can use to help ensure the security and integrity of these systems, which will ultimately enhance the reliability and security of the Nation's electrical power infrastructure.

Development of Virtual Control Systems Environment Tool (SNL)

Principal Investigator: Pete Sholander, SNL – peshola@sandia.gov

The Virtual Control System Environment (VCSE) tool will simulate control systems devices and network communications to enable real-time, hardware-in-the-loop (HITL) emulation. The VCSE tool addresses the ***Roadmap to Secure Control Systems in the Energy Sector*** strategy to "Measure and Assess Security Posture" by performing analyses on modeled control systems to help analysts determine the robustness of the control system security postures. By supporting the design, integration, and evaluation of security solutions used in legacy systems, the VCSE tool also addresses a key roadmap challenge: "security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance."

The VCSE tool will analyze and assess large control systems in a simulation environment without disrupting current operations. The proposed VCSE tool focuses on (a) the rapid development of new models for the control systems element; (b) easy federation of existing simulation, visualization, and analytic tools; and (c) evaluation of cyber security postures in large infrastructures.

As control system complexity and interconnectivity increase, so does the threat environment. Modeling tools such as the VCSE will assist asset owners in making better-informed decisions in the selection of security solutions for their current and next-generation systems, and will help overcome the technological challenges associated with securing both current and emerging control systems components and system architectures.

Cyber Security Assessment of Advanced Metering Infrastructure (SNL)

Principal Investigator: Raymond Parks, SNL – rcparks@sandia.gov

This project will investigate cyber security issues regarding the use of advanced metering infrastructures (AMI) in electric utilities and then use these findings to develop a sustainable security *good practices* guide to facilitate the secure deployment of future AMI systems. AMI is the next logical development of Automatic Meter Reading (AMR). AMR has been deployed by utilities throughout North America and Europe. AMI adds the communications infrastructure to provide two-way communications to Advanced or Smart Meters. AMI systems have been deployed in Italy (27 million connected meters), Alabama, and Mississippi, although the latter two locations implement full demand response only for commercial and industrial customers. AMI will be deployed within the next two years in Sweden, in the Netherlands, and by several utilities in California. AMI will be a major contributor to the stabilization of the electric grid in the future—not just through peak load management, but through the other distribution technologies it enables.

Although the Electric Power Research Institute (EPRI) is working on AMI standards and an OpenAMI group has been formed to promote open standards for AMI, these standards address

functionality more than security. During a recent SANS SCADA Security Summit, representatives of several California utilities expressed concern regarding the cyber security of AMI technologies, and were clearly not confident that vendors or standards groups have adequately addressed AMI security. In addition to these concerns, the NSTB's AMI cyber security assessment also directly addresses a research and development priority identified by industry in the ***Roadmap to Secure Control Systems in the Energy Sector*** recommending the development of baseline security requirements defined across the system life-cycle regarding the fundamental, intermediate, and advanced security posture of AMI.

Open Architecture, Interoperable Design for Control Systems (SNL)

Principal Investigator: Jason Stamp, SNL – jestamp@sandia.gov

The Open Architecture and Interoperable Design to Secure Legacy Systems project seeks to design add-on devices that will bring the security of legacy systems up to an acceptable level. This work addresses two strategies from the ***Roadmap to Secure Control Systems in the Energy Sector:*** "Develop and Integrate Protective Measures" and "Detect Intrusion and Implement Response Strategies." The design will be based upon an open architecture to promote interoperability and to provide better resistance to cyber attack, improved authentication for data and access, and control systems security and state-of-health monitoring capability.

The Open Architecture and Interoperable Design (OA/IO) utilizes bump-in-the-wire devices to provide encryption, authentication, secure remote management, logging, intrusion detection, and firewalls to legacy automation platforms on a per-platform basis. These legacy systems range from older, serial- and mainframe-based systems to more modern ones that are poorly secured, including yet-to-be installed systems that may benefit from ongoing but nascent automation security efforts.

AGA-12 Cyber Security Assessment Performance Testing (PNNL)

Principal Investigator: Mark Hadley, PNNL – Mark.Hadley@pnl.gov

This task consisted of developing a test plan for performance testing of serial cryptographic (encryption and authentication) hardware. Developed in collaboration with the North American Electric Reliability Council Control Systems Security Working Group (NERC CSSWG), the test plan includes a variety of protocols and industry environments that cryptographic hardware devices may encounter in operational settings in the electric utility industry. In FY 2005, limited security testing of actual hardware devices was initially conducted to validate the test plan for specific protocols and operational environments, which helped prepare for FY 2006 performance testing. Current testing is now far more comprehensive in nature and includes testing of individual devices as well as examination of the impact and overhead of multiple cryptographic devices in a virtual wired and/or wireless network (i.e., test results for this activity will be used to accurately simulate the impact of cryptographic devices in networks).

NSTB's AGA-12 performance testing will create a detailed test plan for use by multiple industries based on an impartial review of performance data. In turn, these tests will help industry understand the expected performance impacts associated with introducing AGA-12 cryptographic modules into serial communication environments.

AGA-12 Cyber Security Assessment Cryptographic Analysis (SNL)

Principal Investigator: Jason Stamp, SNL – jestamp@sandia.gov

This task consisted of an analytical review of AGA-12, Part 2 for cryptographic security. It focused on the core cryptographic elements of AGA-12, Part 2, including the algorithms, protocols, and key management for encryption and authentication of SCADA communications. From this analysis, the NSTB documented security findings and recommendations and communicated these findings back to the AGA-12, Part 2 authors. These recommendations were incorporated into subsequent revisions of the AGA-12, Part 2 standard and had a significant impact on the final standard issued in March 2006. The adoption of the recommendations by AGA will ultimately improve the security of AGA-12 certified encryption devices for use in energy sector control systems, while also providing vendors with a validated standard for the development of AGA-12 security technologies. As part of this research, NSTB also prepared a separate report providing guidance for the future testing of similar control systems security devices.

Security Metrics for Control Systems (SNL)

Principal Investigator: Annie McIntyre, SNL – amcinty@sandia.gov

This project will develop an approach to security metrics for control systems that the asset owner or manager can apply at the organizational level. The work includes development of a metrics taxonomy and guidelines for using metrics to measure standards compliance. Responding to the "Measure and Assess Security Posture" strategy of the ***Roadmap to Secure Control Systems in the Energy Sector***, this project seeks to develop reliable and widely accepted security metrics to gauge the security posture of control systems. It also addresses industry stakeholder requests for a way to measure the cost/benefit of security alternatives. Successful completion of this project requires the identification and analysis of existing metrics, the development and testing of new metrics, and metric categorization and implementation strategies.

This project targets asset owners and control systems management as the appropriate organizational level to measure levels of compliance with existing and emerging control systems standards. The project will identify existing metrics, their use within the control systems environment, how those metrics are implemented, and resulting conclusions. In addition, this task will develop a common language for asset owners to understand security metrics and how they align with operational priorities. Finally, asset owner will receive guidance on the use of metrics to measure levels of compliance with existing standards. This approach will influence security at the appropriate organizational levels and allow industry feedback to guide activities for maximum impact.

Trustworthy Cyber Infrastructure for the Power Grid

Principal Investigator: Bill Sanders, Univeristy of Illinois at Urbana-Champaign – whs@uiuc.edu

The Trustworthy Cyber Infrastructure for the Power Grid Initiative (TCIP) National Science Foundation (NSF) Cyber Trust Center was created in August 2005 to address the challenge of how to protect the nation's power grid. The NSF awarded $7.5 million over five years to the project, which is led by the University of Illinois ITI team and also involves researchers at

Cornell University, Dartmouth College, and Washington State University. The Department of Energy and the Department of Homeland Security have also joined with NSF in funding and managing the effort.

The TCIP seeks to protect the nation's power grid by providing the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. The center will significantly improve the way the power grid cyber infrastructure is built, making it more secure, reliable, and safe.

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

oe.energy.gov/randd/css.htm