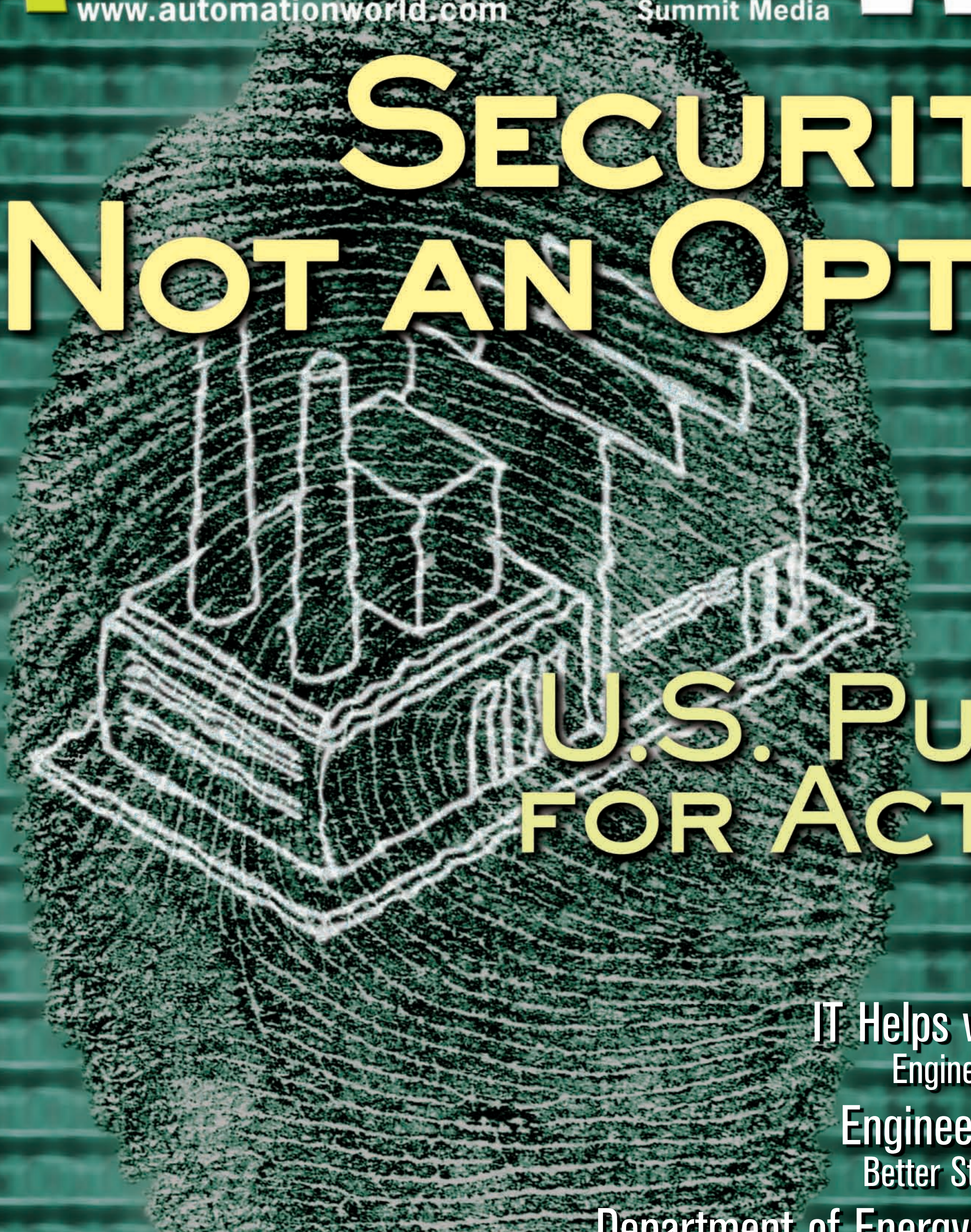
FIFTH ANNIVERSARY ISSUE

Automation World®

www.automationworld.com

Summit Media

June 2008



Security is Not an Option

U.S. Pushes for Action

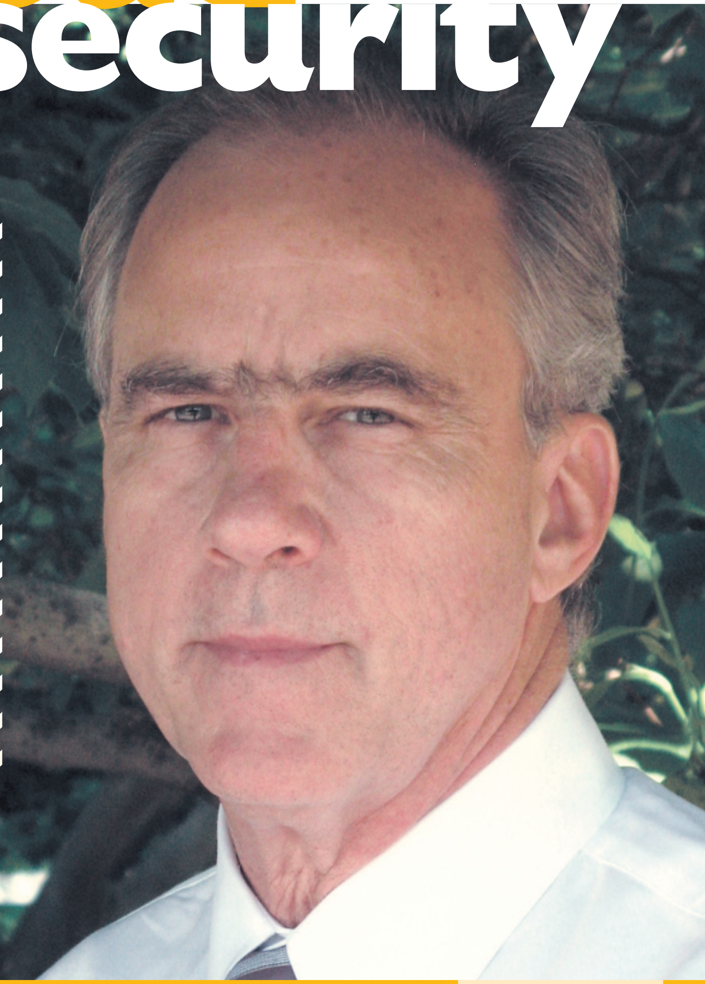
IT Helps with Plant Security
Engineers Ensure Plant Uptime

Engineers Building Models
Better Standards, Less Ambiguity

Department of Energy on Cyber Security
Exclusive Interview

Special Pullout Section
Packaging Automation Review

on the road to cyber security



A 10-year roadmap for achieving control system cyber security in the energy industry has been hailed as a model for other industries. Here's a look at progress to date.

Among the many initiatives aimed at providing cyber security for the nation's critical infrastructure, the effort that led to a January 2006 document known as the "Roadmap to Secure Control Systems in the Energy Sector" stands out as one involving significant public/private sector collaboration.

The Roadmap, which lays out a 10-year vision, has been recommended by the National Infrastructure Advisory Council as a model for other industries to follow in developing their own sector-specific roadmaps. In March this year, the Water Sector Coordinating Council Cyber Security Working Group published a "Roadmap to Secure Control Systems in the Water Sector," which lays out a similar 10-year vision.

Hank Kenchington, a senior manager with the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (OE), was a member of the Control Systems Roadmap Steering Group for the Energy Roadmap, and is called out in the foreword for his "outstanding leadership" on the project. Kenchington serves as program manager for the OE's National SCADA Test Bed (NSTB), which is playing an important role in achieving the Roadmap vision.

To get an update on the Roadmap initiative as well as the latest NSTB activities, *Automation World* Managing Editor Wes Iversen recently submitted a series of e-mail questions to Kenchington.

Automation World: The Roadmap to Secure Control Systems in the Energy Sector was published in January 2006. Can you briefly describe the genesis of that document?

Hank Kenchington: The importance of adequately securing control systems has been known for some time. In 1998, the President's Commission on Critical Infrastructure Protection highlighted the criticality of control systems and the increasing risk of energy disruptions due to cyber attack. In 2003, the Bush Administration elevated the issue, stating in its "National Strategy to Secure Cyberspace" that "securing SCADA/DCS is a national priority" (in reference to supervisory control and data acquisition/distributed control systems).

The Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability (OE) has been working with the private sector to enhance critical infrastructure protection since the 1990s. In 2003, the Bush Administration, through the DOE, initiated the development of the Roadmap, working in partnership with the oil, gas, and electricity industries. At that time, a number of activities designed to help secure control systems were underway. However there was no clear vision or strategic framework for coordinating these diverse activities. Moreover, while a number of reports recognized the threat and potential consequences of a cyber attack on control systems, the control system security needs of private sector asset owners and operators were not being addressed. The private sector – which collectively owns and operates approximately 80% of U.S. energy sector assets – lacked a compelling business case to support investment in cyber security. Coupled with the scope and complexity of the problem, these issues underscored a significant need for increased public-private partnership to maximize limited resources and effectively enhance control system security. Private- and public-sector energy stakeholders alike recognized that securing energy sector control systems was a shared responsibility.

From a technology perspective, 85 projects from nearly 20 public and private organizations have been launched supporting the goals identified in the Roadmap.

To develop the Roadmap, DOE collaborated with the U.S. Department of Homeland Security (DHS), and Natural Resources Canada to facilitate a two-day workshop in 2005. We worked closely with industry leaders through a 17-member Roadmap Steering Group to design and conduct the workshop and synthesize the results, careful to ensure that the resulting Roadmap was an industry-driven plan. Accordingly, the majority of the workshop's 55 participants were electricity, oil, and natural gas asset owners and operators, while the remainder consisted primarily of control systems vendors, national laboratories, and academia. The final Roadmap was published in January of 2006.

In 2003, Homeland Security Presidential Directive-7 (HSPD-7) designated DOE as the Sector-Specific Agency responsible for coordinating activities with the energy sector to enhance protection of Critical Infrastructure and Key Resources (CI/KR). These activities are carried out within the framework of the DHS National Infrastructure Protection Plan (NIPP). As noted in the Energy Sector-Specific Plan of the NIPP, the Roadmap established the key cyber security goals addressing the "full spectrum of cyber security priorities in the energy sector."

AW: The overriding vision stated in the Roadmap is that in 10 years, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function. At just beyond two years into that 10-year period, how would you assess the early progress toward that goal?

Kenchington: I think we are making progress along several fronts. From a technology perspective, 85 projects from nearly 20 public and private organizations have been launched supporting the goals identified in the Roadmap. To help track progress, DOE created the ieRoadmap (Interactive Energy Roadmap), a Web-based tool that allows principal investigators to register and self-populate a database that links to the challenges identified in the Roadmap. The ieRoadmap, hosted on the Process Control Systems Forum Web site (www.pcsforum.org), provides a mechanism to encourage collaboration, identify active areas of work, expose gaps and enable partners to leverage resources, as well as inform owners and operators of emerging technologies.

DOE supports the Roadmap primarily through our National SCADA Test Bed (NSTB) program, which conducts cyber security assessments of control systems and related technologies, develops advanced control system technologies, conducts modeling and simulation to better evaluate risk, and engages in industry partnership and outreach. To date, the NSTB has conducted test bed and on-site field vulnerability assessments of 15 control systems from vendors including ABB, Areva, GE, OSI, Siemens, Telvent and others, as well as assessments of four control system component technologies at the test bed. As a result of this work, six next-generation "hardened" systems have been developed by the participating vendors—21 of one vendor's hardened systems have been deployed in the marketplace. Participating vendors have issued five software patches addressing six critical security issues in response to vulnerabilities discovered by NSTB. One particular software patch issued by one vendor to secure its legacy systems has been downloaded by 82 utilities currently operating those systems.

System assessments have revealed common vulnerabilities and easy-to-implement, immediate security fixes that apply across the board. Outreach has helped disseminate this knowledge. For example, more than 1,200 energy sector stakeholders have participated in training workshops conducted by NSTB that educate system operators on best practices for control systems security. Approximately another 500 individuals were expected to participate in scheduled NSTB training events through April and May of 2008. In addition, NSTB partners with the North American Electric Reliability Corp.'s (NERC) Control Systems Security Working Group to publish mitigations for the vulnerabilities in the annual "Top 10 Vulnerabilities of Control

Systems and Their Associated Mitigations" report.

The recently formed Energy Sector Control Systems Working Group will drive further implementation of the Roadmap and has already launched key initiatives to accelerate progress. For example, the working group was scheduled to hold an ieRoadmap Workshop in Chicago on May 28-29. The workshop was designed to provide presenters with an opportunity to discuss their control systems security research and projects with the working group and other stakeholders, and to receive feedback on how each project aligns with the Roadmap goals and potential ways to improve the relevance of project results. The workshop was intended to provide participating energy sector owners and operators with a better understanding of the relevance of each project to the Roadmap and how it can help them better secure their control systems.

Energy Sector Control Systems Working Group

In December 2007, leaders from the electric, and oil and natural gas industries, and government formed the Energy Sector Control Systems Working Group to help guide implementation of Roadmap priorities. The Working Group members are:

DAVE BATZ, Alliant Energy

STUART BRINDLEY, IESO Ontario

PAGE CLARK, El Paso Corp.

STEVE ELWART, Ergon Refining Inc.

ERIC FLETCHER, NiSource

TOM FLOWERS, CenterPoint Energy Inc.

ED GOFF, Progress Energy

MORGAN HENRIE, Alyeska Pipeline

HANK KENCHINGTON, DOE

DOUG MAUGHAN, DHS S&T

SEÁN MCGURK, DHS NCSD

DAVE NORTON, Entergy Corp.

DAVE SCHEULEN, BP

AW: What are among the key elements in the strategy for achieving the 10-year goal?

Kenchington: To achieve the Roadmap vision, a framework based on sound risk management principles emphasizes four strategic areas:

- Measure and Assess Security Posture. Within 10 years, the sector will help ensure that energy asset owners have the ability and commitment to perform fully-automated security state monitoring of their control system networks with real-time remediation.
- Develop and Integrate Protective Measures. Within 10 years, next-generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.
- Detect Intrusion and Implement Response Strategies. Within 10 years, the energy sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.
- Sustain Security Improvements. Over the next 10 years, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.

The existence of the Roadmap will not by itself create action. Strong leadership and commitment is needed at each step to ensure that important requirements do not fall through the cracks. Collaboration from both industry and government is essential to achieving success.

To help guide implementation of the Roadmap, industry leaders formed the Energy Sector Control Systems Working Group. The working group, which ratified its charter in December 2007, is made up of representatives from the Government Coordinating Council for Energy, the Electric Sector Coordinating Council, and the Oil & Natural Gas Sector Coordinating Council. It operates under the framework of the Critical Infrastructure Partnership Advisory Council, a group formed under the National Infrastructure Protection Plan to support the private sector and government in collaborating on critical infrastructure protection activities.

Working group members have outlined **four objectives** for their efforts:

1. Help identify and implement practical, near-term activities that are high priority for the industry
2. Promote the value to the industry of achieving the goals of the Roadmap
3. Recommend critical areas for public and private investment
4. Measure progress toward Roadmap goals and milestones.

AW: What would you say are among the biggest challenges in achieving that 10-year vision?

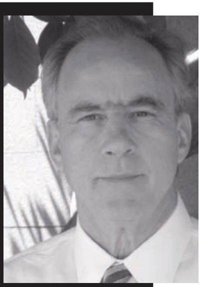
Kenchington: Some of the biggest challenges to achieving the vision include:

- Keeping pace with the rapidly changing and growing threat environment. New cyber vulnerabilities are discovered on a weekly basis. Sophisticated software tools, widely available on the Internet and sometimes traded for profit by cyber extortionists, allow hostile actors to develop and launch new cyber attacks faster than ever (even with limited control system knowledge). The result is a vicious cycle in which there is a constant need for new countermeasures that require increasingly faster implementation.
- Accelerating the commercialization of inherently secure and resilient control systems. As these systems become more integrated into enterprise and corporate-wide systems, it is essential to transform the state-of-the-art for control systems technology from an inherently insecure technology that requires layers of defense and costly management processes to provide adequate security to a technology that provides built-in security and robustness.
- Increasing understanding of cyber risks. While our understanding of the risk of cyber attacks on the energy infrastructure has been improved through Roadmap-related research, energy asset owners and operators still do not have the capabilities to fully understand the risk associated with the cyber threats of today and tomorrow. Without a better understanding of the risks, costs, and potential consequence, it will continue to be difficult to make a strong business case for cyber security investments.

AW: How has the response to the Roadmap been from asset owners, and from vendors?

Kenchington: So far, we've received very positive feedback on the Roadmap from the energy sector. For example, the NERC Critical Infrastructure Protection (CIP) Committee voted unanimously to approve and support the implementation of the Roadmap. In addi-

PROFILE



Hank Kenchington is a senior manager with the Department of Energy's Office of Electricity Delivery and Energy Reliability (OE). Kenchington currently manages OE's National SCADA Test Bed program designed to help reduce the risk of energy disruptions (oil, gas, and electricity) due to cyber attacks on control systems. Prior to joining DOE, Kenchington directed a strategic business unit for a major manufacturer of industrial equipment and automated control systems with responsibility for systems engineering, sales and marketing, and new product development. He holds a Bachelor of Science degree in mechanical and nuclear engineering from Virginia Polytechnic Institute and State University and a master's degree in engineering management from the George Washington University.

tion, in 2007, the Government Accountability Office (GAO) interviewed industry experts in developing their report "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain." The experts stated that the "roadmap was a positive step for the industry" and that the roadmap process "succeeded in identifying industry needs and was a catalyst for bringing agencies and government coordinating councils together and that it was a good idea for other industries to develop plans similar to the roadmap."

Asset owners and vendors have embraced the Roadmap and are actively pursuing solutions to achieve its goals. In December 2007, leaders from the electric, oil and natural gas industries, and government formed the Energy Sector Control Systems Working Group to help guide implementation of Roadmap priorities. The working group planned to conduct the first ieRoadmap Workshop in May and based on pre-workshop response, strong participation by asset owners, vendors, and researchers was expected.

Roadmap recognition has also come from outside the energy sector. In a January 16, 2007 report, President Bush's National Infrastructure Advisory Council (NIAC) recognized the Roadmap's success in developing and implementing cyber security solutions for control systems. The report recommended that all critical infrastructures use the energy sector Roadmap as a model to develop their own sector-specific roadmaps.

Also in 2007, the Council on Competitiveness, in its report "Transform. Enterprise Resilience: The Resilient Economy: Integrating Competitiveness and Security," stated that each control system that has been assessed by NSTB "represents a class of more secure SCADA technology, creating a powerful multiplier effect on energy resilience nationwide."

AW: Can you provide some examples of projects or initiatives underway in support of the Roadmap?

Kenchington: DOE has aligned the NSTB program to support the goals identified in the Roadmap. Recently, DOE also awarded five industry projects that are developing and integrating technologically advanced controls and cyber-security devices into our electric grid and energy infrastructure. These projects include:

1. Hallmark Project. This project will commercialize the Secure SCADA Communications Protocol (SSCP). - Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, CenterPoint Energy

2. Detection and Analysis of Threats to the Energy Sector (DATES). The team will develop an intrusion detection system (IDS) (network, host, and device level), event correlation framework, and a sector-wide, distributed, privacy-preserving repository of security events for participants to automatically contribute without attribution. - SRI International, ArcSight, Sandia National Laboratories, ERCOT

3. Cyber Audit and Attack Detection Toolkit. The team will extend the capability of existing vulnerability scanning tools to evaluate SCADA security configurations (supports compliance with NERC CIP-005 and CIP-007); develop templates for a security event monitoring system by mining data in PI Systems. - Digital Bond, Tenable Network Security, OSIsoft, Constellation Energy, PacifiCorp, TVA

4. Lemnos Interoperable Security Program. The project will conduct testing, validation, and outreach to increase the availability of cost-effective, interoperable security solutions for IP-based communications. - EnerNex Corp., Schweitzer Engineering Laboratories, TVA, Sandia National Laboratories

5. Protecting Intelligent Distributed Power Grids Against Cyber Attacks. The team is developing a risk-based critical asset identification system and an integrated and distributed security system with optimization to establish the best topology for networking the security components - Siemens Corporate Research, Idaho National Laboratory, Rutgers Center for Advanced Energy Systems

For a more complete listing and description of additional public- and private-sector projects addressing Roadmap challenges and goals, visit http://www.pcsforum.org/roadmap.

AW: How are these initiatives being funded?

Kenchington: Many organizations are funding projects to support the Roadmap. For example, DOE is funding NSTB and cost-sharing five industry projects mentioned above. DOE, DHS, and the National Science Foundation (NSF) are funding the Trustworthy Cyber Infrastructure for the Power Grid initiative led by the University of Illinois – Urbana-Champaign. DHS has developed the Control System Cyber Security Self-Assessment Tool (CS2SAT), which helps utilities determine their compliance with standards through a questionnaire. DHS is also funding the Institute for Information Infrastructure Protection (I3P) projects. The Electric Power Research Institute (EPRI) is funding a project titled "Security Metrics for Energy Management Systems." Other organizations funding research include Cisco Systems, Digital Bond, TNS, Inc., Mu Security, Raytheon, the DOD Technical Support Working Group (TSWG), Wurldtech Security Technologies, and more.

AW: What role do the NERC CIP standards play as part of the plan laid out in the Roadmap?

Kenchington: The Roadmap provides a strategic framework to guide the development of projects and align activities with a common vision. Industry standards (including the NERC CIP standards) are critical to achieving the Roadmap vision. Standards can ensure that ongoing control systems security practices are conducted consistently across an organization, as well as the entire sector. Standards also help owners and operators determine the degree to which security integration is occurring and measure progress. For example, the Roadmap identified standards for secure data exchange and communications as a priority need to help sustain security improvements.

AW: What role does the National SCADA Test Bed play in achieving the Roadmap goals?

Kenchington: The need for a national test bed has been identified in several documents, including the "National Strategy to Secure Cyberspace," and most recently in President Bush's Council of Advisors on Science and Technology report "Leadership Under Challenge: Information Technology R&D in a Competitive World" (August 2007). The Roadmap also identifies this need.

The NSTB provides a singular, state-of-the-art national resource to support industry and government efforts to secure control systems in the energy sector. NSTB researchers have developed considerable expertise in conducting cyber security assessments of controls systems in the test bed and in actual field installations. NSTB has developed specialized modeling and simulation capabilities to more comprehensively understand the risk associated with cyber attacks on our energy infrastructure. NSTB has aided the development of advanced security technologies primed for commercialization, such as the Secure SCADA Communications Protocol (SSCP), which marks SCADA messages with a unique identifier that must be authenticated before the function is carried out, ensuring message integrity. The NSTB also conducts operator training in control systems security, as well as outreach activities to help raise awareness of cyber vulnerabilities and risks among energy executives and operators.

AW: How does the NSTB process work, and how many vendors have had their products tested at NSTB?

Kenchington: The NSTB program involves several activities, including cyber security assessments of control systems in a controlled environment—the test bed. Vendors are providing control systems and security technologies for assessment in the test beds, and owners are providing access to their control systems for on-site assessments and validation of test bed results. Interested vendors work with DOE through a Cooperative Research and Development Agreement (CRADA). Vendors provide approximately 50 percent in cost-sharing to perform the tests. The vendor and DOE develop a test plan with specific targets of evaluation and goals for the assessment. Researchers then install the system in the test bed and assess it using the most up-to-date security exploits and provide a report to the vendor identifying the identified vulnerabilities along with recommendations to mitigate the vulnerability. Fifteen system assessments have been completed so far, and another four are underway. NSTB has conducted system vulnerability assessments in partnership with vendors including ABB, Areva, GE, OSI, Siemens, Telvent, PacifiCorp, and Teltone.

Vendor and asset owner interest in NSTB assessments continues to grow. Twelve utilities from the U.S. and Australia have formed a consortium with ABB, a SCADA system vendor, to privately fund advanced research and testing through the NSTB. The newly formed consortium will fund testing of the latest assessment targets for ABB's SCADA/EMS product, NMR3, and ensure that all previously discovered vulnerabilities have been mitigated. The assessment will be completed this year. Utilities making up the consortium include: Austin Energy, Detroit Edison, Indianapolis Power & Light Company, ITC Transmission, Kansas City Power & Light (KCP&L), LCRA, the New York Independent System Operator (NYISO), Snowy Hydro Ltd., and Tri-State G&T Association.

The NSTB program has also been recognized by other organizations. In December of 2007, the SANS Institute released a report highlighting the NSTB as one of six federal projects that have had the most success in increasing the nation's capacity to secure cyberspace. The report noted that the test bed has "already substantially and measurably improved the security of systems that control much of the nation's most critical infrastructures."

AW: To what degree, to your knowledge, have controls system and SCADA vendors taken steps to "harden" their products, based on NSTB test results?

Kenchington: Fifteen control system vulnerability assessments have been completed to date, and another four are currently in process. Vendors have shared details of the assessments with their users, and some have shared the assessment reports directly. Vendors have also rapidly acted to create system fixes and alert operators of security threats, and six vendors have developed next-generation hardened systems. One vendor who is working with NSTB to improve system security has now sold its improved systems to 21 customers who collectively control more than 235,000 MW of electrical power—about 5.8 percent of net U.S. generation in 2005. Another vendor reported that 82 of its utility customers have downloaded its vendor-specific security patch developed using mitigations recommended by NSTB. The remaining vendors have implemented or are in the process of implementing the recommended mitigations on their systems.

Where can interested parties find out more about the Roadmap and other topics discussed in this interview?

Hank Kenchington
Program Manager, National SCADA Test Bed
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
1000 Independence Ave., SW
Washington, DC 20585
202-586-1878
henry.kenchington@hq.doe.gov