ieROADMAP NEWS

CONTROL SYSTEMS SECURITY ACROSS THE ENERGY SECTOR

Summer 2010

INSIDE

Meet the ESCSWG

Dave Batz, Edison Electric Institute
Jim Brenton, ERCOT
David Dunn, IESO Ontario
Page Clark, El Paso Corporation
Steve Elwart, Ergon Refining Inc.
Eric Fletcher, NiSource
Tom Flowers, Control Center Solutions
Ed Goff, Progress Energy
Carol Hawk, DOE OE
Morgan Henrie, Alyeska Pipeline
Hank Kenchington, DOE
Doug Maughan, DHS S&T
Seán McGurk, DHS NCSD
Dave Norton, Entergy Corporation
Dave Scheulen, BP

Made up of control systems experts from the public and private sector, the Energy Sector Control Systems Working Group (ESCSWG) formed to guide the energy sector in implementing the industry-led *Roadmap to Secure Control Systems in the Energy Sector.* It aims to increase public-private collaboration, help identify high-priority security activities, promote the value of the Roadmap, and accelerate progress toward achieving the Roadmap goals.

ENERGY SECTOR CONTROL SYSTEMS WORKING GROUP

From Challenges to Champions

This issue puts the magnifying glass to the hard parts of implementing the *Roadmap to Secure Control Systems in the Energy Sector*. We've taken some of the persistent challenges the sector faces—including information sharing, true public-private coordination, and leveraging tight time and resources—and asked our contributors to share how they made real progress to improve the cybersecurity of the energy sector in the face of these challenges. None of these are minor accomplishments or easy wins; they are significant steps made possible by dedicated, determined leaders that we call Roadmap champions.

Make Your Voice Heard

This issue features unique voices and perspectives from across the sector — vendors, asset owners, and government representatives. Next issue, we want to hear from you. Have an article idea or a topic you'd like to write about? Send your ideas to the Energy Sector Control Systems Working Group at ieRoadmapNews@energetics.com.

The Public-Private Partnership Delivers: Solutions You Can Use Today

By: Hank Kenchington

Deputy Assistant Secretary for R&D
U.S. Department of Energy Office of Electricity Delivery and Energy Reliability

Following the effort to develop the first *Roadmap to Secure Control Systems in the Energy Sector* in 2006, the Department of Energy worked with stakeholders to take on cybersecurity efforts in support of the Roadmap's vision. DOE's newly re-named Cybersecurity for Energy Delivery Systems (CEDS) program continues to work directly with this community to support Roadmap-aligned R&D through the National SCADA Test Bed (NSTB) and other partnerships with industry and academia.

One thing we learned early on from our industry partners was that useful, relevant technologies and capabilities cannot be developed in isolation. Projects that move promising ideas into implemented solutions require the expertise and resources of researchers, the experience and knowledge of vendors and integrators, and the input and perspective of end users.

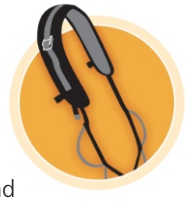
We've been employing this model in our projects to produce tangible results. The following select technologies and capabilities are available now to energy sector stakeholders, and they exemplify how public-private partnership efforts can deliver solutions to some of the sector's most challenging problems.

- **Security Profiles for the Smart Grid:** DOE is working with leading energy utilities to develop a baseline set of security controls for smart grid applications, which utilities and vendors can use to improve the security of smart grid applications and implementations. Security profiles have been completed for securing the advanced metering infrastructure (AMI) and for securing third-party data access. A third security profile for securing distribution automation systems is currently in progress. The AMI security profile was incorporated into the draft NIST document, *Smart Grid Cyber Security Strategy and Requirements*.
- **Hardened Control Systems and Informed Risk Management:** 12 more secure, hardened SCADA and energy management system designs are now in the marketplace—with 49 currently deployed—due to the NSTB's on-site and test bed cyber vulnerability assessments of the

majority of SCADA and EMS systems in the marketplace. Vendor partnerships make it possible, and vendors increasingly share assessment results with users, who have in turn contributed funding for additional testing. You can use the vulnerability knowledge researchers have amassed to optimize your control system configuration by downloading the Idaho National Laboratory's *Common Vulnerabilities Report*, which includes anonymous vulnerability information and mitigation techniques.

- **Secure Serial Communications Using the Secure SCADA Communications Protocol (SSCP):** Energy sector asset owners can safeguard serial SCADA communications between remote devices and the control center using the SSCP, which enables receiving devices to identify and authenticate the engineer requesting access. In a DOE co-funded effort, Schweitzer Engineering Laboratories (SEL) incorporated the SSCP (originally developed by Pacific Northwest National Laboratory) into the soon-to-be-released SEL-3025 Link Module and SEL-3045 Cryptographic Card. The products will secure new and legacy system designs and give other vendors flexibility to incorporate the technology into their products.

- **Optimized Security Configurations and Event Detection Capability:** Asset owners can optimize their security configurations using Bandolier Audit Files and use the Portaledge event detection capability to add control systems security monitoring to OSIsoft's PI Server. Developed by Digital Bond through a DOE-supported project, both products leverage widely used tools in the energy sector. Both products are available as Digital Bond subscriber content, and more than 200 organizations are subscribing.



- 

- **Proven Processes to Enable Interoperability Among Control System Devices:** The DOE-supported Lemnos project developed interoperable configuration profiles to guide vendors in developing interoperable security solutions. SEL's Ethernet Security Gateway, the first tool built to those profiles, is now available.
- **Intensive, Hands-On Training for Asset Owners and Operators:** NSTB has trained more than 100 energy sector asset owner personnel in its Advanced Red Team/Blue Team SCADA Security Training, a week-long, intensive course designed to leave participants with security techniques they can immediately use in their facility. Each includes a 12-hour hands-on exercise in which the group either attacks or defends a control system network, building operational experience and skills.

For more information on the CEDS Program, visit http://www.oe.energy.gov/controlsecurity.htm.

Letter from a Working Group Member

Inside these pages, you are hearing from true leaders who have faced real challenges while making impressive enhancements to the security of energy sector control systems. Each of these organizations has something in common: they didn't do it alone. In fact, all of them will tell you that the turning point where they began making progress was when they entered into real partnerships that stretched across the public and private aisles. Looking across these cases, it's clear we're no longer a disparate set of stakeholders, but a cohesive community.

Nowhere is that community better represented than on the interactive energy Roadmap (ieRoadmap), an online tool where you can find information on current R&D projects across the sector, a library of critical publications, and the latest news and updates from the Roadmap community.

While many of you may know the ieRoadmap well, I'd like to share some of the unique aspects that make this such a useful tool for the energy sector:

- **Upload a project.** Learn about more than 60 projects now under way by more than 20 organizations, and submit information about your project to share with fellow researchers and potential end users.
- **See who is involved.** Visit the Contributors page to read about the organizations who have mapped their cybersecurity efforts to the Roadmap. See the Links page for more information on other active organizations in control systems security.
- **Browse a one-stop-shop of resources.** The Documents page contains a comprehensive list of best practices, technical reports, articles, and guidance documents.
- **Get news and updates**. Visit the News page, follow the ieRoadmap on Twitter, and check out the event calendar to find relevant conferences and workshops.
- **Highlight your participation.** Download a linkable graphic from the Link to Us page to promote your leadership in the Roadmap effort on your own website.

Remember, the ieRoadmap is your tool. Do you have a Roadmap effort to share? Know of a conference, publication, or news not listed? If there's something you think should be on the ieRoadmap e-mail ieRoadmapNews@energetics.com to get it posted.

SIncerely,

David Batz, CISSP
Edison Electric Institute

EnergySec Breaks the Info Sharing Mold

By Seth Bromberger
Treasurer, EnergySec

EnergySec is a forum designed to facilitate information sharing, communication, and coordination among energy sector asset owners, government agencies, and product vendors for the purpose of strengthening the security of critical infrastructures in the energy sector. Specifically, it aims to provide its members with:

- Near real-time security intelligence analysis and dissemination
- Industry and government outreach and education for security issues
- Experienced guidance on topics of security and regulatory compliance

EnergySec began as an informal organization of security professionals within the electric industry interested in discussing common security practices, challenges, and principles relevant to the protection of their company's assets and the power grid at large. The group was originally known as Energy Security Northwest (E-Sec NW), reflecting its original membership's origins in the northwestern United States. Since its inception in 2004, participation has grown to include representation from organizations located in nearly all regions of North America.

EnergySec's primary participants are electric industry asset owners. As of June 2010, participation in EnergySec consists of more than 300 individual industry professionals representing more than 95 organizations including energy companies, government, academia, and national laboratories. We expect membership to grow to 600 professionals from 200 companies by January 2012. Our current membership represents more than 46% of U.S. electric generation capacity, and almost 60% of U.S. electric distribution. Membership remains free for NERC-registered asset owners and government agencies, and there are sponsorship programs in place for other interested parties.

Why have we been successful?

Quite simply, our model works because of the trust that we have been able to build within the membership, through open and honest communication and frank discussion of real-world security issues. As an example, not too long ago McAfee had a well-publicized issue with a virus definition file update that wound up affecting critical systems in multiple industries. Because of the trust and openness within the EnergySec community, members were alerted to this via our portal well in advance of news postings, prior to McAfee's official disclosure, and hours before any notification was released by US-CERT. The members who were alerted were able to avoid any service interruption as a result of applying the faulty update.

Here's an example of more strategic collaboration: one of our members recently developed a framework for information security within the utility sector that represents a best-in-class approach to defining and organizing the capabilities necessary to provide infosec services in critical infrastructure. Rather than keeping this knowledge to himself, he decided to share it with his colleagues on the EnergySec portal. The resulting feedback and interaction have provided benefits to everyone involved. This is the essence of what we're trying to accomplish.

There's a lot of talk about information sharing within government and the industry, but this is often referring to executive-level or classified government information. EnergySec seeks to provide actionable information directly from and to staff-level individuals. This is information sharing that has real, immediate, and positive impact on the security of our critical energy infrastructure because it puts information in the hands of the "boots on the ground" staff who can directly and rapidly apply it to their day-to-day work.

For more information, visit www.energysec.org.

The Energy Sector Security Consortium (EnergySec) is a registered 501(c)(3) non-profit corporation focused on information sharing and awareness as they relate to security issues in the energy sector. EnergySec's current board of directors and advisory teams consist of industry professionals in the areas of information security, physical security, engineering, plant operations, disaster recovery, telecommunications, and other related disciplines.

ABB Brings Customers Value Through Partnership

By Phil Beekman
ABB

ABB has been involved in cybersecurity for control systems for more than a decade; in that time it has identified cybersecurity as a key requirement and committed to providing customers with products, systems, and services that clearly address cybersecurity.

As part of this commitment, ABB was the first vendor to provide an EMS system to the Department of Energy's National SCADA Test Bed (NSTB) at the Idaho National Laboratory (INL) in 2004. Since that time, ABB has participated in several additional NSTB cybersecurity assessments as an individual vendor, in combination with an individual customer utility, and with a consortium of utility customers.

Cybersecurity for control systems is a complex and challenging issue. ABB strongly believes that partnerships and collaboration between all involved stakeholders (including vendors, end users, security solution providers, government organizations, research institutes, etc.) is absolutely essential to effectively and efficiently advance cybersecurity for critical infrastructure.

One large challenge we faced has been to have all levels of our company and the end users' organizations see the need to move forward to improve control system security. We faced contrary ideas in our efforts that needed to be rethought—ranging from "We are isolated from the bad guys" to "Security costs will make our products less competitive in the market." These old ideas have faded with the adoption of the NERC CIP standards and the realization that the market now demands adequate security in all products and systems.

Why have we been successful?

The greatest benefit to ABB from partnering with customers, the staff of the NSTB, or vendors of security products is the great amount of shared knowledge and expertise that results. Putting these minds together has enabled more comprehensive improvements to be incorporated into products and systems, resulting in more secure and robust offerings for customers.

One of the most rewarding parts of this process is sharing information with our customers about their concerns, and the successes we've realized in securing their systems. Our original concepts broadened considerably after hearing customers' perspectives and experiences. We believe that this information exchange has resulted in strong systems that give a tremendous boost to the security of the energy sector's critical infrastructure.

Engagement Feeds Value Directly to Progress Energy

By Ed Goff
Enterprise Architect - IT&T Security
Progress Energy

With current threat trends and emerging technologies, asset owner collaboration and partnership with our peers, solution providers, government agencies, and compliance groups will become more critical. Our engagement has fed direct value — whether through awareness, best practices, or standards—directly into Progress Energy's cybersecurity efforts. We see this directly affecting our responsibility and commitment to how we maintain reliability and protect our portion of the critical infrastructure.

Asset owners, Progress Energy included, have faced a number of challenges to better engagement. Travel budgets are small. The most valuable participants have limited time. It's difficult to fit schedule constraints of participants for the most important groups, and there is some overlap in the scope of these groups, making it difficult to prioritize. The industry could benefit from a wider adoption of virtual and remote participation options, and a cleared facility for classified briefings.

Why have we been successful?

We have top-level support for collaboration. We've had to make tough choices on what to participate in, but we've employed a divide-and-conquer approach, where we send one subject matter expert that shares valuable information back to our internal stakeholders. We've seen some success with this on a larger scale by leveraging our peers to represent the industry on some groups or standards development activities. This is an approach that needs more attention. Because of our approach, we've realized great value:

1. **We don't waste time and resources reinventing the wheel.** Our engagement with the national labs and other organizations over the past decade has given us threat awareness, relevant standards, and best practices that influence our security solutions and improve our posture.
2. **Participation in interoperability and security standards directly benefits our own projects and reduces the risk of stranded investments.** Our work with the NIST smart grid initiative has been pumping standards and adherence information into our Smart Grid Investment Grant initiatives.
3. **Peer engagement encourages an informal benchmarking**. We learn how our peers are approaching certain aspects of asset protection—a high-value outcome of our participation.
4. **We have built invaluable relationships that are critical to our success.**

Progress Energy's Engagement

- Member of industry advisory team for Pacific Northwest National Laboratory's Secure Data Transfer and Security Visualization Tool projects
- Member of the Energy Sector Control Systems Working Group
- Member of the NIST Smart Grid Cyber Security Working Group
- Voting member of the NIST Smart Grid Interoperability Panel since its inception
- Chair of the Edison Electric Institute Security Committee Cyber Subcommittee—leads monthly member discussion on emerging threats and issues
- Active participation in NERC Critical Infrastructure Protection Committees—information and best practices sharing
- Formed an internal Smart Grid Interoperability Standards Task Force—ensures appropriate engagement with NIST interoperability and cyber standards activities
- Reached out to all of its control system suppliers/partners to collaborate on and support more appropriate cyber security in their offerings; main areas of focus have been access control and logging and monitoring

ATTEND

IEEE Power and Energy Society (PES) General Meeting
Minneapolis, MN
July 25–29
www.ieee.org/conf/pesgm10/

GovEnergy
Dallas, TX
Aug. 15–18
www.govenergy.com

DOE CyberCap Workshop – co-located with GovEnergy
Dallas, TX
Aug. 15–18
www.netl.doe.gov/events/10conferences/cybercap/
Register by Aug. 2

CLICK

New Report: NERC and DOE High-Impact, Low-Frequency Event Risk to the North American Bulk Power System
www.controlsystemsroadmap.net/pdfs/HILF.pdf.

CONTRIBUTE

Submit events, articles, news, and ideas for this quarterly newsletter to ieRoadmapNews@energetics.com.