Homeland Security

June 2011

ICSJWG Quarterly Newsletter

New Government Coordinating Council Sector Co-Chair

Marty Edwards, in his new role as Director of the Control Systems Security Program (CSSP), National Cyber Security Division, DHS, replaced Amit Khosla as the new Government Coordinating Council (GCC) co-chair of the Industrial Control Systems Joint Working Group (ICSJWG). Previously, Mr. Edwards was a Program Manager focused on control systems security work at the Idaho National Laboratory (INL).

Upcoming ICSJWG 2011 Fall Conference!

Come to California this October! The ICSJWG 2011 Fall Conference dates have been finalized as October 24 – 27, 2011. This conference will be held at The Westin Long Beach in Long Beach, California. The ICSJWG 2011 Fall Conference is open to all members interested in learning about cybersecurity issues facing the nation's critical infrastructure control systems. This is an excellent resource for government professionals (federal, state, local, tribal, and international); control system vendors and systems integrators; research, development, and academic professionals; and owners and operators (management, engineering, production, and IT). Conference attendees will be able to discuss the latest initiatives impacting security of industrial control systems and will have the opportunity to interact with colleagues and peers who may be addressing the risks of threats and vulnerabilities to their systems.

There is no cost to attend the conference sessions or any associated meetings and training. Travel, accommodations, meals, beverages, and other incidental expenses are the responsibility of the conference participants and will NOT be covered by ICSJWG or CSSP. Check out the ICSJWG site for conference information and stay tuned for upcoming ICSJWG 2011 Fall Conference announcements and "Call for Abstracts" information! http://www.us-cert.gov/control_systems/icsjwg/

About the ICSJWG

The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC). The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR.

For more information, visit http://www.us-cert.gov/control_systems/icsjwg/

Table of Contents

New Government Coordinating Council Sector Co-Chair 1

Upcoming ICSJWG 2011 Fall Conference! 1

ICSJWG 2011 Spring Conference Information 2

Transportation Cybersecurity Control Systems Roadmap 2

Standards & Metrics Subgroup Co-Chairs Needed 2

ICSJWG Subgroup Status 2

Homeland Security Information Network 4

Advanced Training Events Scheduled for 2011 4

Industrial Control Systems Contributed Content 5

Participation is Key! 11

CSSP Contact Information 12

ICSJWG 2011 Spring Conference Information

The ICSJWG 2011 Spring Conference was a success, thanks to participants and presenters. We appreciate the participation, comments, and insight provided during the subgroup meetings, the presentations, and the training. The contributions of industry and government professionals ensure that our mutual efforts to secure control systems will continue to be successful. The presentations illustrate and enhance the collaborative partnership fostered between federal agencies and departments—as well as between private asset owners and operators of industrial control systems.

Presentations with speaker release forms and the final agenda are posted on the ICSJWG site - http://www.us-cert.gov/control_systems/icsjwg/conference.html and in HSIN https://cs.hsin.gov/C10/C1/ICSJWG/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Spring%202011%20Conference%20Presentations&View=%7b6F252F6A%2d18EB%2d447A%2d96D4%2d106024729AB9%7d.

Transportation Cybersecurity Control Systems Roadmap

DHS CSSP is leading the development of a Transportation Cybersecurity Control Systems Roadmap (Transportation Roadmap). This document will build upon previous critical infrastructure/key resources (CIKR) roadmaps developed to address control systems in the Energy, Water, and Chemical Sectors. It will also utilize key methodology information developed during the creation of the Cross-Sector Roadmap for Cybersecurity Control Systems. The Transportation Roadmap will provide a ten-year outlook framework for all transportation modes (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline) in the form of cybersecurity control systems goals and milestones.

Individuals interested in participating in the Transportation Roadmap Working Group are encouraged to contact Dawn Johnson or John (Jack) Whitsitt, Transportation Roadmap co-chairs, at Dawn.Johnson@dot.gov or John.Whitsitt@dhs.gov.

Standards & Metrics Subgroup Co-Chairs Needed

Have you heard about the new Standards & Metrics subgroup? At the May 2nd, 2011 GCC/SCC meeting, the working group proposed the formation of a Standards & Metrics subgroup that will address how to actualize standards within the control systems space and measure performance with outcome- or process-based metrics. The group needs to find passionate co-chairs to formulate and articulate the group's vision, goals, and objectives. If you are interested in the Standards & Metrics Government Coordinating Council (GCC) or Sector Coordinating Council (SCC) co-chair positions, please contact icsjwg@dhs.gov.

ICSJWG Subgroup Status

Below is an update on the progress of the ICSJWG subgroups. If you would like to become a member of any of the subgroups, send an email with your contact information to icsjwg@dhs.gov or contact the co-chairs directly.

- **Roadmap to Secure Industrial Control Systems Subgroup**
  GCC Co-Chair: Perry Pederson (Perry.Pederson@nrc.gov)
  SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)

  The Roadmap subgroup completed the initial Cross-Sector Roadmap document. As they move into the next phase of the approval process, the subgroup invited the co-chairs of the other ICSJWG subgroups to provide their input and feedback. Co-chairs have been asked to send their questions and any feedback on the document to icsjwg@dhs.gov.

- **Vendor Subgroup**
  GCC Co-Chair: Marty Edwards (Marty.Edwards@dhs.gov)
  SCC Co-Chair: Eric Cosman (ECCosman@dow.com)

  Marty Edwards, the new Director of CSSP, replaced Amit Khosla as the new Vendor GCC co-chair. The Vendor subgroup continues to refine its purpose/scope, membership composition, and goals. At the ICSJWG 2011 Spring Conference, members explored a variety of topics and future work products related to vulnerability disclosure, incident response, and information sharing.

- **Workforce Development Subgroup**
  GCC Co-Chair: Keri Nusbaum (Keri.Nusbaum@dhs.gov)
  SCC Co-Chair: Michael Glover (M.Glover@prime-controls.com)

  The Workforce Development subgroup has two new co-chairs: Keri Nusbaum (GCC – DHS) and Mike Glover (SCC – Prime Controls). They introduced themselves at the ICSJWG 2011 Spring Conference and have already conducted another subgroup meeting that focused on charter updates and related tasks.

- **Research & Development Subgroup**
  GCC Co-Chair: Dr. Douglas Maughan (Douglas.Maughan@dhs.gov)
  SCC Co-Chair: VACANT

  The R&D Subgroup is on hold due to the resignation of the SCC co-chair. If anyone is interested in applying for the position, please send an email to icsjwg@dhs.gov. We are looking for subject matter experts who have the time and resources to dedicate to the position.

- **Standards & Metrics Subgroup**
  Temporary GCC Co-Chair: Lisa Kaiser (Lisa.Kaiser@dhs.gov)
  Temporary SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)

  The recently created Standards & Metrics subgroup is looking for permanent co-chairs. The acting co-chairs are working to develop a draft charter. All who want to help guide this sub-group to success from its inception may apply by sending an email to icsjwg@dhs.gov.

- **International Subgroup**
  GCC Co-Chair: Seán McGurk (cssp@dhs.gov)
  SCC Co-Chair: Graham Speake (graham.speake@us.yokogawa.com)

  The International subgroup will continue to serve as a registration point for industrial control systems professionals and will be informed of activities taking place in the ICSJWG community. While no actual meetings are currently planned, International members will be notified of all ICSJWG news and are welcome to attend ICSJWG events.

Homeland Security Information Network

HSIN is the information sharing tool used by ICSJWG subgroup members. Subgroup members can keep abreast of upcoming meetings through the calendars and subgroup reference materials in HSIN (e.g., charters, meeting minutes, agendas, etc.).

In addition, the "Alert Me" feature notifies users of changes to the portal, which eliminates the need for users to constantly log in to find out if updates have been made. Alerts can be sent immediately, daily, or weekly. To sign up for alerts, click on the "Alert Me" link on the left-hand side of the ICSJWG homepage and choose your delivery option. ICSJWG subgroup members who still need access to HSIN can send an email to icsjwg@dhs.gov to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations.

At this time, DHS is not able to grant International subgroup members access to the HSIN portal. The owners of the HSIN portal are reviewing sharing agreements concerning information posted to the site. Until that process is complete, International subgroup user accounts will be on hold. ICSJWG Communications will contact all International subgroup members immediately if there are new developments.

Advanced Training Events Scheduled for 2011

CSSP is currently offering advanced cybersecurity training sessions at the Control Systems Analysis Center located in Idaho Falls, Idaho. These sessions provide intensive hands-on training in protecting and securing control systems from cyber attacks, including a realistic Red Team/Blue Team exercise that is conducted within an actual control systems environment. It also provides an opportunity for attendees to network and collaborate with other colleagues involved in operating and protecting control systems networks.

- **Day 1:** Welcome, overview of DHS CSSP, a brief review of cybersecurity for industrial control systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.

- **Day 2:** Hands-on classroom training on Network Discovery, instruction for using Metasploit, and separation into Red and Blue Teams.

- **Day 3:** Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.

- **Day 4:** A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations to a batch-mixing plant and an electrical distribution Supervisory Control and Data Acquisition (SCADA) system.

- **Day 5:** Red Team/Blue Team lessons learned and roundtable discussion.

The following advanced training events have been scheduled for 2011:

- **June 20-24:** Industry Partners
- **July 18-22:** Industry Partners
- **September 12-16:** International Partners
- **October 10-14:** Industry Partners
- **November 7-11:** Reserved
- **December 5-9:** Industry Partners

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant.

Additional offerings are being planned and will be announced once dates are finalized. As scheduled advanced training gets closer, an invitation along with a link to register for the course will be sent out and posted to the following website - http://www.us-cert.gov/control_systems/cscalendar.html. Please check back periodically, as this schedule is occasionally updated.

Register by clicking on the link provided on our webpage - http://www.us-cert.gov/control_systems/cscalendar.html. Registration is open approximately 2 months before the start of a class. Due to high demand, class size is limited to approximately 35 people with a maximum of 2 individuals per company per event. Classes fill quickly, so early registration is encouraged. Notification of cancellation is appreciated, with as much advance notice as possible so that others who wish to take the course can do so.

Industrial Control Systems Contributed Content

ICSJWG is now accepting contributions from the community pertaining to control systems security for the September quarterly newsletter. If you want to submit an article for the September newsletter, please email icsjwg@dhs.gov, and we will take your submission into consideration for publication. The deadline for submissions for the September newsletter is **August 26, 2011**.

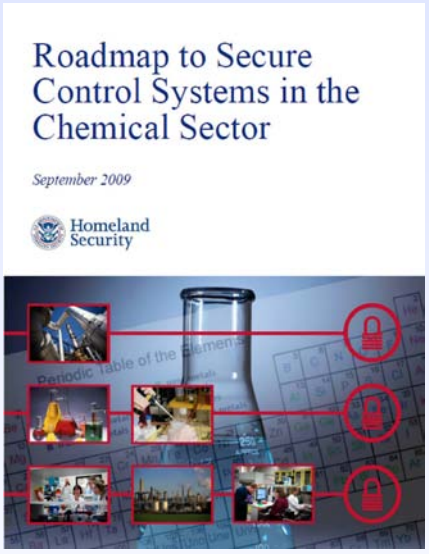
Past ICSJWG newsletters are located on the CSSP website http://www.us-cert.gov/control_systems/icsjwg/index.html and in HSIN https://cs.hsin.gov/C10/C1/ICSJWG/default.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters&View=%7b7F0225B9%2d1943%2d4074%2dB349%2d32C32A4EB8E7%7d.

Also, thank you to all members who contributed content for the June quarterly newsletter! The following content was submitted by members of the ICSJWG for publication and distribution to the ICSJWG community. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations. The advice and instructions provided in the contributed content should be confirmed and tested prior to implementation.

Chemical Sector Makes a Case for Security Industrial Control Systems

By Esther Langer, submitted for the Chemical Sector

In 2009, the chemical industry partnered with DHS to publish the *Roadmap to Secure Control Systems in the Chemical Sector* (Roadmap). This document provides a vision, supporting goals, and objectives for improving the cybersecurity posture of Industrial Control Systems (ICS) within the sector.



With a central emphasis on achieving objectives through public-private partnerships, the Roadmap calls for a comprehensive plan for improving the availability, security, reliability, and functionality of ICS by identifying key milestones over the next decade.

The Chemical Sector-Specific Agency partnered with chemical industry owners and operators, the Chemical Sector Coordinating Council, and the National Cyber Security Division to form the Roadmap Implementation Working Group to address the milestones described in the document.

The proactive coordination of this effort proved to be timely. The emergence of Stuxnet, the first malware created specifically to target ICS, signaled a paradigm shift for the process control and automation industries. No longer are legacy control system environments isolated or invulnerable to information technology-specific threats. News of this malware's impacts on ICS proved helpful in making the case for securing ICS in the Chemical Sector.

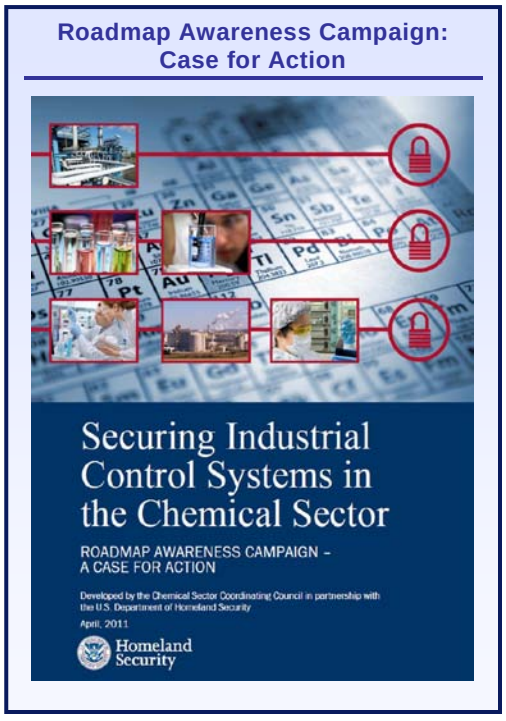
Launching the Roadmap Awareness Campaign

The working group identified milestone 1.1 of the Roadmap as the essential first step for implementation. This milestone specifically calls for the partnership to:

"Establish an industry-driven awareness effort to communicate information relating to the cybersecurity threats, vulnerabilities, and risks and the availability of accepted practices, tools, and training materials to the Chemical Sector."

The working group collected extensive training and reference information to assist owners and operators in addressing ICS security. Roadmap awareness materials include the following:

- **Case for Action** – The campaign's central document demonstrates the importance of taking action with the materials provided.



- **ICS Security Training Resource** – This guide lists available training resources for professionals who work in areas relevant to the process control and automation industries.

- **Standards and Guidelines** – This guide is designed to facilitate research on existing standards in the area of control systems security.

- **Incident Response and Reporting** – This document describes the proper procedures for a chemical company to report a cyber incident to ICS-CERT and how this can positively impact the Chemical Sector.

- **ICS Procurement Language** – This document provides example language that companies can incorporate into ICS procurement specifications.

Additional references and tools available to sector partners and stakeholders are the Cyber Security Evaluation Tool (CSET); the ICS-CERT *2010 Year in Review* and Incident Handling brochure; and a newly developed, scalable, cyber tabletop exercise that is available at no cost and includes scenarios for both business systems and ICS.

Milestones related to metrics and secure information sharing are the next steps in the Roadmap implementation process.

Reaching Out to the ICS Community

The working group identified owner and operator, vendor, and government conferences as important venues to deliver presentations and distribute awareness DVDs about the sector's work in this area. Owners and operators can obtain the awareness package free of charge by emailing chemicalsector@dhs.gov. It is also available for download on the Homeland Security Information Network–Critical Sectors (HSIN-CS) Chemical Portal.

The Four Layers of Smart Grid Security

By Ernie Hayden, CISSP CEH
(Note: This blog was also featured on Asian Power Magazine and Ernie Hayden's blog spots: Energy Central and Think Forward.)

Globally one of the energy topics atop many electric utility executive's minds is what we are all calling the "Smart Grid." Of course what constitutes the Smart Grid can mean many different things from new digital meters on someone's house to advanced Flexible AC Transmission Systems (FACTS) to new sensors on transmission lines and substations. Regardless of the exact deployment for an electric utility, a key consideration—something on my agenda every day—is the security of the Smart Grid deployment.

What exactly does "security" mean? What does it include? That's what I'd like to explain.

First of all, a very simple axiom for security is the "CIA" model. That is, security means that we need to protect the equipment and information so that the necessary **Confidentiality**, **Integrity**, and **Availability** of the system in question are maintained. For instance, you can hide that information from view through encryption thus maintaining its confidentiality. Integrity means that the information cannot be changed without one realizing it was modified. And of course the term availability means that the system, information, or equipment is there and usable when it is needed.

So, for the Smart Grid we need to keep the CIA in mind. However, what are the next things we need to worry about?

This brings me to the Four Layers of Smart Grid Security.

Security of the Smart Grid can be defined and segmented into four layers of concern that require the electric utility's attention. These layers include:

- Physical protection
- Cyber security and defense
- Privacy protection
- Data management and storage

Physical Protection

First and foremost, you need to protect your smart grid assets from theft, vandalism, and modification by miscreants. You also need to protect your assets from the weather, earthquakes, floods, and cyclones. You take these actions to reduce equipment replacement costs and to protect against someone breaking into your smart meters or sensors and loading a cyber worm or virus that can attack your system.

An interesting thought experiment about this concern was demonstrated by a Seattle information security company called IOActive at the Black Hat Conference in Las Vegas in 2009. At this conference, IOActive showed how they had disassembled a smart meter, learned how it worked from a cyber perspective, and then imagined what would happen if a smart meter in a Seattle neighborhood had a cyber malware/worm installed. IOActive showed that their work could result in 15,000 meters being infected and dysfunctional in a matter of 24 hours. This exercise was examined by many cyber experts and the consensus was that such an attack is very viable.

Hence, this is a good reason to figure out ways to protect your smart meters and sensors and keep the attacker from gaining physical access to the inside of the meter.

Cyber Protection

Because the smart meters, smart sensors, and advanced communications devices are essentially all computers and microprocessors, they can all be subject to cyber attacks ranging from denial of service and "man-in-the-middle" injects to reading (stealing) and/or changing the data in transit.

Just think of the implications of any of these attacks. Essentially, these attacks can seriously impact your "CIA" management and could result in angry customers and failures in your smart grid system.

For your cyber protection, you need to consider such techniques as encrypting and/or "tunneling" the data in transit to keep someone from reading/stealing the information. Also, you may want to consider such techniques as "hashing" the data so that you can immediately identify if your data has been changed while in transit.

For more ideas on considerations for data protection, please check the 2010 Verizon Data Breach Protection Report.

Privacy Protection

In many places of the world, privacy of personal information is truly an operational imperative. For instance, in the European Union (EU) and Canada the privacy dialogue is at the forefront. Privacy of smart grid data is becoming an important issue in the EU and Canada but also is becoming a key point of review in California and Ohio in the U.S.

Why is this even being discussed?

Smart grid data—especially from smart meters at individual homes and apartments—contains information that could be used to actually determine the lifestyle of the individuals living in the metered house. There have been studies done to show that smart meter data taken every 15 minutes could reveal such information as when a person rises in the morning and retires at night. When they turn on the oven or stove and when they use their washer and dryer. In fact, you could also determine if someone is home, which a potential burglar would find very interesting.

Because of this data, electric utility executives need to realize that this data needs to be protected. Unauthorized release of this "personal data" could be considered a "data breach" subject to litigation and possible law suits. Hence, the privacy of this data is one more layer to be addressed.

Data Management and Storage

As the smart grid concept evolves, one new surprise for many utility executives is all the data that will be generated by the smart meters and intelligent devices. For instance, Austin Energy in the United States state of Texas is one of the pioneers in the smart grid domain. For instance, with Austin Energy moving their meter data collection from monthly to hourly, readings will increase their data handling by over 730 times. Austin Energy also notes that with their Phase 1 Roll Out of 500,000 meters would result in their yearly data storage requirements increasing from 20 TerraBytes (TB) to 200 TB inclusive of disaster recovery redundancy.

This massive change in the data management and storage requirements for utilities is considerable. Utility executives will need to put their arms around this issue before data is lost, damaged, or stolen.

By the way, 200 TB is nothing when you look at other utilities reporting that they may have over 100 PetaBytes of data accumulated over 10 years.

Conclusion

The smart grid concepts and deployments are very exciting for electric utilities around the world. The new systems and sensors should result in new efficiencies and new services for the customers; however, there are consequences to be considered. As such, the security requirements need to be built into your smart grid designs before deployment and do not forget to at least consider the four layers of security listed above.

About the Author

Ernie is currently a Managing Principal for Verizon Business with extensive experience in the power utility industry, critical infrastructure protection/information security, and cybercrime and cyberwarfare. His primary focus is on supporting customer projects regarding smart grid security, energy supply security, and electric grid security with special emphasis on North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. He travels extensively and speaks at many security and energy conferences.

Ernie is a featured speaker at many industry-leading conferences around the globe and presented this topic at the ICSJWG 2011 Spring Conference this past May in Dallas, Texas. Feel free to contact him at ernest.hayden@verizonbusiness.com to arrange a meeting or speaking opportunity.

The VIKING Project – A Holistic Approach to SCADA System Security

By Mathias Ekstedt and Gunnar Björkman

The VIKING project was started to investigate the increased cyber security risks for deliberate attacks on critical infrastructures coming from SCADA systems and to propose mitigation. The project is partly financed by EU under the Framework 7 Programme. VIKING stands for Vital Infrastructure, NetworKs, INformation and Control Systems ManaGement and has the main objective to make SCADA system more resilient against cyber attacks.

Society is increasingly dependent on the proper functioning of the electric power system, which in turn supports most other critical infrastructures. Power outages might lead to situations of fully nonfunctioning societies with devastating economical and humanitarian consequences. The operation and management of the electric power grid depends on computerized industrial control systems, SCADA systems. Keeping these systems secure and resilient to external attacks is thus vital for uninterrupted service.

The VIKING project takes a holistic approach and investigates the risks for cyber attacks on all parts of the SCADA system including substation control systems, communication networks, and central control systems. The project aims to model the whole chain from cyber attacks, modeled via attack trees, over architectural SCADA system models, power system models, down to societal models. The societal model is used for calculating the societal cost from power outages by means of a virtual society that can be parameterized to most European countries based on statistics from Eurostat. In addition to the theoretical model studies, the VIKING project implements a Test bed. The Test bed includes an actual SCADA system with physical devices like PLCs and RTUs as well as simulators of the power grid and the society. The research has already shown that intelligent cyber attacks can fool the control system operators to make wrong decisions which could cause non-optimal operational or even physical damage to the grid.

The VIKING project was initiated as a result of discussions about control system security between the academic world and industry. The consortium is composed of a balanced mix between academics and industrial partners. This balance ensures that project results are applicable in industrial-scale applications. Partners include:

- ABB, a world leading SCADA/EMS vendor
- E.ON, one of the major utilities in Europe
- Astron, a medium size system integrator in Hungary
- Kungliga Tekniska Högskolan (KTH) in Sweden
- Eidgenössiche Technische Hochschule (ETH) in Switzerland
- University of Maryland, United States

The VIKING project will be finished at the end of 2011 and we can now see results which could have substantial, practical importance for the implementation and usage of SCADA systems. Some of these outcomes will be direct results of the VIKING project while others will be spin-offs that could be explored by the academic or industrial partners.

The following list outlines some of the ideas which have been investigated within the project:

- The security architecture model could be used to evaluate individual SCADA systems for their persistence to cyber attacks. Such an analysis would be performed in a dedicated tool. The tool would, as an end result, give an aggregated probabilistic value of the cyber security of the analyzed system architecture as well as propose enhancements.
- The grid can be formally analyzed to find which process values are most sensitive to external manipulation. It has been shown in the project that such manipulation of a limited number of process values can be used to deceive the power system application without being detected. In a corresponding, way the same information can be used to decide where to optimally apply secure communication measures on a limited part of the communication network to make such attacks impossible or much more difficult.
- Since one of the goals of the VIKING project is to bring proposed mitigation closer to the industrial practice, the research results will be tested in a Test bed based on a real-life SCADA system. The Test Bed will mainly be used for demonstrations of potential attacks and their consequences but also for testing and verifying mitigation. The Test bed could be used to train operators to identify cyber attacks and to increase the awareness of these types of threats.

More information about the VIKING project can be found on www.vikingproject.eu.

Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of the ICSJWG in coordinating cybersecurity efforts to secure industrial control systems across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

CSSP Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/.

In addition, the ICS-CERT Monthly Monitors are published on HSIN as appendices to the ICSJWG newsletter.

Other important contact information:
Website Address: http://www.us-cert.gov/control_systems/
ICS-CERT Email: ics-cert@dhs.gov
Phone: 1-877-776-7585
CSSP Email: cssp@dhs.gov