March 2018

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- April 10-12: ICSJWG 2018 Spring Meeting
  Albuquerque Marriott
  Albuquerque, NM
- April 16–20; April 30–May 4; May 14–18: Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, Idaho
  Registration for these respective trainings is *closed*
- June 4–8; June 25–29: Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, Idaho
  Registration for the June 4 training is *closed*.
  Registration for the June 25 training is *open*.

ICS-CERT Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Latest Monitor

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, linguistic styles, or recommendations.

2018 Spring Meeting—Reminder, Updated Details

As a reminder, the 2018 Spring Industrial Control Systems Joint Working Group (ICSJWG) Meeting will occur April 10–12, 2018, in Albuquerque, New Mexico! The ICSJWG Steering Team (IST) has reviewed all received abstracts and we look forward to a great agenda for this meeting. Registration for the meeting is now open on our website or at: https://secure.inl.gov/ics-cert-briefing/?campaignName=ICSJWG%20Spring%202018.

Detailed information for the Spring Meeting is on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. This includes a link to the official Meeting announcement, our Frequently Asked Questions documents, the agenda, and the meeting and accommodations registrations.

If you have any questions about the upcoming 2018 Spring Meeting, or generally about anything ICSJWG-related, please feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

New Processes, Procedures for ICSJWG Webinars

Based on the continually high demand from interested presenters and interested attendees for ICSJWG Webinars, the ICSJWG team will be implementing new processes and procedures concerning these periodical sessions. These changes, made with input from the ICSWJG Steering Team, are intended to structure and streamline Webinar abstract reception, review, and disposition. We plan to announce this framework by the end of April.

Generally, if you are interested in attending any ICSJWG Webinar, please email us at ICSJWG.Communications@hq.dhs.gov. The next Webinar is tentatively planned for April 2018. We will inform membership of any changes to this timeframe.

Contributed Content Disclaimer: *The advice and instructions provided in the contributed content are specified as is with no warranties and should be confirmed and tested prior to implementation.*

Endpoint Cybersecurity: Mission-Critical Concerns and Solutions

By: Deborah Lee James, 23rd Secretary, U.S. Air Force; Special Advisor, Ultra Electronics, 3eTI

Military field command and control has outgrown analog and the short-wave radio. Today, its home is the cloud with an increasing dependence on public and private internet platforms. America's modern military base, like most civilian industrial facilities, is an intricately interconnected complex that often is a model of efficiency. Within its vast ecosystem blending internet-based networks and industrial control systems (ICS), new mobile and other technologies improve time and cost savings through functions that can now be automated and executed remotely.

For article, click here.

Quantitative Risk Models (QRM) – Enhancing ICS Cybersecurity Risk Assessment

By: Dr. Dona Stewart, Director of Advanced Data Analytics, D-Tech, LCC; and
Dr. Nick Duan, President & CTO, D-Tech, LLC

The cybersecurity risk assessment methodologies practiced today are qualitative in nature and inadequate to address the evolving cybersecurity threats enterprises face in a control system environment. They are primarily designed to support enterprise compliance during system operations and are not part of an enterprise wide integrated risk management process. A quantitative cybersecurity risk model (QRM) solution is urgently needed to help identify, select, and integrate cybersecurity risk functions, to include vulnerability, threat and consequence.

Full article, click here.

Coordinated Approach to Industrial Cyber Security and Functional Safety Systems

By: Daniel Ehrenreich, Consultant and Lecturer, ICS Cyber Security, SCCE

Cyber-attacks on utility infrastructure and manufacturing facilities, have made the challenge of protecting these critical operations a top priority. While the famous slogan for IT security is "Confidentiality-Integrity-Availability (CIA)", for the assurance of cyber resiliency of Industrial Control Systems (ICS) we shall firmly say the parallel slogan "Safety-Reliability-Productivity (SRP)". In order to achieve the SRP goals, ICS experts shall follow specific best practices and guidelines as outlined in both the IEC 62443 and NIST 800-82 referring to ICS cyber security and the International Safety Standards IEC 61508 which refers to the safety instrumented system (SIS). Consequently, we shall deploy cyber defense solutions, which properly and cost-effectively addresses both requirements. This paper will review the link among SIS and the ICS considerations for critical infrastructure protection (CIP).

For full article, click here.

Strong Security Simplifies Compliance for French Operators of Vital Industry

By: Courtney Schneider, Industrial Security Policy Manager, Waterfall Security Solutions

In 2014, France's National Agency for the Security of Information Systems, or ANSSI, issued two detailed cybersecurity guidance documents for Industrial Control Systems:

Cybersecurity for Industrial Control Systems – Classification Method and Key Measures
Cybersecurity for Industrial Control Systems – Detailed Measures

This guidance was and is still today seen as the most comprehensive, clear, and sophisticated industrial control system (ICS) security best practice in the world. In 2016 and 2017, on the tails of this important guidance, have come eleven sets of cybersecurity regulations for critical infrastructure – issued by the French Government's military programming law (LPM) – to protect the Nation's Operators of Vital Importance (OIVs) for various industrial sectors. Other regulations were also issued to cover traditional IT and communications sectors such as Finance and Communications.

To keep reading, click here.

What Every Control System Vendor Should Know About Cybersecurity

By: Michael Chipley, PhD GICSP PMP LEED AP, The PMC Group LLC

This is a two-part article, the first addressing cybersecurity of Operational Technologies (OT) Control Systems which includes the field components and devices, controllers, servers, workstations, mobile and HMI; and the second addressing the Control System Vendor corporate business Information Technology (IT) systems that store and transmit Controlled Unclassified Information (CUI), which typically includes the CAD, BIM, technical specifications and operating manuals about the OT system.

To continue reading, click here for Part 1. | To continue reading, click here for Part 2.