CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

December 2022

UPCOMING EVENTS

Save the Date!

ICSJWG 2023 Spring Meeting
May 9–11, Salt Lake City, Utah
More information coming soon!

Trainings:

Quarterly ChemLock Trainings
January 11 & April 12
Course Information -- Jan Registration -- Apr Registration

Industrial Control Systems Evaluation (401v) Online Virtual Training
December 5–23
Course information -- Registration

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
December 5–23
Course information -- Registration

Industrial Control Systems Cybersecurity (401L) In-Person Training
January 9–27
Course information -- Registration

Industrial Control Systems Evaluation (301v) Online Virtual Training
January 9–27
Course information -- Registration

Industrial Control Systems Evaluation (401v) Online Virtual Training
February 6–24
Course information -- Registration

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
February 6–24
Course information -- Registration

Additional ICS Training
CISA Virtual Learning Portal

The ICSJWG 2022 Fall Meeting Was a Success!

On September 13–14, the Industrial Control Systems Joint Working Group (ICSJWG) hosted its sixth virtual meeting. A total of fourteen presentations were given, with over 500 live attendees and more than 600 on-demand views representing all 16 critical infrastructure sectors. A keynote by the Executive Director of CISA Brandon Wales on *Uniting Cyber Defense* kicked off the meeting on September 13. The meeting also featured a CYBER-CHAMP® presentation, *Cyber-Competency Health and Maturity Progression Mode,l* which was hosted by Dr. Shane D. Stailey from Idaho National Laboratory; technical workshops including *Prototype Hardware-in-the-Loop, Supply Chain Concerns and Mitigations*, and *Holistic Hunting: Leveraging Network and Host Logs to find Bad Actors;* and original and valuable presentations from critical infrastructure experts from the community. A Capture the Flag Activity ran September 10–14, with over 40 teams working to solve challenges in a simulated environment.

For more information, or to view on-demand videos of presentations from the Fall Meeting, click here.

Save the Date for the ICSJWG 2023 Spring Meeting!

The ICSJWG is thrilled to return in person for our Spring Meeting in Salt Lake City, Utah on May 9–11, 2023. We welcome all Industrial Control Systems (ICS) community members from around the globe, including those new to the ICS community. A Call for Abstracts will be available in the new year for those interested in presenting. We look forward to seeing you in person this spring to continue building our partnership and sharing ideas that make our country safer. Stay tuned for updates on registration and accommodations!

Public-Private Collaboration to Enhance Operational Technology Cyber Defense

The ICSJWG hosted its last 2022 quarterly webinar on November 16, featuring Annie Fixler from the Foundation for Defense of Democracies (FDD) and Samuel Chanoski from Idaho National Laboratory (INL). The presentation, *Public-Private Collaboration to Enhance Operational Technology Cyber Defense*, provided an overview of a program created by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response to enhance bi-directional conversations and strengthen relationships between and among cyber experts in the U.S. government and Operational Technology (OT) operational and security managers across the energy sector. The session focused on lessons learned that can be applied across all critical infrastructure sectors and sector risk management agencies to enhance cyber defense.

Join Our Steering Team!

The ICSJWG Steering Team (IST) is looking to fill a role with a subject matter expert in the Food/Agriculture sector. The objective of the IST is to enhance and grow collaboration efforts of the ICSJWG and provide guidance on programming efforts. The IST is comprised of a diverse group of representatives from the ICS community, and we are actively searching for our next member! If you or a colleague is interested in learning more about this opportunity, please contact us at ICSJWGCommunications@cisa.dhs.gov.

Cybersecurity Defense Education and Training

In the world of Industrial Control Systems (ICS), understanding cybersecurity is critical. To help Industrial Control Operators learn about Information Technology (IT), Operational Technology (OT), and the strategies used to protect these networks, CISA offered its 200th session of the Industrial Control Systems Cybersecurity 301 Lab. This hands-on ICS course delivered beyond standard lectures and lessons. Hosted by the Idaho National Laboratory, the four-day course offered training for understanding, protecting, and securing ICS from cyber-attacks. This in-person experience provided exercises for students sharing examples of the dangers that come from the manipulation of IT and OT systems. The class mimicked hacking into a traffic light system, altering the ladder logic, and turning all lights green at an intersection, highlighting the chaos that can occur from an OT system breach. Students also participated in escape rooms. Four theme-based escape rooms were used, incorporating teamwork among participants of different skill levels. Each room contained IT and OT components drawing on skills taught in the labs, which included problem solving, offense/defense tactics (Red Team/Blue Team), and non-technical logic puzzle components.

Continue to full article…

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.

Measuring Stakeholder Alignment to Overcome Control System Vulnerability

By: Aleksandra Scalco and Steve Simske

Cyber introduces new capabilities to control systems.However, professionals' uncertainty and lack of agreement about the cyber domain create system vulnerability. Such disagreement leads to misalignment, which leads to vulnerability. Why is this important? Reports of significant cyber incidents targeting infrastructure over the past year are increasing globally. Advanced persistent threat attacks on critical infrastructure sectors, such as on a power grid or water treatment facility, can result in severe consequences. Thus, there is a tremendous effort to design the next generation of capabilities to reduce incidents and inform entities about known security issues, vulnerabilities, and exploits in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems (CISA, 2022). In response, the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) releases cybersecurity advisories and provides sector-specific cybersecurity framework guidance to help inform stakeholders about vulnerabilities and how to remediate them.

Continue to full article…

Where Does Cybersecurity End for Electric Utilities?

By: Danielle Jablanski

Across the energy sector and between various electric sector locations, there are several assets and systems deemed “crown jewel assets” or “mission-critical systems.”. Depending on who you ask, nearly every digital component they rely on is potentially at risk in some way. This painstaking reality has led to a focus on securing critical assets—the machines, equipment, and systems providing critical resources and services—and critical functions—actions, activities, or operations to connect, distribute, manage, and supply essential resources, products, or services. In the energy sector, cybersecurity assessments routinely reveal hundreds of insecure protocols and device vulnerabilities, as well as dozens of insecure password protections. In a case study of an electric utility with over 600 global sites serving millions of customers, focusing on the four outlined weaknesses improved the overall reliability, efficiency, and maturity of the operators’ cybersecurity program. The operations required in-depth support for specific IEC protocols, and centralized and automated monitoring of hydroelectric, thermoelectric, and wind generation plants. The collaboration of people, tools, and processes allow for notification of root cause analysis of accidental, misconfiguration, and potentially malicious cyber events around the clock. This helps eliminate time-consuming manual OT/ICS and IoT mapping, troubleshooting, and vulnerability correlation efforts.

Continue to full article…

A Picture is Worth 1000 Words in DoD Facility-Related Control Systems Cybersecurity Design

By: Susan Howard

A key item missing from the current UFC 4-010-06 and the UFGS Division 25 specifications is the requirement for a cybersecurity network drawing. For those of us providing and reviewing design submittals for our clients in the DoD such as Navy Facilities Engineering Command (NAVFAC), Air Force Civil Engineering Center (AFCEC), and United States Army Corps of Engineers (USACE), the result of this key omission results in numerous Requests for

Information (RFIs) and delays by contractors during installation of FRCS like fire systems, building automation systems, advanced meter infrastructure, supervisory control and data acquisition (SCADA), and many others. System integrators and engineers use drawings as their primary source of information during installation and commissioning. Without a drawing, it is very challenging to decipher the requirements noted in UFGS Division 25 specifications and understand the complex interconnectivity of multiple FRCS. A key reason for this practice is primarily a security concern, as many of these drawings contain sensitive infrastructure data that cannot be openly shared.

Continue to full article…

Building an Industrial Cybersecurity Workforce for the Future

By: Idaho National Laboratory

Idaho National Laboratory (INL) has facilitated an Industrial Cybersecurity Community of Practice (ICSCOP) since 2020 that has grown to include over 250 registered members from more than 100 companies, universities, and national labs in over 25 countries. The objective of the community is to bring together professionals focused on industrial cybersecurity education, training, and workforce development efforts throughout government, academia, and industry. The group leverages INL's existing industrial control systems cybersecurity experience, research, and training to:

- Integrate stakeholders and practitioners with similar interest in a consolidated framework.
- Develop common views on career pathways in operational technology cybersecurity.
- Map foundational pedagogical paradigms to educate and train our workforce.

The ICSCOP is comprised of subgroups, quarterly meetings, and biannual workshops. Meetings for each of these tracks are held periodically and feature presentations and vibrant discussions on leading topics.

Continue to full article…

The Anomaly Detection Systems Defense Weaponry for Internal Cyber Threats in Industrial Control Systems

By: Thibaud Ecarot, Djeff Kanda Nkashama, Marc Frappier, and Pierre-Martin Tardif

Sensitive industries and services have been facing growing numbers of ever evolving cyberattacks over the years, and healthcare is one of the most targeted industries. In late 2020, healthcare companies lost US $6 trillion to safety breaches, while unauthorized access led up to 34% of data leaks. Like any other sensitive industry, the healthcare sector had to handle a heterogenous infrastructure with several different networks (cloud computing, IoT), connected unique devices, and multiple sensors actuators to various hardware components. The attackers are often hacktivists, cybercriminals, or state-backed rogue groups. The commonalities between these attacks, the attacking groups, and the targeted industries are characterized by an increasingly complex attack surface and several too-porous physical/cyber environments.

Continue to full article…