INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

December 2020

Upcoming Events

ICSJWG Webinar Series

"Bow Tie Model of Destructive Malware – ICS Historian Case Study"

Wednesday, January 27, 2021
1:00PM-2:15PM (EST)

Industrial Control Systems Cybersecurity Training provided by INL in Idaho Falls, Idaho

Training Calendar at INL

January 11 – 22 (401v)*
January 18 – 29 (301v)
February 1 – 12 (301v)
February 8 – 19 (401v)*
February 15 – 26 (301v)

**401 Training – must have completed 301 to attend this session.*

CISA Resources

COVID-19
CISA Service Catalog
CISA ICS Security Offerings
Training Resources
Incident Reporting
Assessments
CSET®
Alerts
Advisories
HSIN
Information Products

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.

ICSJWG Steering Team (IST) Volunteers Wanted!

As part of our ongoing improvement efforts, we are expanding the membership of the ICSJWG Steering Team (IST). The team of volunteer ICSJWG members is intended to be representative of all sectors and roles within the industrial control systems (ICS) and critical infrastructure (CI) community. The IST is chartered to augment the ICSWJG leadership with suggestions about the multitude of items needed for the ICSJWG to continue its focus on the mission of information sharing in this space. ICSJWG relies on the networking and subject matter expertise of the IST membership to provide timely, relevant, and substantial inputs into meeting formats, topics, and speakers of interest, as well as any ICSJWG activities leading to best practices, documented methodology, and future actions.

The IST Representative openings include: Asset Owners & Operators (1), Vendors & Suppliers (1), Consultants-Integrators (1), Industry Association & NGO (2), International Stakeholders (1), SLTT Representatives (2), and University, Academia, and Research (2). Typical time and involvement include quarterly meetings of 1-hour duration and review of abstracts submitted for the biannual meetings (approximately 1-hour review for each meeting).

If you are interested in volunteering your time and expertise to the IST, please provide your name, professional title, company, IST position you are interested in, and a brief biography relevant to ICS and CI for the current IST to consider. Send your information to ICSJWG.Communications@cisa.dhs.gov. We will compile the various candidate's information for IST discussion during the next IST meeting. The IST will decide on a status and will schedule additional interviews.

We look forward to your input and will consider all applications.

The ICSJWG 2021 Spring Virtual Meeting—Save the Date!

The ICSJWG is currently planning the next bi-annual meeting, again in a virtual format. We expect to launch the event in April 2021. We will provide updates as they occur, but for now, SAVE THE DATE for the ICSJWG Spring 2021 Virtual Meeting!

ICSJWG Webinar

Bow Tie Model of Destructive Malware—ICS Historian Case Study
Presented by Daniel Michaud-Soucy (Dragos) & Lubos Mlcoch (OSISoft)

This presentation explores the concept of utilizing the Bow Tie model to help asset owners improve their Industrial Control System's (ICS) reliability and resiliency. The model helps identify relevant threats, defenses against those threats, impacts, and methods to reduce those associated impacts from creating an adverse event related to the inherent hazard of operating an ICS environment. In particular, the focus is on a destructive malware type event affecting a process data historian server. Speakers will present their methodology and analysis highlights (including tie-ins to the MITRE ATT&CK

framework). Key takeaways are focused on leveraging this model to visually represent the controls asset owners can implement to assess and manage risk levels for their environment. Further, ransomware campaigns are a genuine risk for ICS asset owners. This case-study can immediately provide insights into what actionable items are available to reduce the likelihood of such an event or mitigate the impact should an event occur.

This ICSJWG webinar will be provided Wednesday, January 27, 2021; 1:00 PM – 2:15 PM (EST). To participate in this webinar, please use this link or respond to ICSJWG.Communications@cisa.dhs.gov with a work-related email including your name, company's name, role (vendor, owner-operator, etc.), State or Country from which you will be calling, and sector affiliation no later than Tuesday, January 26, 2021.

Program Update: Control Environment Laboratory Resource (CELR)

CELR Overview

The Cybersecurity and Infrastructure Security Agency (CISA) continues to develop The Control Environment Laboratory Resource (CELR). CELR is an environment for government and private industry partners to experience the possible effects of kinetic cyber physical attacks. CELR allows users to perform security research on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. CELR is a test range that uses multiple platforms capable of hosting simulated risk scenarios against real critical infrastructure (CI) processes. CELR enables the study of complete cyber warfare against our Nation's CI which are often targeted by our cyber adversaries. CELR is highly adaptable, simulates numerous corporate network configurations, and provides control system hardware and kinetic outputs of various CI sectors. With the ability to host multiple concurrent simulations, analysts across the Nation can interact with the environment while being both on and offsite through extended range connections.

CELR Program Update

As the CELR program continues to mature, CISA is excited to provide updates to the ICSJWG community on the progress being made in our development efforts. Exciting work is being done on new skids that will facilitate CISA's ability to collaborate with CI and manufacturing partners on automotive cybersecurity. The development of an automotive skid is underway! Although still in the technical requirements and design phases, it is anticipated that this skid will feature a full-sized vehicle for the purpose of demonstrations and simulations of cyber-attacks, which would result in visible physical effects.

The goal of the automotive skid is to create a realistic and true-scale environment where the interconnectivity of the CANbus components and the vehicle's Electronic Control Units (ECUs) can be tested from a cybersecurity perspective. While not all inclusive, the ECUs which have been discussed as possibilities for cyber-kinetic effects as part of the initial technical requirements gathering process include:

- Adaptive cruise control
- Braking system
- Accelerator pedal
- Door control unit
- Sunroof control unit
- Side satellites
- Sensor cluster
- Airbag control unit

These requirements would facilitate the ability of the CELR automotive skid to test and evaluate many different attack scenarios as it relates to automotive cybersecurity and its interconnected systems and subsystems. The current design plan indicates that these scenarios should be plausible from either a direct hardwire connection to the vehicle, or through various wireless protocols that may be present (Wi-Fi, Bluetooth, etc.). The proposed scenarios include, but are not limited to:

- Starting and stopping the engine
- Opening the doors or trunk
- Locking or unlocking the doors
- Opening and closing the windows
- Activating braking system or manipulating proximity sensor data
- Manipulating rate of speed
- Manipulating speed during adaptive cruise control
- Altering or deleting data on the vehicle's display unit(s)

The Automotive skid within CISA's CELR environment is in the early phases of technical requirements gathering and design. However, CISA recognizes the importance of making tangible and meaningful contributions to the field of automotive cybersecurity. The interconnectedness of vehicles and the ability to interact with other control system environments (charging stations, traffic control, etc.) will continue to increase in the next 3-5 years. The industry will also likely begin to see an increase in fully autonomous vehicles which will create an increase in risk for cyber-kinetic impacts to occur in these systems. The development of the automotive skid will ultimately allow CELR users to train in incident response scenarios, perform vulnerability discovery, and provide risk mitigation and prevention guidance as they apply to automotive systems.

Increasing the cybersecurity posture in CI is a whole of community approach that requires participation from government and private industry alike. If you are working in the automotive industry and have suggestions, or want to collaborate on ideas, CISA would love to hear from you! Please contact Casey Kahsen (casey.kahsen@cisa.dhs.gov) or Drew Batten (drew.batten@hq.dhs.gov) if you have questions or comments.

CISA ICS Offerings and Capabilities Fact Sheet

Industrial Control Systems (ICS) are important to supporting US critical infrastructure (CI) and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.

To support the ICS community's cyber risk management efforts, CISA offers ICS owners and operators a wide range of products, services, and capabilities. Please visit the CISA ICS Security Offerings page to learn more.

CISA Services Catalog

The CISA Services Catalog is all of CISA, all in one place. The Catalog is a single resource that provides users with access to information on services across all CISA's mission areas that are available to Federal Government; State, Local, Tribal and Territorial Government; Private Industry; Academia; NGO and Non-Profit; and General Public stakeholders.

The Catalog is interactive, allowing users to filter and quickly home in on applicable services with just a few clicks.

This Catalog is intended for electronic viewing on desktop devices only. For the most seamless experience, users should download and save a copy of the Catalog to their computer, then view it in full-screen mode with a PDF viewer. For questions about the services featured in the CISA Services Catalog, or for questions about the Catalog itself, please email Central@cisa.gov.

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*

Authenticity and Integrity

By: Salvatore Bellassai, FoxGuard Solutions

Unless you write your own code for everything, and build your own hardware from scratch, authenticity and integrity are essential concepts in cyber security. Simply put, authenticity is the act of ensuring the end product you've received, came from the intended source. Integrity ensures that no part of that product has been changed since leaving the manufacturer.

Continue to full "Authenticity" article...

Cyber Secured Power Utility Operations

By: Daniel Ehrenreich, Secure Communication and Control Experts

Power utilities use Industrial Control System (ICS) to manage their operations including the six typical zones: Generation, High Voltage (HV) Transmission System operation (TSO), Medium Voltage (MV) Distribution System operation (DSO), MV Distributed Generation, Low Voltage (LV) power delivery and LV Distributed Generation. Each of these zones include mechanical assets, computers and communications, some which perform local control within their zone and others, which communicate with other zones. This power grid structure is in line with deployment of the smart grid, distributed generation and of Industrial Internet of Things (IIoT). All these effective solutions enhance the control capability, but they also increase the cyber-attack surface.

Continue to full "Cyber Secured Power" article...

Data Privacy Considerations during Requirements Phase of IOT Product Development

By: Harsha Banavara, Signify North America Corporation

This paper addresses the continuing issues of comprehensive consideration and integration of data privacy into product and solution development to enable compliance to applicable standards, rules and regulations. The data privacy landscape is in continuous flux with more countries and regional entities placing increased importance and rigor upon the handling of specific categories of people data: personally identifiable information (PII) or personal data, protected health information (PHI), and sensitive information (SI). A process is offered which promotes early consideration of what kinds of data need to be collected, processed, and stored; determination of the implications based upon intended geographic locations of sales or services; and concluding with generation of comprehensive security requirements.

Continue to full "Data Privacy" article...

Model Driven Deception for Defense of Operational Technology Environments

By: Thomas W. Edgar, William Hofer, and Marc Feghali, Pacific Northwest National Laboratory and Attivo Networks

There is an ever-increasing number of cyber-attacks targeted at cyber-physical systems vital to the operation of our critical infrastructure. Everything from disruption (Lee, Assante, and Conway 2016), destruction (Cyber.nj.gov 2017), data loss (Greenberg 2018), or general rampant internet threats (Honeywell 2018) have become a risk to cyber-physical systems that were once thought isolated and secure from cyber threats. As with the advent and proliferation of Internet in the 90s, deploying cyber defenses is critical to robust and resilient operation.

Continue to full "Model Driven Deception" article...

Dragos Manufacturing Threat Perspective

By: Dragos

Cyber risk to the manufacturing sector is increasing, led by disruptive cyberattacks impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from Industrial Control Systems (ICS)-targeting adversaries. Dragos currently publicly tracks five ICS-focused activity groups targeting manufacturing: CHRYSENE, PARISITE, MAGNALLIUM, WASSONITE, and XENOTIME in addition to various ransomware activities capable of disrupting operations.

Continue to full "Dragos" article...

The Need to Change the Paradigm of Control System Cyber Security

By: Joe Weiss, Applied Control Solutions

There have been many articles, webinars, and even books written on cyber security of control systems. I put them into three bins. The first bin includes those presentations and papers that apply to "keeping lights on and water lowing". The second bin includes those presentations and papers that apply to Operational Technology (OT) networks but do not include "keeping lights on and water flowing". This is generally where the IT/OT convergence discussions lie. The third bin are those presentations and papers that are factually not correct or not applicable to control systems. Unfortunately, there are very few articles and discussions that fit into the first bin. Most fit into the second bin. This article addresses what is needed to address the first bin.

Continue to full "Change the Paradigm" article...

Building a More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic

By: Cybersecurity and Infrastructure Security Agency (CISA)

The impacts of the COVID-19 pandemic on the Information Technology and Communication (ICT) sector's supply chains are still unfolding. To understand how IT companies have been impacted, and to identify lessons learned about supply chain vulnerabilities and the potential ways to address them going forward, the Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, a partnership between the IT and Communications Sector Coordinating Councils and the Cybersecurity & Infrastructure Security Agency (CISA) formed a study group (collectively, "the Study Group"). The goal of the Study Group was to uncover the impacts of COVID-19 on the ICT supply chains and make practical recommendations that can support policy and operational decisions to strengthen and build additional resilience into ICT supply chains in the future. These recommendations can support policy and operational decisions intended to strengthen supply chains going forward. The study also provides a high-level visual mapping of how goods and services flow through the generalized ICT supply chain, from the raw materials stage through to sale to the consumer.

Continue to full "Resilient ICT" article...

Navigating ICS Security—A Field Guide

By: Gary DiFazio and Gabe Authier of Tripwire, Kristen Poulos and Keith Blodorn of Belden

Nearly every aspect of modern life depends upon the uninterrupted function of industrial control systems (ICS). ICSs keep the lights on, ensure clean drinking water, and provide other critical infrastructure processes. Beyond power, energy, and other utilities, ICSs are also responsible for the manufacturing of your computer, your car, and countless other physical items we rely on every day.

Continue to full "Navigating ICS Security" article...

Embedded Cybersecurity for Industrial Control Systems: Putting Protection Where It Matters Most

By: Brian Romansky, Chief Innovation Officer, Owl Cyber Defense

Operational technology gets smarter and more connected each year. As the amount of data generated and processed within OT networks continues to grow, new opportunities have arisen for threat actors—ranging from individual cybercriminals to nation states—to wreak havoc on critical systems.

Continue to full "Embedded Cybersecurity" article...

Securing the Digital Plant

By: Sam Galpin, Bedrock Automation

Manufacturing and process industry executives have been hearing about the promise of the digital enterprise for more than 30 years and now, and just when it looked like it was about to surge, a problem emerged: making the most of digital connectivity requires standards-based technology, which unfortunately can come with cyber vulnerability.

Continue to full "Securing the Digital Plant" article...

For Industrial Control Systems, 802.1X is the Impossible Dream

By: Katherine Gronberg, Forescout Technologies and Susan Howard, Jacobs

802.1X is a decades-old networking protocol established by the Institute of Electrical and Electronics Engineers (IEEE) that governs how devices join wired and wireless computer networks. In industry parlance, this process is referred to as "network access control," or "NAC." 802.1X works decently well for wireless devices connecting to information technology (IT) systems. When implemented properly, it reliably regulates how devices join these environments in business enterprises. However, it offers little in terms of security and can be tedious and expensive to implement.

Continue to full "802.1X" article...