CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG

QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

June 2023

UPCOMING EVENTS

Register to Attend!

Our next ICSJWG quarterly webinar will be on **June 14 from 1:00–2:15 p.m. ET**. We are looking forward to a presentation provided by Aleksandra Scalco from the Institute of Electrical and Electronics Engineers and Steven Simske from Colorado State University on ***Measuring Stakeholder Alignment to Overcome Control System Vulnerability***.

This webinar will discuss differences in perspective among professionals involved in the cybersecurity operations of organizations due to variances in engineering practice, paradigms, processes, and culture for people in these roles.

Register for the webinar

Upcoming ICS Trainings

Industrial Control Systems Evaluation (401L)
In-Person Training - 3 days
June 27–29

Industrial Control Systems Cybersecurity (301L) In-Person Training - 4 days
July 10–13

Industrial Control Systems (101, 201, & 202) Louisiana In-Person Training - 3 days
July 24–27

See calendar for all offerings

ICSJWG 2023 Spring Meeting Success

The ICSJWG 2023 Spring Meeting returned in person last month, May 9–11, in Salt Lake City, Utah. A total of 246 members from the ICS community gathered to participate in a diverse range of technical presentations, a VR immersive experience with CELR, and CDET provided educational trainings and cyber-theme escape room. CISA's Executive Assistant Director for Cybersecurity, Eric Goldstein, delivered keynote remarks along with remarks by JCDC's Associate Director, Clayton Romans. Attendees raced to complete this year's extremely popular Capture the Flag virtual activity and had the opportunity to network and explore the vendor expo. Thank you to our presenters and those who made it out to Salt Lake City!

Capture the Flag Highlights

1400+ users | 595 teams

Top Scorers: WPICSC ("TheMuffinMob"), CubeMastery, cl4r0ty, RumbleInTheJungle, and Legalize Nuclear Bombs

Main Room Presentation at the ICSJWG 2023 Spring Meeting.

The U.S. government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. government.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG

QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

June 2023

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.

Cyber Security Evaluation Tool (CSET) Survey

Do you have all the support you need to manage your cybersecurity? Do you need to convey your situation to management? If so, the tools provided are there to help you convey the situation to management, address the needs for additional training, and highlight your organizations strengths and weaknesses.

Take this CSET survey that asks about a few CISA resources that could potentially help get you the support you need. If you have any questions about the survey, please reach out to Barry Hansen at Barry.hansen@inl.gov.

Achieving Visibility and Control in OT Systems: Remote Maintenance, Securing Remote Access, and the Zero-Trust Approach

By: Erik Peterson, Cybercore Integration Center, Idaho National Laboratory

As organizations continue to rely on OT systems to streamline operations, they also face significant cybersecurity risks. The increased reliance on remote work in the wake of the COVID-19 pandemic has further highlighted the need for secure remote access to OT systems. With employees accessing these systems from remote locations, the risk of unauthorized access and data breaches has risen significantly. As such, organizations must implement secure remote access protocols that ensure only authorized personnel can access their OT systems and data transmissions remain secure. In this paper, we will explore the challenges associated with securing remote access to OT systems and provide practical solutions to mitigate these risks.

Continue to full article…

Application Driven Certificate Validation Policy Management

By: John Iwasz, AVEVA

Public Key Infrastructure (PKI) is a set of protocols, technologies, and policies that develop a framework for managing digital certificates, public/private key pairs, and digital signatures; such features provide secure communications between IoT devices and applications. Certificates like X.509 secure TLS/SSL channels such as web browser block sites that have expired or have invalid certificates; however, OT operations could cease if a system administrator fails to renew a certificate. With organizations creating internal IT and OT solutions and engaging with vendors to provide possible solutions, commercial IIoT should provide the needed flexibility to ensure credential integrity and status. With a secure-by-default approach that embodies STRICT policies, an administrator will be capable of adjusting environmental challenges, providing consistency across products and operating systems.

Continue to full article…

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG

QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

June 2023

Beyond Vulnerability Discovery: The Importance of a Risk-Based Approach to OT Security

By: Yair Attar, OTORIO

For years, we've been primarily focused on vulnerability discovery. We've been using tools and technologies to identify vulnerabilities in our OT environment, but let's face it, that's just the tip of the iceberg. It's time to move beyond vulnerability discovery and shift towards a risk-based approach.

Continue to full article…

Correctly Analyzing and Understanding ICS-OT Cyber Incidents

By: Daniel Ehrenreich, SCCE

Industrial Control Systems (ICS) Operation Technology (OT) experts often conduct a debate about the actual number of ICS-OT cyber incidents which have occurred worldwide since 2010 (Stuxnet). Among the published attacks are those that impact only the IT operation or may directly or indirectly affect the ICS zone and the industrial process. Most cyber security experts agree that the actual number of incidents are unknown, mainly because many "light" events are not detected, and many detected incidents were not adequately analyzed or reported. This paper aims to help the readers correctly analyze the various ICS-OT directed cyber incidents which might lead to operation outages, damage to machinery, a risk to lives, loss of access to data, damage to data integrity, and more.

Continue to full article…

Inaugural Program Aims to Demonstrate Operating Site Compliance With ISA/IEC 62443

By: Andre Ristaino, ISA

The International Society of Automation (ISA) along with the ISA Security Compliance Institute (ISCI) have announced their intention to create a new conformity assessment scheme for automation systems deployed at operating sites—a critical and long overdue addition to the landscape of operational technology (OT) cybersecurity solutions.

Continue to full article…

Trucks and OT

By: Swedish Civil Contingencies Agency

The control systems of heavy road vehicles exhibit similarities with traditional Operational Technology (OT). Modern trucks are computerized to much the same degree as many other systems in our environment. While traditional OT may rely on ever more advanced programmable logic controllers (PLC), the operation of a modern heavy vehicle similarly relies on up to a hundred or more electronic control units (ECU) that manage the entire functionality of the vehicle, from entertainment systems to the steering, brakes, and engine. The operating systems used for these types of units are usually very simple and designed to be reliable, but often without considering cybersecurity aspects.

Continue to full article…

The U.S. government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. government.