December 2018

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- **ICSJWG Webinar Series**
  January 16, 2019
- **March 11–15, 2019**
  (Tentative) Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho
  Registration for this training will open about 90 days before the scheduled start date
- **April 23–25, 2019**
  ICSJWG 2019 Spring Meeting
  Kansas City, Missouri

NCCIC Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Information Products

NCCIC Service Menus

Federal Government
Private Industry
State-Local-Tribal-Territorial
International Partners

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.

2019 Spring Meeting Save-the-Date

Next year, 2019, will be the 10th anniversary of the ICSJWG as a driving force behind information sharing and stakeholder engagement for the security of our Nation’s critical infrastructure. If you have any ideas to help celebrate this decade of growth, or to recognize those who have participated since the beginning, please let us know.

The ICSJWG team produced the Call for Abstracts on November 20th to allow for more time for the membership to generate ideas and provide abstracts to help celebrate the beginning of the10th anniversary of our biannual meetings. The Call for Abstracts form is available on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

If you have any questions about the upcoming 2019 Spring Meeting, or generally about anything ICSJWG-related, please feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

ICSJWG Webinar Series Update

“In the course of the last twenty-four months there have been unprecedented changes to industrial operations such as yours. With a more heterogeneous community accessing your OT network on more devices and conducting more operations through IIoT enabled devices, the integrity of those operations have never been more complex. Failure to adjust to this new reality can result in visibility, security, and control gaps that can put your organization at risk.”

The next webinar in our series is scheduled for January 16, 2019. Mr. Michael Rothschild, Director of Marketing of Indegy, will be presenting ***“Five Ways to Ensure the Integrity of Your Operations.”***

About the speaker: with a proven track record of 20+ years in security and networking, Mr. Rothschild has a passion for inspiring and motivating world class marketing teams in product and field marketing. Prior to joining Indegy, Michael was the Global Director of Marketing at Thales. Michael occupies a board seat at Rutgers University and has published a variety of works. In his spare time volunteers as an Emergency Medical Technician.

The formal announcement and information about signing up for this webinar will be posted soon to our webpage and sent to the ICSJWG community.

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.*

Differentiating Among M2M and IIoT Ecosystems

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Industry experts know well the term M2M (Machine to Machine), referring to control devices which directly communicate with Industrial Control Systems (ICS). The M2M model may utilize physical, wireless, analog, digital, etc., media and may involve a wide range of smart sensors and instrumentation. The M2M communication enables these field devices to exchange application-oriented data and sending alarms to the ICS computer.

Using a similar approach, the innovators made a step ahead and introduced the Internet of Things (IoT) ecosystem for consumer applications and the Industrial IoT (IIoT) for critical infrastructure, utility operations and manufacturing plants. Among these IoT and IIoT ecosystems you may find smart homes, food stores, machinery, medical instruments, water pumps, power generators, smart city lighting, public transportations and more. For article, click here.