ICS / SCADA Cybersecurity Symposium

https://ics-scada-symposium.com **Organized by:** SGO Smart Grid Observer

Organizations in manufacturing, transportation, energy, water treatment, healthcare and other critical sectors face the increasingly present threat of cyber attacks to their industrial control systems (ICS). Advanced persistent threat (APT) groups have the resources and support to mount attacks that are complex, orchestrated, and ever-more sophisticated. Operators of critical infrastructure face the critical task of continually safeguarding key OT and IT systems from this kind of compromise and damage.

The 2nd Annual **ICS/SCADA Cybersecurity Symposium**, June 16-18, 2026 in Chicago, is focused on providing real-world preparation to critical infrastructure operators for successfully dealing with cybersecurity threats. Emerging enabling technologies and strategies are examined in detail, with the aim of preparing asset owners for the threats that confront their unique type of ICS/SCADA infrastructures.

If your organization is faced with safeguarding critical infrastructure from challenges such as ransomware and nation-state APT actors, this is a must-attend opportunity to network one-on-one with key colleagues, industry thought leaders and solution providers.

Topics to be addressed include:

- The current status of nation-state level APTs
- Defense-in-depth strategies for ICS/SCADA environments
- Meeting and exceeding regulatory requirements
- Protecting ICS networks from ransomware attacks
- Architecting a network security solution to address cyber threats
- Deception technology and other emerging innovations
- Conducting in-depth risk assessments
- Extending protections to cloud-connected OT assets
- Machine learning and AI in next-gen ICS cybersecurity
- Addressing the growing convergence between IT and OT networks
- Cybersecurity for operational technologies and smart systems
- Software-defined perimeters for securing ICS remote access
- Restricting communication paths and limiting potential attack vectors
- Reducing supply chain risks for ICS networks
- The role of network monitoring and centralized security analytics
- Partnerships for public-private collaboration and information sharing
- Case studies and lessons learned: Insights and key takeaways across industry verticals
- And more

Organizations that have participated in SGO's Utility Cybersecurity Forum

Acronis
AlertEnterprise
Arizona Public Service Co. Awesense
Basler Electric Co.
BC Hydro
Black & Veatch
Blockchain Engineering Council (BEC)
Bonneville Power Authority
Burns & McDonnell
Calpine
Citrix
Cleco Corporation
Consolidated Edison
Control Infotech Pvt Ltd
Cordoba Corporation
CPS Energy
CSA Group
CybSecBCML, Inc.
Dispersive Networks
Dominion Energy
Doyon Utilities, LLC
Dragos, Inc.
Duke Energy
DynTek
EDF Renewables
Edison Electric Institute
Element
El Paso Water
EPRI
Exclusive Networks
Exelon Corporation
Finite State
Fortinet
GridBright
Guardtime Energy
Guernsey
Guidehouse Insights
HYAS
Illinois Commerce Commission
IncSys
Indegy
JPEmbedded LLC
JSC Institute of Information Technology
Kent Power
Lea County Electric Cooperative, Inc.
Los Angeles Dept of Water & Power
McAfee
Microsoft
Midcontinent ISO
MITRE Corporation
National Cybersecurity Center of Excellence, NIST NES
Network Perception Nevermore Security Northern Indiana Public Service Co.
Norwegian University of Science and Technology (NTNU)
Nozomi Networks
NRG Energy
OASD HD&GS, Office of the Principal Cyber Advisor
OMICRON Electronics
OPSWAT
Pacific Gas and Electric Co. Pacific Northwest National Laboratory
Pepco Holdings
POWER Engineers
Protect Our Power
Public Service Electric & Gas Company (PSE&G)
Puget Sound Energy
Pyramid Security Advisors
Quadra Applications & Technology Resilience
RSI Security
S&C Electric Company
Sandia National Laboratory
Sargent & Lundy
Schweitzer Engineering Laboratories
Sempra / SDGE / SoCalGas Southern California Edison Southern Company
Synack
Tenable
The CSA Group
The Market Connection Transformer Protector Corp.
Tri-County Electric Coop.
Vectren Energy
West Monroe Partners
West Wing Advisory Services
XONA
XTec Inc.

Job Titles

Regional Sales Manager
Co-Founder
CEO
Global Enablement Engineer Associate
Professor of Energy Engineering
Manager Engineer IV
Senior Cybersecurity Analyst IT Infrastructure Manager
IT Manager
Technical Team Lead
Energy Cybersecurity Research Engineer
Senior Security Architect
Director, Cybersecurity
Principal Product Manager
Executive Assistant
System Operations Manager
Director, IT
Senior Research Analyst Consultant
Substation Automation Engineer
Cybersecurity Architect – IoT
Senior Manager, Cybersecurity
Head of Business Development
Power Utility Communication Chief
Cybersecurity Specialist
Application Engineer
Account Manager
Manager, Cyber Security Ops Manager, Utility of the Future
IT Governance/ Enterprise Architecture
Manager
VP, Technology Services Senior
Research Scientist
President
Manager Communications/IT
Senior Cyber Security Advisor
Senior Engineer
Manager, Real-Time Systems Security Engineering
VP-Power System Solutions
Sr. Director Product Dev
AI/ML Data Scientist
Cyber Defense Analyst Solutions Architect

Preliminary Agenda

Note: Subject to change. If interested in speaking, please contact us.

Day 1 - Tuesday, June 16, 2026

Theme: Foundations & Threat Landscape

9:00 – 9:30 am
Opening Keynote Address
Contextualizing OT security in an era of decentralized infrastructure (growth in number of endpoints, the need to connect via IoT, and the impracticality of air gapping)

Julian Durand, General Manager, Intertrust Secure Systems and CSO, **Intertrust**

9:30 – 10:30 am
Session 1: ICS/SCADA Security Basics – What Makes OT Different?
A primer on industrial control systems, their architecture, and why traditional IT security models don't directly apply.

- Key ICS/SCADA components (PLCs, RTUs, HMIs, historians)
- OT vs. IT priorities and constraints
- Terminology clarity
- Common ICS protocols and legacy design assumptions
- Real-world safety and reliability impacts
- Convergence of OT/IoT Technologies: Security of the Airgap – becoming non-existent

James Harmening, Cybersecurity & Risk Management Director, **Illinois Commerce Commission**
Blake Gilson, Industrial IT Cybersecurity Operations Manager, **ExxonMobil**
Beth Windisch, Deputy Director of Homeland Security, **State of Illinois**
Wei Chen Lin, Cybersecurity Advisor, **U.S. Cybersecurity and Infrastructure Security Agency**

10:30 – 11:00 am Networking Coffee Break

11:00 – 12:30 pm
Session 2: Threat Landscape & Notable ICS Incidents – The Impact of AI
An exploration of past and present attacks on industrial systems and the adversaries behind them.

- Recent OT case studies (ransomware attacks, DOS, etc.)
- New levels of instability in networks of OT systems leading to system-wide collapse
- Nation-state, criminal, and insider threats
- Impact of AI / ML in transforming the threat landscape: A threat tool as well as a robust part of the toolkit in addressing breaches
- Common attack vectors bridging IT and OT
- Use of physics attacks that are not addressed by traditional OT security systems
- Emerging risks in cloud-connected and remote-access-heavy environments

Patrick Miller, CEO, **Ampyx**
Sai Molige, Sr. Manager of Threat Hunting, **Forescout Technologies**
Chris Sistrunk, Technical Leader, OT, **Google Cloud Security**

12:30 – 1:30 pm Lunch

1:30 – 2:45 pm
Session 3: ICS Risk Assessment & Threat Modeling
How to identify, quantify, and prioritize risks in complex industrial control environments.

- Mapping critical assets and "crown jewels"
- OT threat modeling (attack trees, kill chains)
- Leveraging AI
- MITRE attack framework for ICS and ATLAS
- Bringing lessons from IT into OT
- Integrating safety and cyber risk
- Communicating OT risk to executives and operations leaders

Ramesh Reddi, Chief Technology Officer, **CybersecBCML**
M. K. Palmore, CEO & Founder, **Apogee Global RMS**
Liliane Scarpari, Senior Solution Engineer, **Microsoft**

2:45 – 3:15 pm Networking Coffee Break

3:15 – 4:15 pm
Roundtable discussions
Three main challenges, small group discussions of solutions, and reporting back to larger group.

4:15 – 5:15 pm
Session 4: Network Architectures & Segmentation for ICS
Design patterns to limit lateral movement and contain incidents across IT/OT boundaries.

- Zero-trust security for OT (how to administer, enforce, etc.)
- Encryption – resilience in a post-quantum future
- Purdue model relevance and alternatives
- Network zoning and conduits: DMZs, data diodes, jump hosts
- Secure remote access for vendors and maintenance teams: making sure updates are secure via mutually attestable communications
- Balancing segmentation with uptime and reliability
- Continuing forward some discussion from Session 2 and opening keynote

Bruce Tulloch, Chair of Requirements Working Group, **Trusted Energy Interoperability Alliance**, and CDIO Advisor, **JERA Japan**
Jason Bowen, Chief Information Security Officer, **State of Illinois**
David Emmerich, Principal Cyber-Physical Range Architect, **Information Trust Institute, University of Illinois Urbana-Champaign**

5:15 – 6:30 pm Reception

Day 2 - Wednesday, June 17, 2026

Theme: Detection, Response & Resilience

9:00 – 9:15 am
Review of Day 1's key takeaways, overview of Day 2's themes

9:15 – 10:30 am
Session 5: ICS Monitoring, Anomaly Detection & Logging
Techniques to detect malicious or anomalous activity without disrupting sensitive systems.

- CIP 14
- Passive monitoring and traffic capture approaches
- ICS-aware IDS/IPS and protocol-deep inspection
- Logging strategies for constrained OT networks
- Behavioral baselining and anomaly detection

Sai Molige, Sr. Manager of Threat Hunting, **Forescout Technologies**
Vivek Ponnada, Senior Vice President - Growth & Strategy, **Frenos**
Additional panelist TBA

10:30 – 11:00 am Networking Coffee Break

11:00 am – 12:30 pm
Session 6: Incident Response in ICS Environments
Adapting IR to preserve safety and uptime in industrial operations.

- Unique IR challenges in OT
- OT-specific containment strategies
- Coordination with plant operations and engineering
- Evidence collection and post-incident reviews
- Operating in a compromised environment – redundancy and defense-in-depth

Chris Sistrunk, Technical Leader, OT, **Google Cloud Security**
Mary Gannon, Senior OT Incident Response Engineer, **GuidePoint Security**
Representative from Southern Company TBA

12:30 – 1:30 pm Lunch

1:30 – 3:00 pm
Session 7: Secure Engineering, Patch Management & Lifecycle Security
Embedding security into design, procurement, and asset lifecycle management.

- Security-by-design for new and legacy systems
- Cyber-informed engineering (applicable across a number of sessions in this Symposium)
- What is the fail-safe / fail over scenario
- Patch/vulnerability management with limited downtime
- Secure configurations for controllers, HMIs, and historian systems

Benjamin Lampe, Instrumentation & Controls Engineer, **Idaho National Laboratory**
Additional panelists TBA

3:00 – 3:30 pm Networking Coffee Break

3:30 – 5:00 pm
Session 8: Building a Long-Term OT Security Program
Strategic frameworks and governance models for sustained ICS security maturity.

- NIST 800-82, ISA/IEC 62443, NERC CIP
- Governance roles and ownership in OT security
- Training and cultural alignment between IT and OT
- Roadmap planning and maturity measurement

Carter Mauncy, Senior Director - Cybersecurity, **National Rural Electric Cooperative Association (NRECA)**
Tim Gale, Director - Industrial Cybersecurity - Security and Risk Consulting, **1898 & Co.**
Jacob Kitchel, Security Leader - Senior Manager, Operations Technology for Transmission Operations, **Invenergy**
Additional panelist TBA

Day 3 - Thursday, June 18, 2026

Masterclass / Workshop: The Influence of AI and ML Agents on ICS Cybersecurity in the Electric Sector

9:00 - 10:15 am
- The use of agentic actors in complex energy systems
- Integrity of data used to train models

10:45 am - 12:00 pm
- Compromise of agentic actors: Reliably identifying and authenticating actors
- Building independent skills regardless of the data the model is trained on

1:00 - 2:15 pm
- Developing acceptable guiderails for what an agent is allowed to see: Output guiderails for checking what is produced before it is put live
- Best practices as infrastructure becomes more decentralized and millions of end points interoperate with the grid

2:45 - 4:00 pm
- Identifying particular work flows for specific use cases
- Guard rails for agents that operate without human interaction

Matt Luallen, Lead Research Scientist for Education Translation, Information Trust Institute, **University of Illinois**
Ramesh Reddi, Chief Technology Officer, **CybersecBCML**
Liliane Scarpari, Senior Solution Engineer, **Microsoft**
Bruce Tulloch, Chair of Requirements Working Group, **Trusted Energy Interoperability Alliance**, and CDIO Advisor, **JERA Japan**

About the Organizer

The Smart Grid Observer is an online information resource serving the global smart energy industry. SGO delivers the latest news and information on a daily basis concerning key technology developments, deployment updates, standards work, business issues, and market trends worldwide. SGO produces several conferences each year on topics such as microgrids, grid modernization, data centers, EV charging, V2G, next-gen smart grid technologies, distributed energy resources, and more. For a list of upcoming and recently concluded SGO conferences, visit https://smartgridobserver.com/events

Event Partners

Event Venue

Chicago Executive Conference Center

205 W. Wacker Drive, Chicago

Located in downtown Chicago's Loop, the Conference Center is steps away from the city's magnificent lakefront with world-renowned Millennium and Grant Parks, marvelous museums, restaurants and retail shopping.

Registration

Includes copy of presentation PDFs, attendee list, and access to exhibits, networking lunches, coffee breaks and drink receptions. To register securely online, visit: https://ics-scada-symposium.com/register

Standard — $1,095.00

Equipment and software vendors, consultants, and services providers. Access to main conference on June 16-17 plus Masterclass on June 18.

Non-Profit and Asset Owners — $895.00

End-user purchasers of cybersecurity software and network devices / hardware. (For academic, government and non-profit organizations, an .edu, .gov or .org email address is required). Access to main conference on June 16-17 plus Masterclass on June 18.

Masterclass Only — $595.00

Access to Masterclass on June 18 only. Includes presentation PDFs, Masterclass attendee list, coffee breaks and lunch.

"An awesome opportunity to network and find interesting paradigms in cyber security. I found the presentations engaging and insightful to see different perspectives."
- Jorge Hurtado, Intel 471

"Everything went well. The topics and speakers chosen are very relevant to what is happening in the industry. In fact, the presentations contents are state of the art. The conference is able to attract the utilities, which is always a challenge."
- Ramesh Reddi, CTO, CybSecBCML, Inc

"It was an excellent event with the perfect mixture of people interested in cybersecurity."
- Josh Schmidt, Director - Cyber Security Assessment Services, BPM

"Just the right size. Excellent industry participants, excellent speakers, excellent networking."
- Dr. Robin Podmore, President, IncSys

"Well organized and very informative. The panels of experts were well selected. Excellent presentations - well done!"
- Anita Bhat, Principal Member of Technical Staff, Sandia National Laboratories

"Really enjoyed the conversations. The presentations were extremely useful. Very relevant."
- April Morelock, Lead, Cyber Security Operations Team, Midcontinent ISO

Sponsorship Packages

Gold Level Sponsor $6,000

Top-level logo recognition as Gold-Level Sponsor
Speaking slot on panel session or stand-alone
Tabletop exhibit in networking break and reception area
Booth in Symposium Virtual Exhibit
3 complimentary conference passes
30% off additional registrations
Top logo positioning in Official Program Guide, event website, and email communications
Corporate description on event website
Logo in on-site banners and signage
Dedicated floor-standing banner (provided by sponsor)
Company information or flyer distributed to all attendees at check-in
Attendee List with contact details (for attendees who give permission)

Silver Level Sponsor $4,000

Logo recognition as Silver-Level Sponsor
Tabletop exhibit in networking break and reception area
Booth in Symposium Virtual Exhibit
2 complimentary conference passes
20% off additional registrations
Logo positioning in Official Program Guide, event website, and email communications
Corporate description on event website
Logo positioning in on-site banners and signage
Dedicated floor-standing banner (provided by sponsor)
Attendee List with contact details (for attendees who give permission)

Bronze Level Sponsor $2,500

Logo recognition as Bronze-Level Sponsor
Tabletop exhibit in networking break and reception area
Booth in Symposium Virtual Exhibit
1 complimentary conference pass
15% off additional registrations
Logo positioning in Official Program Guide and event website
Corporate description on event website
Logo recognition in on-site banners and signage
Attendee List with contact details (for attendees who give permission)

Lanyard Sponsor $5,000

Corporate logo printed on lanyards distributed to all attendees
Same deliverables as Silver level

To arrange your participation, contact Daniel Coran, Program Manager, at dcoran@smartgridobserver.com