

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

Job Titles

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

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)

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

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

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

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

5:15 – 6:30 pm Reception

Day 2 - Wednesday, June 17, 2026

Theme: Detection, Response & Resilience

9:00 – 9:15 am

Day 2 Kickoff & Recap

- 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

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

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
- Working with vendors: SLAs, procurement language, SBOMs

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

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

10:15 - 10:45 am Networking Coffee Break

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

12:00 - 1:00 pm Lunch

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

2:15 - 2:45 pm Networking Coffee Break

2:45 - 4:00 pm

- Identifying particular work flows for specific use cases
- Guard rails for agents that operate without human interaction

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>

Media 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.



Early Bird 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>

Early Bird Main Conference - Standard \$795.00

Equipment and software vendors, consultants, and services providers.

Access to Day 1-2, June 16-17. Available until May 15, 2026 - \$995.00 afterwards

Early Bird Main Conference - Non-Profit \$595.00

Academic, Government and Non-Profit organizations (.edu, .gov or .org email address required). Access to Day 1-2, June 16-17. Available until May 15, 2026 - \$795.00 afterwards

Early Bird ICS / SCADA Asset Owners \$595.00

End-user purchasers of cybersecurity software and network devices / hardware

Access to Day 1-2, June 16-17. Available until May 15, 2026 - \$795.00 afterwards

Day 3 Masterclass / Workshop

Main Conference (June 16-17) plus Masterclass (June 18) – Standard \$1,290.00

Main Conference (June 16-17) plus Masterclass (June 18) – Non-Profit \$990.00

Main Conference (June 16-17) plus Masterclass (June 18) – Asset Owners \$990.00

Masterclass (June 18) only \$595.00



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

The roundtable format and size are great. The panels and sessions in the morning were excellent.

- Robin Berthier, CEO and Founder, Network Perception

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

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

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	\$3,000
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

Recent SGO Sponsors Include

