SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

Attacking and Defending Mission Critical ICS Assets

Don C. Weber, Cutaway Security, LLC.

SANS ICS410 ICS/SCADA SECURITY ESSENTIALS – INSTRUCTOR
SANS ICS613 ICS/OT PENETRATION TESTING AND ASSESSMENTS – AUTHOR / INSTRUCTOR

Don C. Weber – SANS Certified Instructor and Author

- USMC - Sergeant 1991 - 1999
- Masters Degree in Information Assurance
- IACS Security Program Maturity
- IACS Security Assessments
- Penetration Testing
- Security Research

ICS613: ICS/OT Penetration Testing & Assessments

ICS410: ICS/SCADA Security Essentials™

Global Industrial Cyber Security Professional (GICSP)

Agenda

- Understanding ICS/OT Concepts
- Example ICS / OT Deployments
- Outlining ICS/OT Attacks
- Summay

Image Source: AI Generated using MidJourney on August 14, 2025

SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

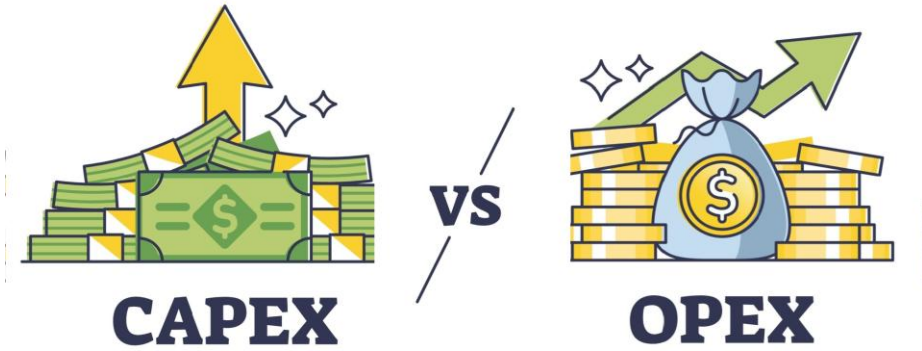
Understanding ICS/OT Concepts

Why is it different than IT?

Differences Between IT and OT Environments

Aspect	Information Technology (IT)	Operational Technology (OT)
Focus	Data, applications, business processes	Physical processes, equipment control
Priority	Confidentiality → Integrity → Availability	Safety → Confidentiality → Integrity → Availability
Lifecycle	3–5 years	15–30 years
Downtime	Tolerated with backups	Minimal tolerance
Change	Frequent, agile	Infrequent, highly controlled
Security Goal	Protect information	Maintain safe, continuous operation
Protocols	Standard IT protocols	Standard IT protocols, Industrial protocols
Environment	Controlled	Harsh, industrial
Ownership	IT staff	Operations/engineering teams

Operational Expenses



- One-time / infrequent purchases
- Asset ownership with long-term value
- High upfront cost with depreciation risk
- Aligns with long-term lifecycle

- Personnel salaries and benefits
- Ongoing operational costs
- Pay-as-you-go services
- Strictly budgeted according to original projections

Anecdotal evidence suggests that **about 95% of all cybersecurity spend goes to enterprise IT, while approximately 5% is allocated to OT.**

– Rob M. Lee, CEO of Dragos – Congressional Testimony 2025

Industrial Assets are the Core of Businesses

- Companies sell products and services
- Industrial / Automation generate and deliver these products and services
- You cannot deliver what you cannot produce
- When the core is affected, all are affected
- **This makes industrial assets the core to businesses and our communities**

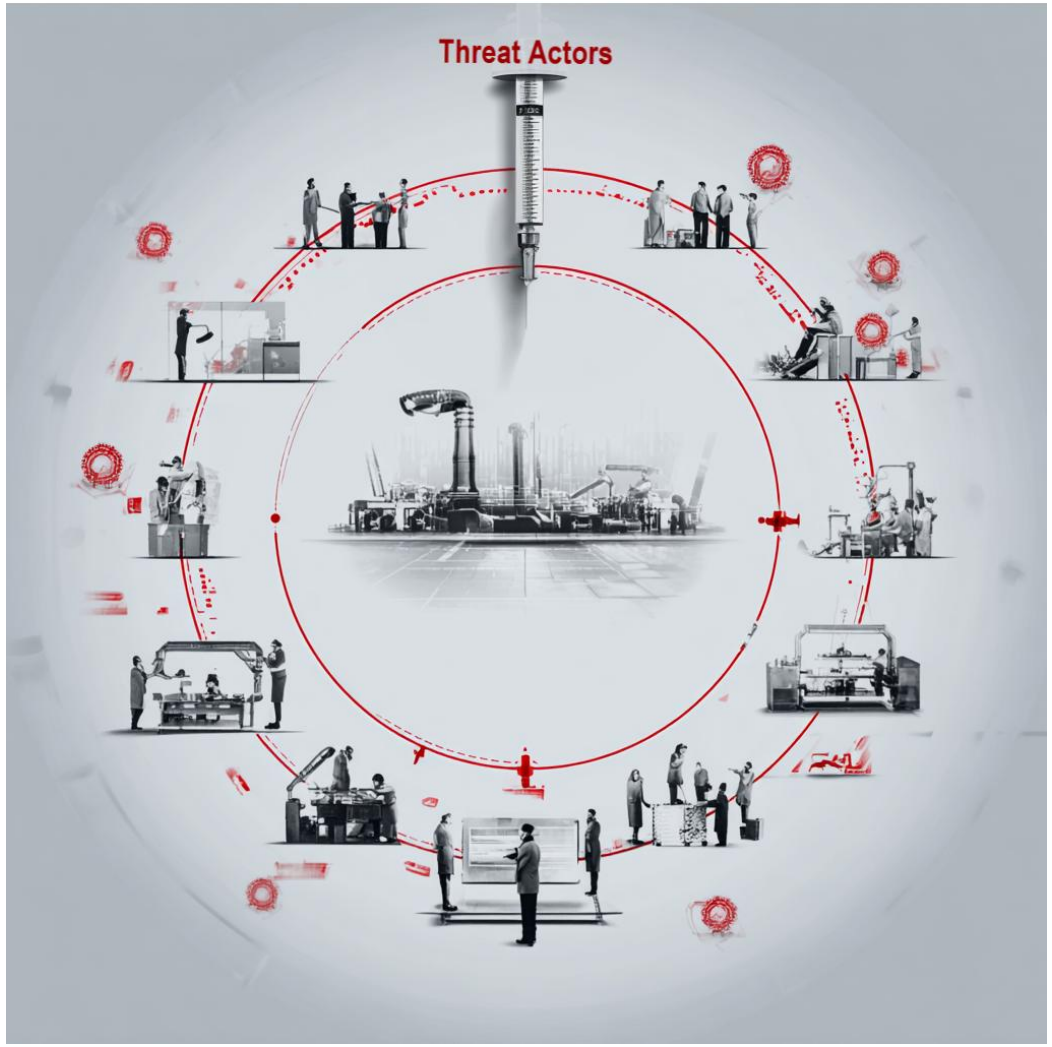


Image Source: AI Generated using MidJourney on August 14, 2025

Section Summary

- ICS / OT is based on different operating requirements
- ICS / OT assets are dedicated to operational actions, not cybersecurity
- Protecting ICS / OT starts with strong perimeter, testing, and monitoring
- **ICS / OT Risk management must include increased budget to ensure operations**

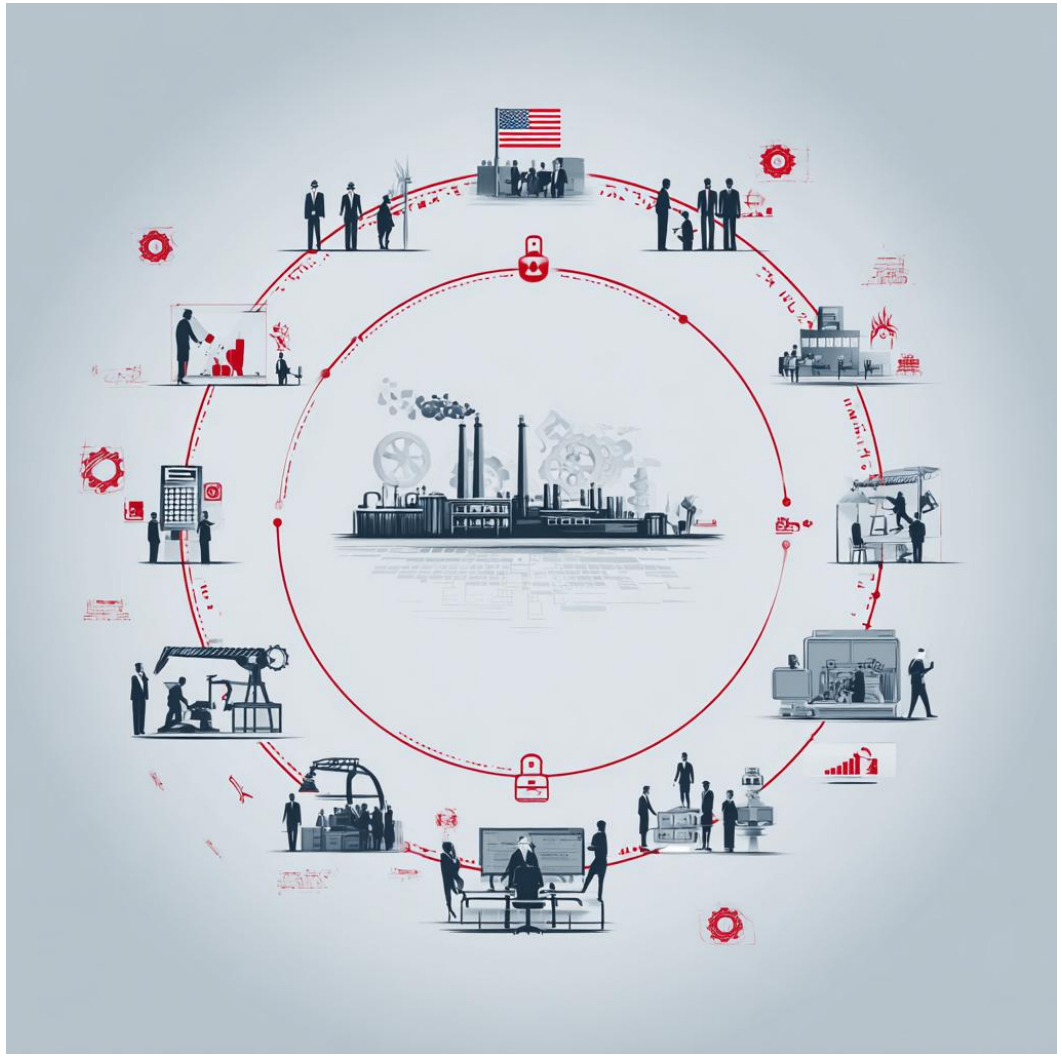


Image Source: AI Generated using MidJourney on August 14, 2025

ICS / OT Examples

ICS / OT is not just a PLC...

Example OT Deployments

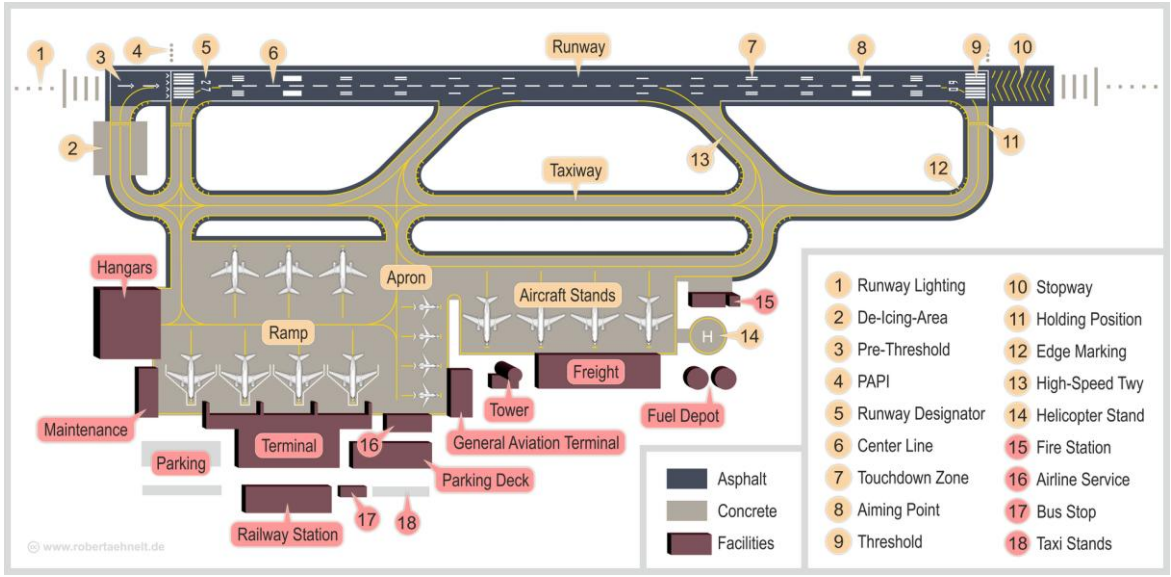
- Airport Processes
- Manufacturing Execution System
- Liquid Natural Gas Plant

Image Source: AI Generated using MidJourney on August 14, 2025

Airport Processes

- Access Control
- Automated People Movers / Light Rail
- Parking Garages
- Baggage Handling Systems
- Baggage Reconciliation System
- Ground Support Equipment
- Computer-Aided Dispatch
- Airfield Ground Lighting
- HVAC
- CCTV
- Water Treatment
- Fuel Distribution
- Ops Messaging
  - ARINC AviNET
  - SITA AIDX
  - IATA Teletype B
- SCADA Control Center

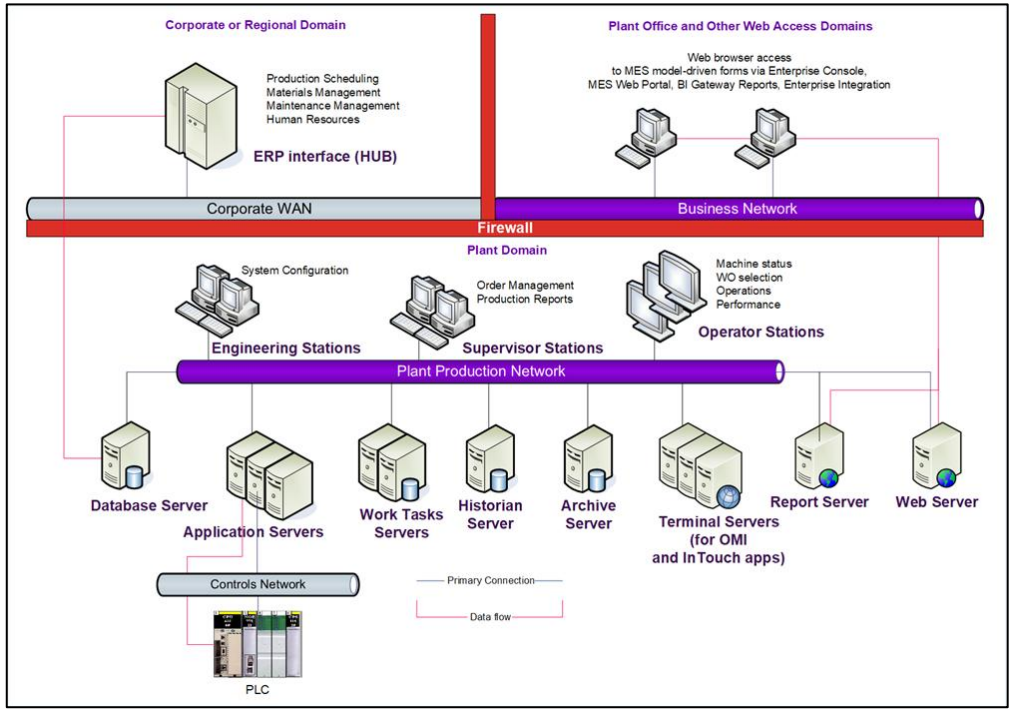
Airport operations function as a tightly integrated ecosystem connecting airlines with numerous third-party providers to coordinate and sustain every critical service.



Airport Infrastructure: https://en.wikipedia.org/wiki/Airport

Manufacturing Execution System

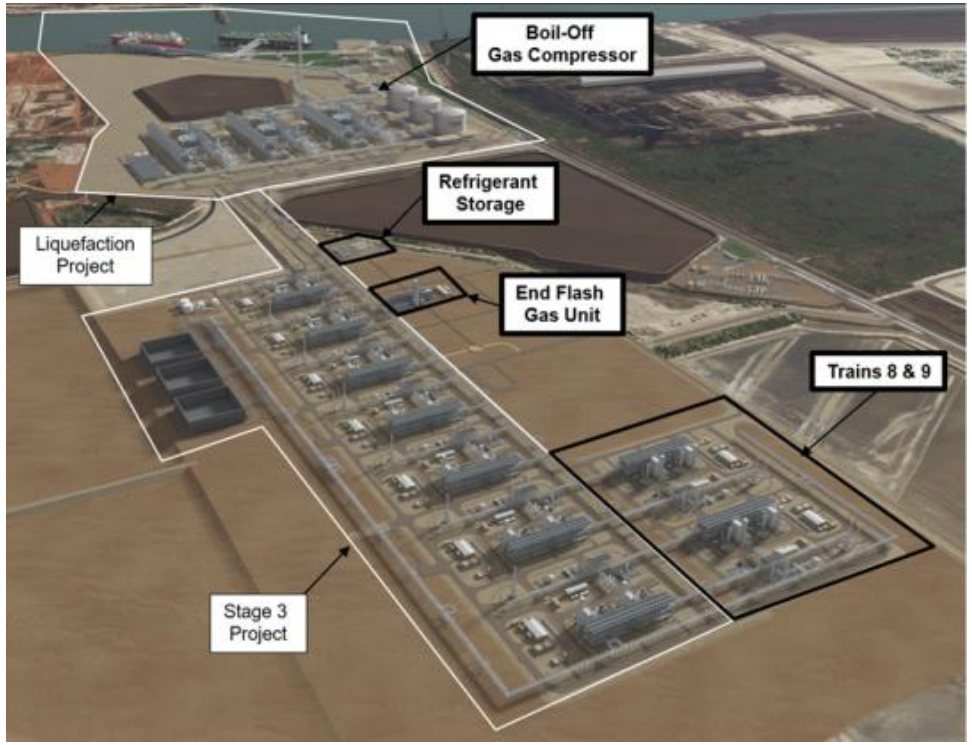
- **Middleware / Application Server**: Core MES logic, models, execution workflows
- **Database Server**: Storage of MES execution, quality, performance data (SQL Server-based)
- **Web Application (Portal) Server**: MES web interface, requires IIS and web infrastructure components
- **Reporting Server**: Secure, performance-optimized report generation and data access
- **Edge Nodes / Plant Collectors**: Local data capture and model adaptation at each site
- **Cloud Integration & Analytics**: Aggregation via AVEVA Connect for analytics, AI, visualization

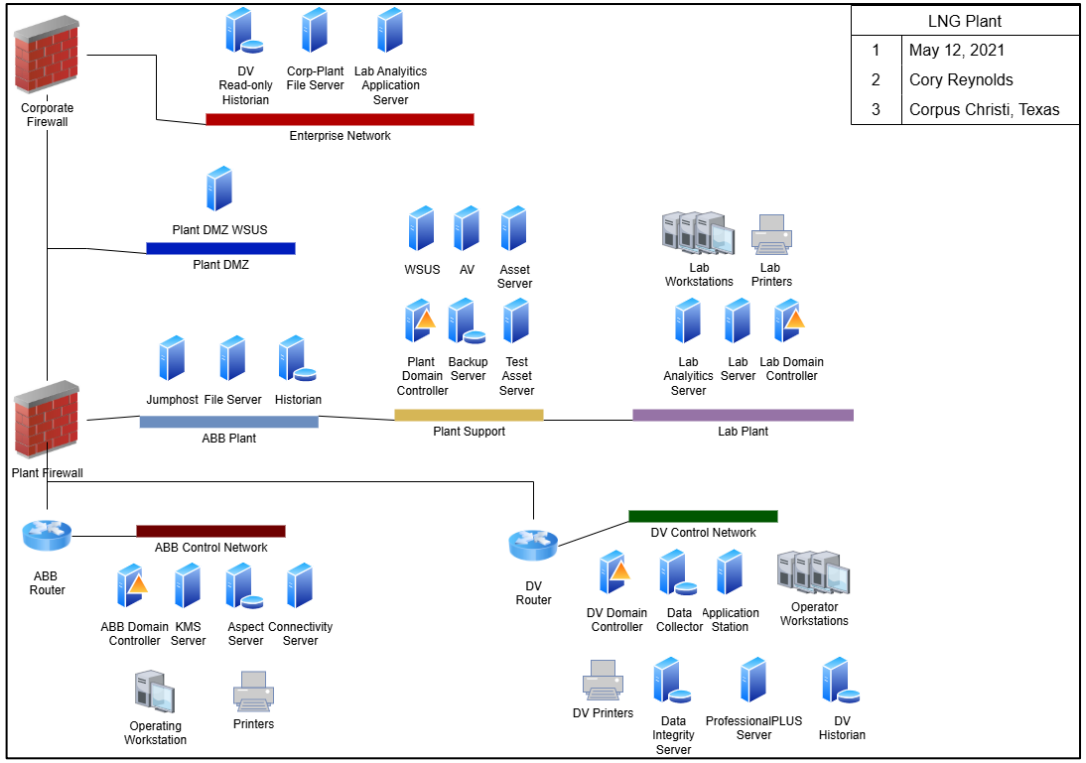


Manufacturing Execution Systems are engineered to keep production running above all else, often relying on fragile, tightly coupled server and device integrations and communications that leave cybersecurity as a secondary concern.

Aveva MES Standard Arch:
https://docs.aveva.com/bundle/manufacturing-execution-system/page/73956.html

Liquid Natural Gas (LNG) Plant





LNG and oil/gas operations are intricate, multi-vendor ecosystems with a significant physical footprint that integrates process control, quality labs, and real-time business data flows with potential impacts to human and environmental safety during incidents.

Section Summary

- ICS / OT operations can be extremely complex
- ICS / OT environments require cooperative asset and operation management
- **ICS / OT technologies focus on complex physics-based decision making, not cybersecurity**

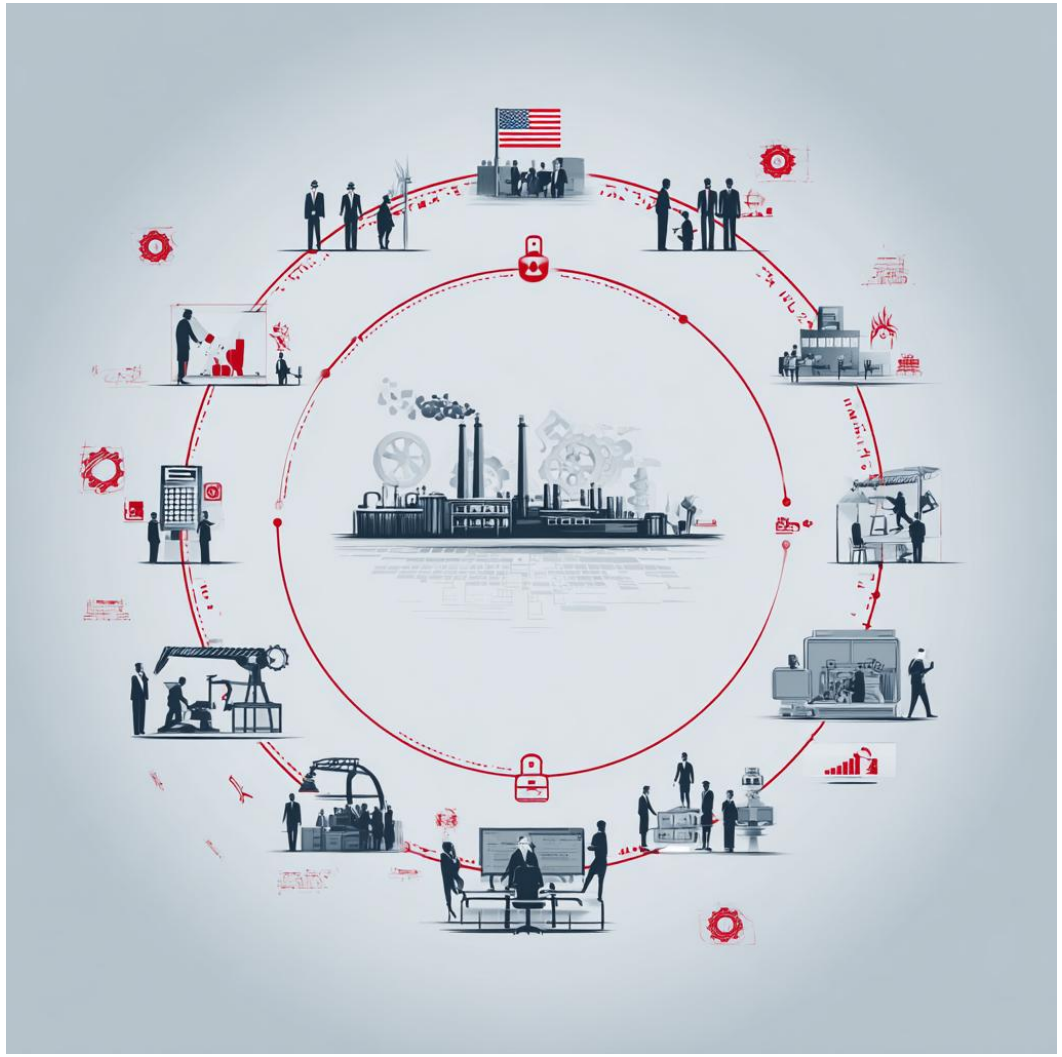


Image Source: AI Generated using MidJourney on August 14, 2025

Outlining ICS/OT Attacks

Process environments are connected to the internet?

Nozomi Top 10 Techniques

Top 10 Most Common MITRE ATT&CK™ Techniques Associated with Raised Alerts

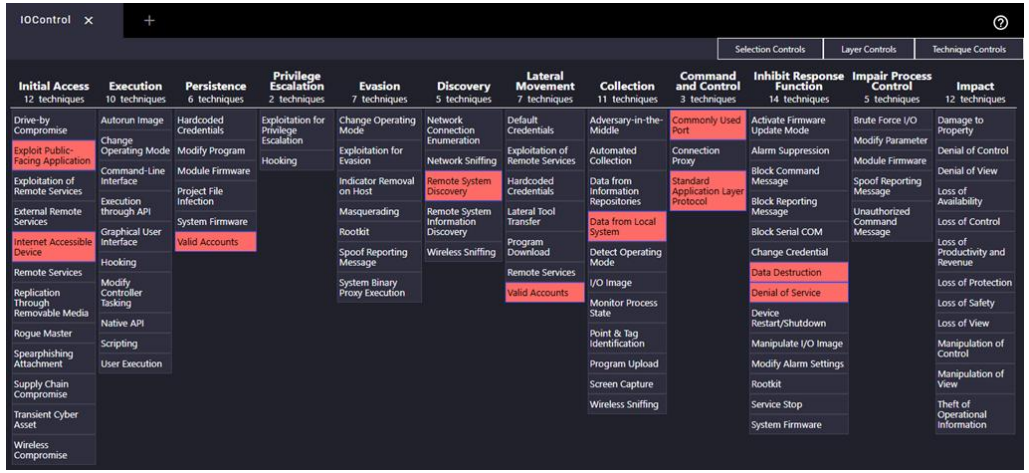
ID	Technique name	Tactic name	%
T1565	Data Manipulation	Impact	39.54%
T1071	Application Layer Protocol	Command and Control	12.29%
T1095	Non-Application Layer Protocol	Command and Control	12.29%
T1498	Network Denial of Service	Impact	8.86%
T0841	Network Service Scanning	Discovery	7.89%
T0846	Remote System Discovery	Discovery	7.89%
T1557	Adversary-in-the-Middle	Credential access; Collection	5.48%
T1110	Brute Force	Credential access	3.20%
T0812	Default Credentials	Lateral Movement	0.89%
T0859	Valid Accounts	Persistence; Lateral Movement	0.89%

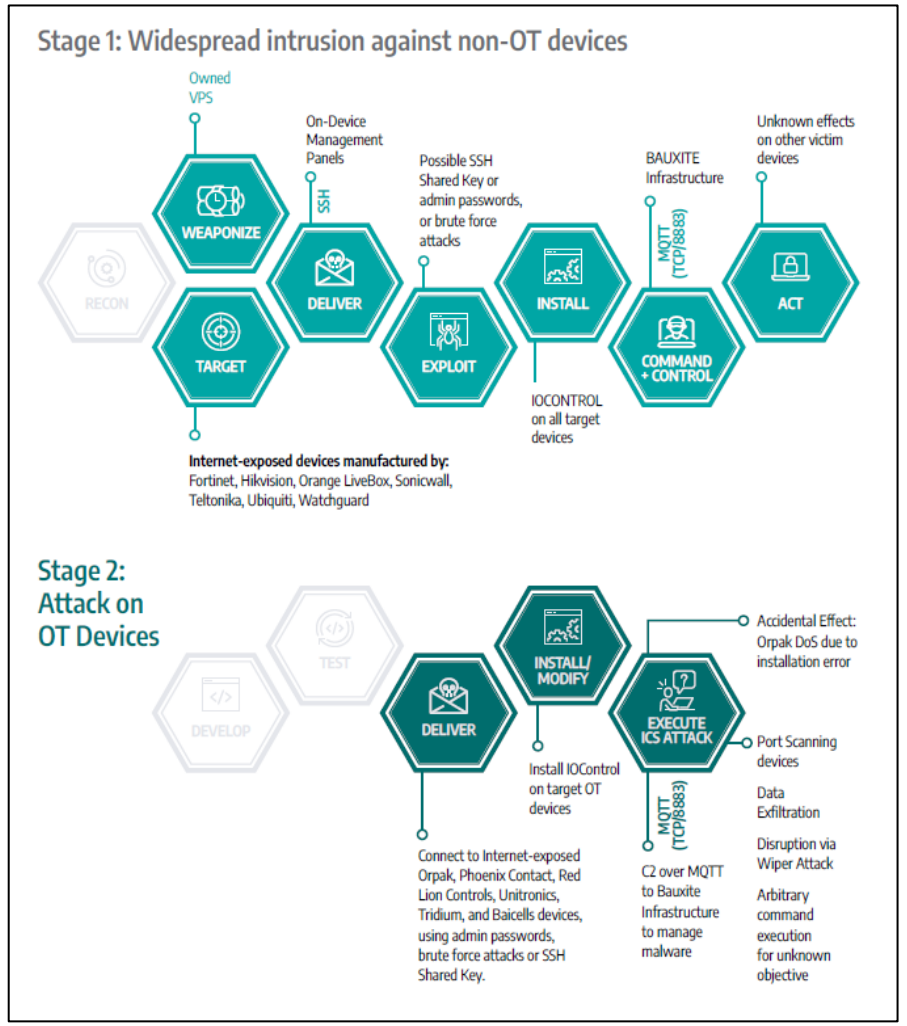
- What data was manipulated? Unclear
  - → Ranges from obscuring operational information to changing logs
- C2 via Protocols
  - → Used standard (HTTP/HTTPS) and non-standard (MQTT) channels
- Denial-of-Service Impact
  - → The SANS 2024 survey highlighted that 38% of ICS/OT ransomware incidents impacted the safety or reliability of the physical process

Nozomi Report: https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2025

BAUXITE IOControl Campaign

- **Two Stage Attack: IT -> OT**
  - → Target: fuel-management systems in the United States and Israel
- **Connected to internet-exposed ICS / OT assets**
- **Installed IOControl malware on devices**
- **Established C2 over MQTT**
- **Denial of Service via Wiper Attack**

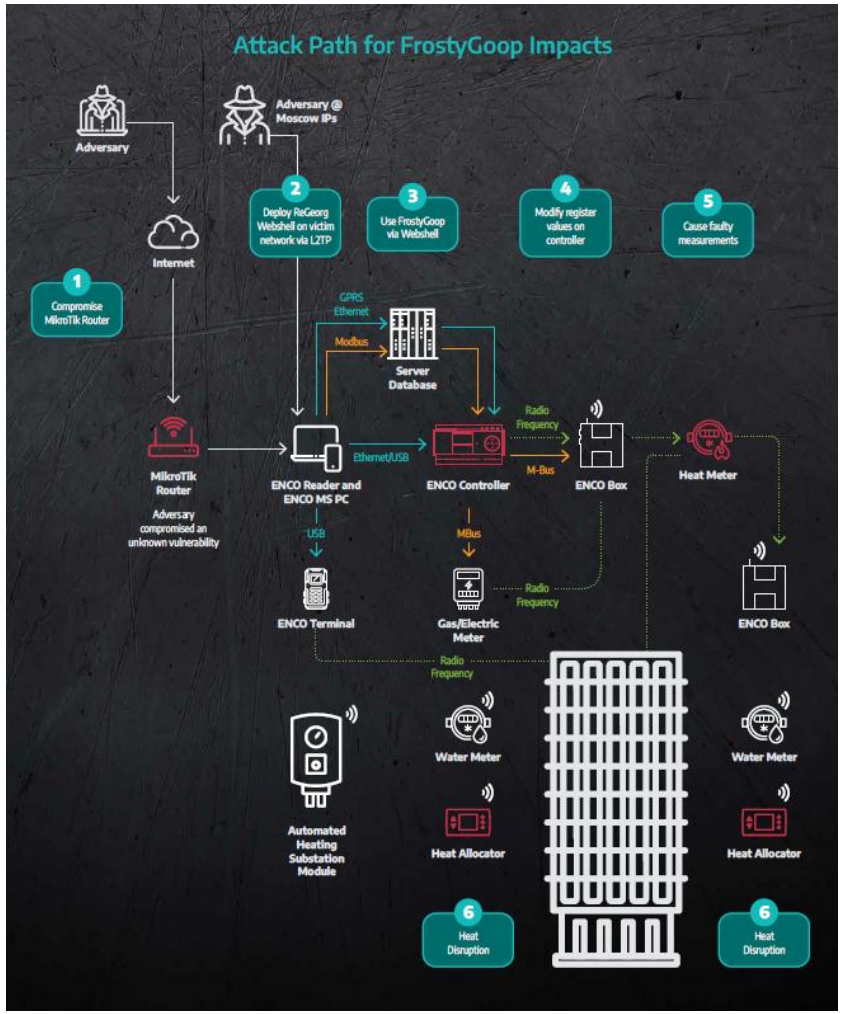




Dragos 2025 Year in Review: https://www.dragos.com/ot-cybersecurity-year-in-review

FrostyGoop Attack

- **Zero-Day Vulnerability in internet-facing MikroTik Routers**
  - → Target: municipal district heating system in Lviv, Ukraine
- **C2 using ReGeorg Webshell on management systems**
- **Threat actors downgraded ENCO controller firmware**
- **Modbus commands to ENCO controller**
  - → Could have targeted other ICS devices
- **Faulty readings affected heat distribution during winter conditions**



Dragos 2025 Year in Review: https://www.dragos.com/ot-cybersecurity-year-in-review

Targeting Remote Access

- The exploitation of vulnerabilities as an initial access vector for breaches has seen significant growth, increasing by 34% from 2023 to 2024, partly supported by zero-day exploits **targeting edge devices and VPNs**

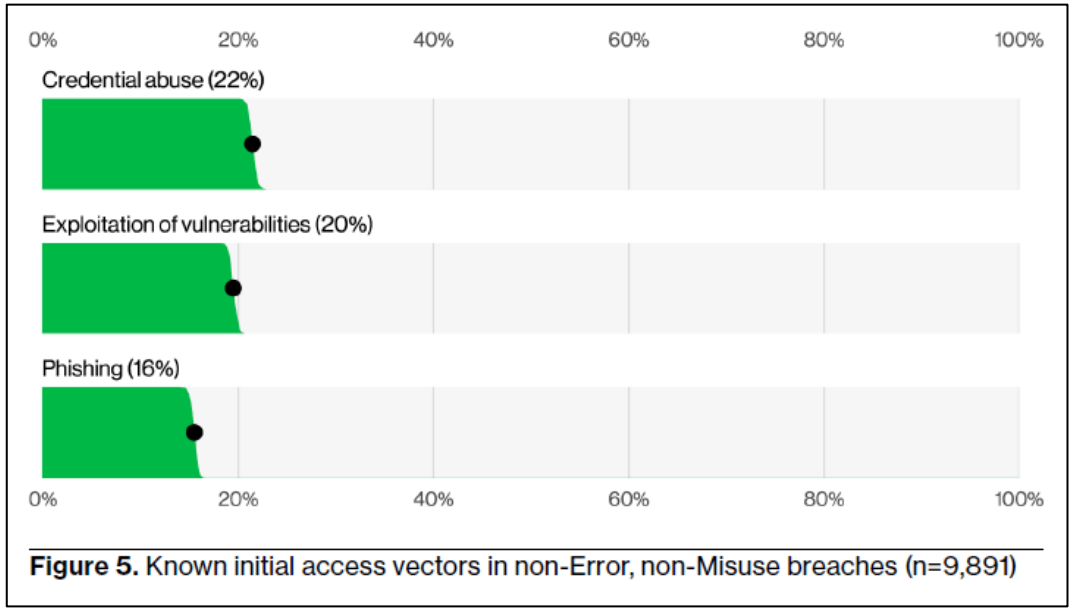
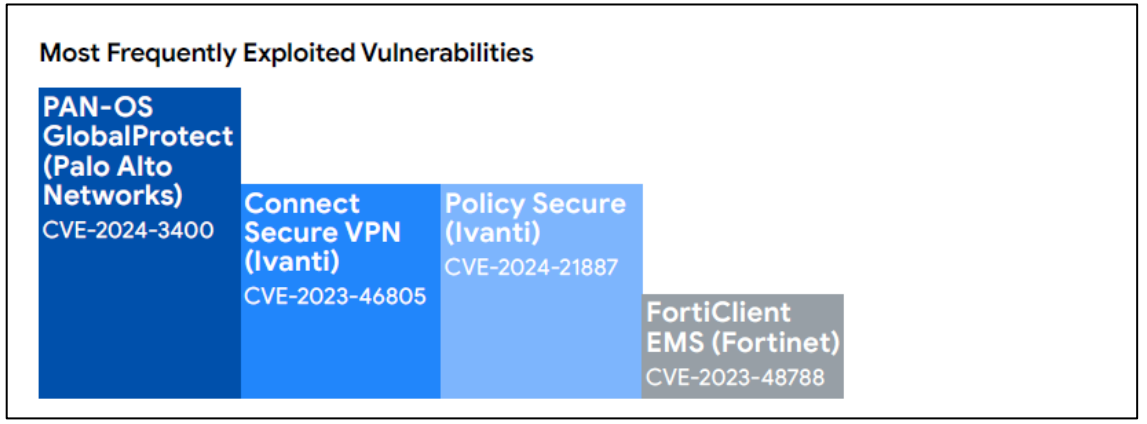


Figure 5. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

Verizon 2025 DBIR: https://www.verizon.com/business/resources/reports/dbir/



Google M-Trends 2025 Report: https://cloud.google.com/security/resources/m-trends

- Most Frequently Exploited Vulnerabilities Among the Mandiant incident response investigations performed in 2024, the most frequently **exploited vulnerabilities affected security devices**, which are, due to their function, typically placed at the **edge of the network**. Three of the four vulnerabilities were first exploited as zerodays.

Section Summary

- Threat actors find internet exposed infrastructure
- They are practiced in weaponizing and exploiting opportunities
- **Lack of ICS / OT monitoring increases threat actor time on target and success**

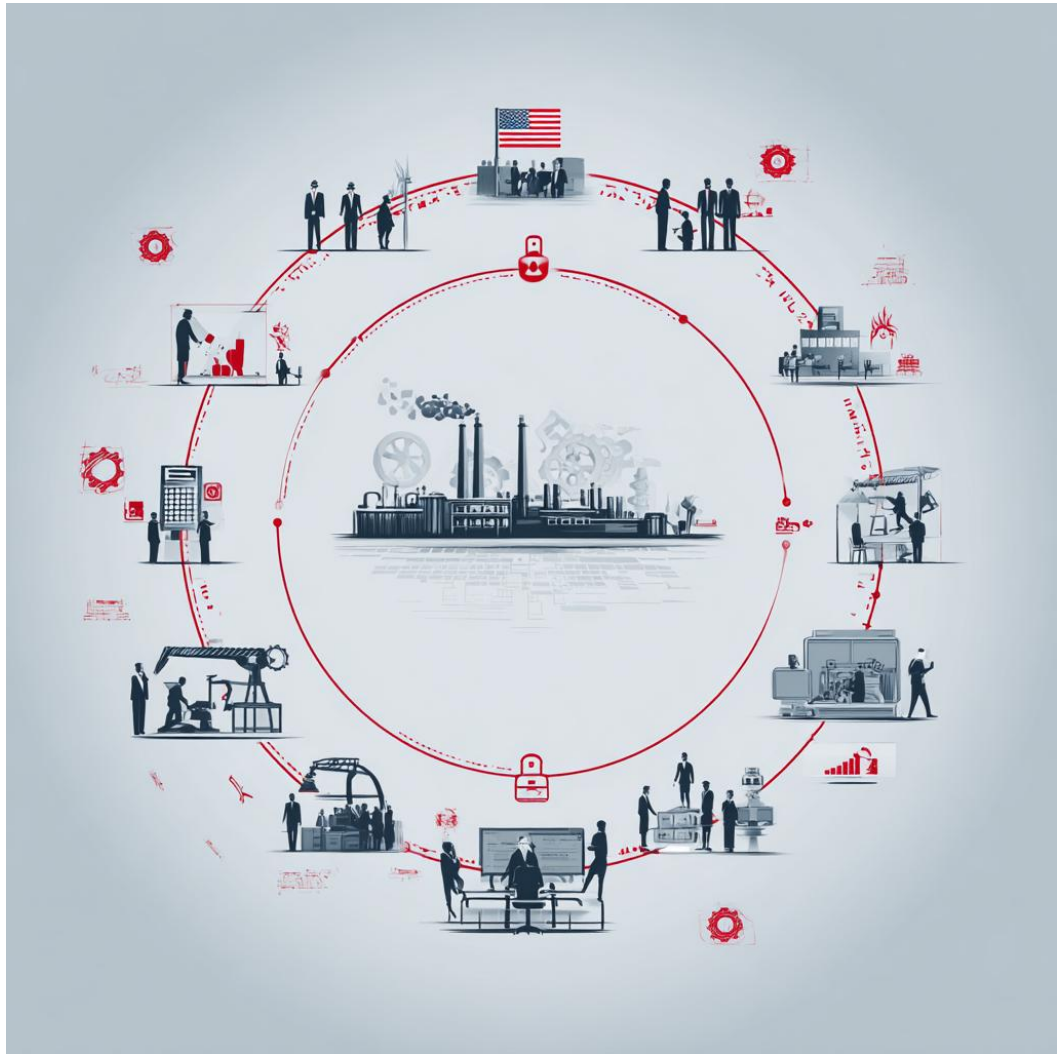


Image Source: AI Generated using MidJourney on August 14, 2025

Summary

How big of a problem is ICS / OT cybersecurity?

Get Good!!! Get Good, Right Now!!!

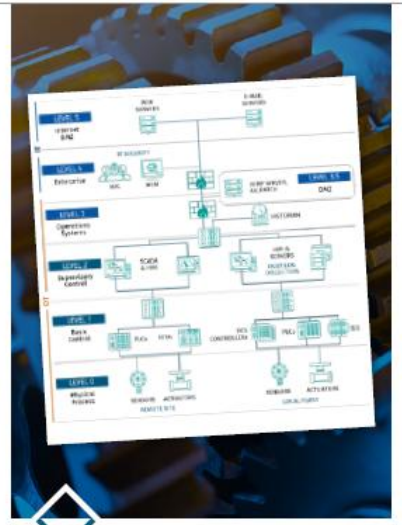
Image Source: https://www.foreignaffairs.com/china/china-winning-cyberwar

SANS 5 ICS Cybersecurity Critical Controls

Do not *force* IT cybersecurity requirements onto OT environments.

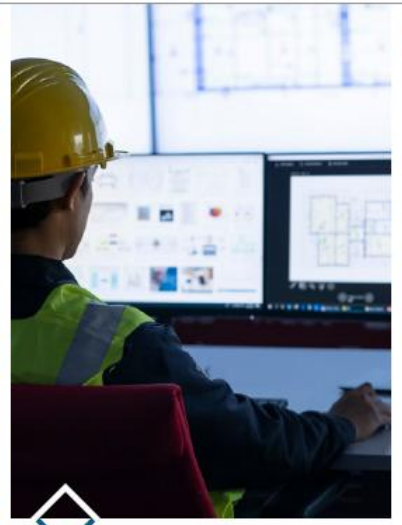
CS INCIDENT RESPONSE

perations-informed IR plan with ocused system integrity and recovery apabilities during an attack. xercises designed to reinforce risk cenarios and use cases tailored to he ICS environment



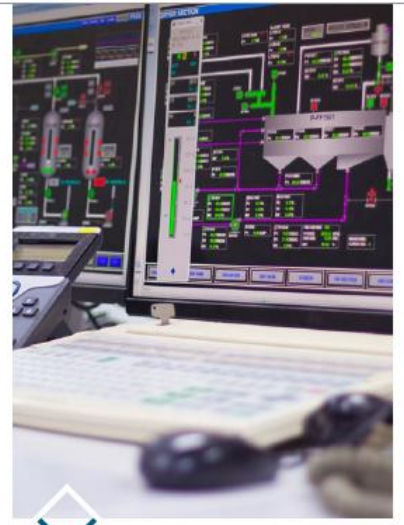
DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement



ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

RISK-BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital control in place and device operating conditio that aid in risk-based vulnerability management decisions to patch for th vulnerability, mitigate the impact, or monitor for possible exploitation

https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls


Q&A

ICS613 Introduction

Beta

ICS613: ICS/OT Penetration Testing & Assessments

In Person (5 days) **30 CPEs**

Industrial Control Systems (ICS) and Operational Technology (OT) are increasingly targeted by adversaries, yet traditional penetration testing approaches often focus on the wrong outcomes and can cause unintended disruptions with severe consequences – including production outages, injury to personnel, loss of life, and environmental hazards. ICS613: ICS/OT Penetration Testing & Assessments introduces engineering, operations, and security professionals with the mindset, methodologies, and techniques to safely and appropriately conduct penetration tests and security assessments, identify practical mitigations, and effectively communicate results to stakeholders and leadership to improve the operational resilience of ICS environments.

Course Authors:

Don C. Weber
Certified Instructor

Jason Dely
Certified Instructor

Tyler Webb

SANS

INDUSTRIAL CONTROL SYSTEMS SECURITY

ICS/OT Penetration Testing & Assessments

sans.org/ics613

Developing World Class ICS / OT Cybersecurity Professionals

BETA In-Person

Salt Lake City, UT

August 25 – 29, 2025

In-Person

SANS CDI 2025 – D.C.

Dec 12 – 16, 2025