Why OT Cybersecurity Can’t Be Solved with IT Tools: A Site-Level Perspective

Alan J Raveling
Senior Technologist @ Interstates

ISA | ISASecure®

May 2025

Who am I?

- Alan Raveling, DCS
  Senior Technologist @ Interstates
- ISA/IEC 62443 Cybersecurity Expert, GICSP, CISSP
- 20 years experience with OT infrastructure and cybersecurity

Agenda

- IT vs OT Security
- Right Tool(s) for the Job
- Challenges With Assessments
- ACSSA
- Q&A

IT vs OT Security

The continual march towards convergence

- Consolidated resources to manage IT-like assets
- Unified technologies to aid with disaster recovery, business continuity, etc.
- Lack of OT cybersecurity materials, expertise creating vacuum for IT professionals to encroach

IT vs OT Security

Increasing connectivity

- Edge-to-cloud data movement
- IT devices serving in OT capacities
- ERP, MES, supply chain, logistics, etc. causing IT/OT firewalls to become more lax

IT vs OT Security

Alignment on risk

- What should be patched & when?
- Application & hardware vulnerabilities?
- How is the risk to the organization quantified?
- Priority for elevating cybersecurity posture of assets to security target level?

IT vs OT Security

What is being protected?

- Safety of personnel, safety of assets, safety of product – not concerns in an IT environment
- How do you explain what zones & conduits are to IT cybersecurity personnel?
- What is your approach for islands of automation?

Right Tool(s) for the Job

My unplanned downtime incidents from using IT tools

- Faulted PLC
- Faulted remote I/O
- Crashed HMI
- Crashed engineering station
- Required networking switches to be power cycled

Right Tool(s) for the Job

Attributes of tools which may cause disruption

- Very fast speed of operation
  - Opening too many connections at once
  - Not closing connections after usage
- Incomplete / improper implementation of protocols
  - Tools side
  - Asset side

Right Tool(s) for the Job

What are the right tools?

- Spreadsheets
- Software from asset vendor / manufacturer
- Well-tested IT tools
- Moderately-tested OT tools

Right Tool(s) for the Job

Qualified / educated personnel

- Bring IT personnel along when performing tasks
- Activities are scheduled & well communicated – nobody should be surprised
- Seek out appropriate training: ISA/IEC 62443 courses

Challenges With Assessments

- What is assessed?
- How it is assessed?
- What body of material is it assessed against?

Challenges With Assessments

- Repeatability?
- Uniformity?
- Credibility?

ACSSA

Automation & Control Systems Security Assurance

- Built upon ISA/IEC 62443 2-1, 2-3, 2-4, 3-2, 3-3
- Assessment Report
- Certification of Conformance

ACSSA

Built upon ISA/IEC 62443 2-1, 2-3, 2-4, 3-2, 3-3

- Well defined and stated objectives and methodologies
- Actively listening to the unique demands of IACS
- Direct correlation to IT cybersecurity standards not always available

ACSSA

Assessment Report

- Clear understanding of gaps
- Consistent between reports due to approach
- Enables multi-site, multi-year comparison leveraging multiple assessing organizations

ACSSA

Certification of Conformance

- Assurance that current assets within scope conform to cybersecurity requirements
- Potential benefit for cybersecurity insurance premiums
- Understanding of cybersecurity maturity of new controls systems as installed

Q&A

- Thank you for attending
- https://isasecure.org/isasecure-site-assessment
- https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards