SANS Five ICS Cybersecurity Critical Controls. Myths Vs. Reality

These myths show common ICS/OT assumptions; the realities show what matters when control systems and safety are on the line.

Control #1: ICS-Specific Incident Response
Myth: IT incident response covers ICS/OT environments.
Reality: ICS/OT response prioritizes safety and equipment, enables engineering-led recovery, and stabilizes processes—not simple asset isolation.

Control #2: Defensible Control System Network Architecture
Myth: Documented segmentation equals defense.
Reality: Defensible ICS/OT architecture requires enforced control system specific traffic paths—not implicit trust or paper-only segmentation.

Control #3: ICS Network Visibility and Monitoring
Myth: More alerts mean better visibility and monitoring.
Reality: ICS/OT visibility comes from understanding control traffic behavior and detecting abnormal or unsafe interactions early—context over volume, always.

Control #4: Secure Remote Access
Myth: MFA makes remote access secure.
Reality: All ICS/OT remote access must have MFA and, be inventoried, time-bound, and monitored; broad or persistent access increases risk unnecessarily.

Control #5: Risk-Based Vulnerability Management
Myth: Patch highest CVSS vulnerabilities first.
Reality: ICS risk decisions depend on asset role, location, safety impact, and compensating controls already in place—not just CVSS scores.

5 ICS Cybersecurity Critical Controls Rapid Assessment

If strengthening your implementation of the SANS Five ICS Cybersecurity Critical Controls is a 2026 priority, this focused 90-minute session delivers clear, prioritized threat-informed direction for your ICS/OT cybersecurity program.

Rapid Virtual 90min call
Any timezone, bring your security and engineering teams at a time that works for them.

Visual Ranking
Visual snapshot ranking across all of the Five ICS Cybersecurity Critical Controls.

Ask Us Anything OT/ICS!
Dedicated time to get insights into addressing your prioritized ICS/OT cybersecurity challenges.