SCADA & ICS CYBERSECURITY ASSESSMENTS FOR CRITICAL INFRASTRUCTURE

The Reality Check Uptime Is No Longer Your Biggest OT Risk

Industrial environments now sit at the collision of always-connected OT, targeted industrial malware, and intense regulatory and stakeholder scrutiny.

Ransomware and ICS-aware attacks jump from IT to OT in minutes. Lines stop, safety systems misbehave, and every decision is later dissected by regulators, investigators, and the board.

What used to be a plant-level outage is now an enterprise event:

- Prolonged downtime and scrap
- Regulatory fines and mandated remediation
- Loss of customer and stakeholder confidence
- Board-level scrutiny of OT practices

OT was built for safety and uptime—not the internet or post-incident forensics. eSureITy's SCADA & ICS Cybersecurity Assessments close that gap.

Where SCADA and ICS Programs Break Down

The issue isn't a lack of tools. It's the gap between how OT actually runs and how risk is documented, governed, and defended after an incident.

Common failure patterns:

- **IT tools on OT problems –** Corporate firewalls, AV, and EDR leave SCADA/ICS blind spots; legacy protocols, flat networks, vendor tunnels, and unpatched devices stay exposed because uptime wins over change.
- **Connectivity without clear boundaries:** Converged IT/OT mixes business systems, HMIs, historians, engineering workstations, remote access, and cloud, with lateral paths from IT to OT left undocumented and untested.
- **Compliance without real assurance:** NIST SP 800-82, ISA/IEC 62443, and internal standards exist on paper, but there's no current, evidence-based view of how controls perform in the field, so regulators and reviewers see gaps, not alignment.
- **Documentation that does not stand up under investigation:** Incomplete inventories, outdated network maps, and risk registers that ignore real ICS devices, networks, and safety-critical functions, so external examiners treat it as unmanaged exposure.

This is where attackers, regulators, and external reviewers now focus.

The New Requirement: Defensible OT Security With Evidence That Holds Up

Regulators and critical-infrastructure stakeholders now expect industrial organizations to treat SCADA and ICS cybersecurity as a measurable, governed discipline—not an extension of IT.

Emerging expectations:

- Alignment with OT-specific standards such as NIST SP 800-82 and ISA/IEC 62443
- Awareness of DHS CISA, DOE, and sector-specific OT security advisories and expectations
- Demonstrable controls for segmentation, remote access, vendor management, and recovery
- A documented, current risk assessment specific to ICS that also supports typical cyber insurance coverage requirements for securing industrial control environments

External reviewers increasingly ask for detailed OT control evidence before sign-off on critical projects and during post-incident reviews.

eSureITy's SCADA & ICS Cybersecurity Assessments are built to generate that level of proof.

Contact Us info@eSureITy.com www.eSureITy.com

What the SCADA and ICS Cybersecurity Assessment Delivers

1. OT Exposure Mapped to Real Attack Paths

SCADA and ICS Vulnerability Testing

Non-disruptive reviews focused on:

- Insecure-by-design protocols and services
- Outdated firmware and unsupported assets
- Exposed interfaces and remote access
- Misconfigurations that enable pivoting or loss of view

SCADA and ICS Risk Assessment

Risk scored and prioritized across:

- Critical devices, controllers, and HMIs
- Networks, zones, and conduits
- Safety-, reliability-, and compliance-critical processesFindings are translated into operational impact—not just CVSS scores.

3. Human, Wireless, and API Attack Surface Reduction

Social Engineering, Wireless, Mobile, and API Testing

Assess how people and connectivity expand OT risk:

- Targeted phishing and social engineering of engineers and operators
- Wireless and mobile access used for maintenance and operations
- APIs and integrations exposing OT telemetry or control

Findings drive concrete control and training changes that harden these paths without blocking legitimate work.

Employee Security Awareness Training

Role-specific training for OT teams to recognize and respond to high-impact attacks on control environments.

How eSurelTy Reframes SCADA and ICS Cyber Risk

eSurelTy links industrial cybersecurity with governance so leaders enter audits, reviews, and board meetings with evidence—not assumptions.

Each assessment is built to:

- Expose technical and process-level weaknesses across SCADA and ICS
- Quantify the business impact of OT exposure in operational terms
- Map controls and gaps to accepted OT frameworks and reviewer expectations
- Provide an action plan that can be executed without disrupting production

You move from hoping your OT controls are sufficient to knowing what will withstand both attackers and independent investigators.

2. IT to OT Segmentation and Lateral Movement Validation

IT Network Penetration Testing and Vulnerability Analysis

Testing that demonstrates how an attacker could move from IT into OT and what would stop them, including:

- Segmentation and firewall rules between enterprise and control networks
- Remote access, vendor connectivity, and third-party pathways
- Authentication, authorization, and monitoring around OT-adjacent assets

The outcome is a clear picture of the actual blast radius of a compromised IT account, workstation, or application.

4. Governance, Response, and Oversight Readiness

Incident Response Planning for OT-Aware Events

Development or refinement of response playbooks that:

- Integrate IT and OT decision-making
- Define clear roles for engineering, operations, and security
- Align evidence collection and notification workflows with regulatory and stakeholder expectations

Security Governance and Advisory Support

Ongoing advisory support to close identified gaps, mature policies, and maintain documentation that stands up to auditors, regulators, and internal stakeholders.

Why eSurelTy

- **Industrial and OT Expertise** - Experience across energy, manufacturing, water, and critical infrastructure environments where uptime and safety cannot be compromised.
- **Governance alignment from day one** – Assessments and deliverables built with auditor, regulator, and board expectations in mind, not retrofitted after findings are produced.
- **End-to-End Visibility** - People, process, and technology evaluated together so gaps, overlaps, and ownership are clear.
- **Actionable Remediation Path** - Findings translated into sequenced, realistic remediation steps that respect maintenance windows, vendor constraints, and operational realities.

Engage eSurelTy to scope a SCADA and ICS Cybersecurity Assessment and put a defensible, audit-ready OT security strategy in place.

Contact Us

info@eSurelTy.com

www.eSurelTy.com