ERPI – Webinar Audience Q&A
11 December 2025

Answers by Ivan Savov, Chairman, European Risk Policy Institute (ERPI)

1. How can UPS systems be secured when accessible over the web, and what cyber risks affect critical power backup? How does ISA/IEC 62443 apply?

Web-accessible UPS systems introduce two immediate risks: unauthorised access and remote manipulation of power states. In industrial environments, tampering with UPS configurations can disrupt controlled shutdowns or create cascading failures during power outages.

Recommended practices aligned with ISA/IEC 62443:

• Network segmentation: The UPS must sit in a protected cell/zone, isolated from corporate IT networks.

• No direct internet exposure: Access must only occur through VPN, jump server, or a secure remote-access solution.

• Role-based access control (RBAC) and multi-factor authentication.

• Vendor-supported secure configurations combined with strong password hygiene.

• Continuous monitoring and logging of UPS-access events.

• Lifecycle patching of firmware and management consoles.

IEC 62443 emphasises a defence-in-depth architecture and places UPS systems within the required segmentation and secure remote-access practices.

2. How can we evaluate patches from many vendors, especially for L1 devices like PLCs? Is there software that helps?

Patch evaluation in OT must follow a triage and risk-based process, not a blanket update strategy.

Key steps:

• Maintain an asset inventory linked to firmware and patch levels.

• Review vendor patch advisories and vulnerability descriptions.

• Assess if the vulnerability is exploitable in your specific architecture (network isolation, physical access, protocol exposure).

• Test patches on a sandbox/test bench before deploying to production.

Tools that assist with patch intelligence:

• Claroty CTD, Tenable.ot, Nozomi Guardian, Dragos Platform – provide vulnerability mapping against asset inventories.

• Vendor security portals (Eaton, Schneider Electric, Siemens, Rockwell) – provide verified patch assessments.

There is no universal tool that can "evaluate all patches automatically," but combining OT-aware vulnerability management with vendor guidance creates a reliable process.

3. **What challenges arise during cybersecurity risk assessment in electrical substations, and what OT protocols are common?**

Key challenges:

• Legacy devices with limited security controls.

• Flat networks without segmentation.

• Limited logging and monitoring capabilities.

• Vendor-specific constraints on patching.

• Insufficient asset visibility and configuration baselines.

• Physical access by contractors or maintenance teams.

Common OT/utility protocols:

• IEC 61850, DNP3/Secure DNP3, Modbus/TCP, IEC 60870-5-104, PROFINET, EtherNet/IP.

These protocols were often designed without native security. Risk assessments must apply segmentation, monitoring, protocol-aware intrusion detection and access-control measures.

4. **What practical steps can stakeholders take to apply Secure by Design and Secure by Operations?**

• Secure by Design: secure defaults, hardened configurations, protected interfaces, lifecycle support.

• Secure by Operations: daily discipline — patch reviews, monitoring, segmentation, least privilege, validated changes.

• Treat OEM → integrator → operator handoff as critical; ensure documentation and baselines are transferred.

Visible risk reduction appears when cybersecurity becomes routine operational behaviour.

5. How can providers, owners, and integrators align on security expectations?

Alignment requires a shared responsibility model:

• OEMs provide hardened defaults, secure guides, SBOMs and lifecycle support.

• Integrators preserve secure defaults and document deviations.

• Operators maintain posture through procedures, monitoring and governance.

• Authorities provide baselines and coordination.

Alignment emerges when all actors use the same configuration baselines and reporting expectations.

6. What is the difference between Secure by Operations and Secure by Continuity?

Secure by Operations (SBO) focuses on daily security behaviour: patching, secure configurations, segmentation, monitoring, access control, backup integrity.

Examples:

• Weekly network-monitoring review and disabling unused PLC services.

• Quarterly patch assessments and selective deployment.

• Integrators validating baselines before commissioning.

• Remote access routed through jump servers with MFA.

Secure by Continuity (SBC) focuses on system stability under converging pressures: cyber, climate, supply-chain stress, ageing assets.

Examples:

• Grid operators merging cyber data with climate-stress forecasts.

• Energy providers correlating OT anomalies with supply-chain shortages.

• Water utilities using cross-value-chain drift dashboards.

• Hospitals running multi-sector continuity exercises.

Summary:

SBO protects the system today. SBC ensures the system remains stable tomorrow.

7. How do you define AI and Zero Trust in OT?

AI in OT:

• anomaly detection, predictive maintenance, situational awareness, accelerated RCA.

AI must be validated carefully; model drift can disrupt operations.

Zero Trust in OT:

• no implicit trust for any device or user,

• authenticated and authorised access for every session,

• segmentation into protected zones,

• continuous verification of device identity and behaviour,

• controlled remote access via jump servers and MFA.

Zero Trust limits blast radius while maintaining reliability.

Prepared by:

Ivan Savov

Chairman, European Risk Policy Institute (ERPI)

PerilScope: Strategic Horizons
Secure by Operations and the Architecture of Continuity

Ivan Savov
Chairman, European Risk Policy Institute (ERPI)

Introduction

The webinar on "Securing Critical Infrastructure Is a Collective Mission – Enabled by Secure by Operations Principles" is part of a much deeper shift. Critical infrastructure is entering an era in which the boundaries between cyber, physical, operational and systemic risks are dissolving. Secure by Design and Secure by Operations describe the technical and procedural layers of this shift. Behind them sits a more difficult question: how do complex infrastructures remain stable when pressures intensify, interdependencies multiply and traditional resilience assumptions no longer hold?

This Strategic Horizons edition is prepared for the participants in the webinar. It distils the main ideas from the discussion and places them in a wider, forward-looking frame that links daily secure-operations practice with the long arc of continuity governance.

From Security to Continuity

Across sectors and geographies, operators work with a similar landscape: legacy systems, expanding connectivity, constrained budgets and rising expectations. Threats move across domains, combining cyber intrusion, supply-chain weakness, misconfiguration, climate stress and human-systems fatigue. In this environment, secure operations are not only about preventing compromise. They are about sustaining function.

If Secure by Design hardens the technology, and Secure by Operations disciplines the way it is used, Secure by Continuity asks what keeps the system stable when pressure is no longer exceptional but constant.

Principles of Secure by Continuity

Continuity is systemic. Operational stability depends on suppliers, integrators, operators and public bodies acting as an ecosystem rather than as isolated actors. Most major incidents are not purely technical failures; they are coordination failures along the value chain.

Continuity is anticipatory. The most damaging events begin long before they are detected: in configuration drift, misaligned expectations, outdated baselines and lack of shared situational awareness. Anticipatory governance makes these vulnerabilities visible early and creates room for adjustment before failure.

Continuity is adaptive. As cyber, climate and geopolitical pressures intensify, continuity requires the ability to adjust configurations, behaviours and processes at a pace that matches the evolving risk. Static controls and one-off projects cannot keep up with a moving threat surface.

Where the Panel Fits in the Continuity Chain

The perspectives in the webinar trace the full continuity chain. The OEM strengthens the product layer and increases visibility into exposed assets and insecure deployments. The integrator translates design principles into real-world decisions about architecture, patching and access control. The operator maintains the daily posture that keeps systems hardened while they deliver their core mission. The policy and governance lens ties these layers together so that responsibility does not break at the seams.

When these actors coordinate around shared baselines, Secure by Operations becomes something larger than a checklist. It becomes a living resilience posture.

Operational Lessons from the Field

Several practical lessons emerge from the experiences shared by the panelists. Awareness and culture determine the uptake of secure practices more than technology alone. Operators engage more strongly when security measures are pragmatic, contextual and clearly connected to real risk rather than to abstract rules. Integrators succeed when they balance production uptime with targeted mitigation instead of applying blanket controls. OEMs carry responsibility not only for secure product design but also for supporting secure lifecycle behaviour and providing usable guidance.

These lessons point to a simple conclusion: continuity emerges from practice, not from aspiration. It is built in the small, repeated decisions that determine how systems are configured, maintained and recovered.

The Governance Horizon

Europe's evolving regulatory landscape – including DORA, the Cyber Resilience Act and NIS2 – is quietly shifting the logic of cyber governance. Compliance is no longer the primary organising principle. Stability is. The new frameworks increasingly expect lifecycle security rather than one-off implementation, cross-border visibility rather than national silos, explicit supply-chain awareness rather than narrow organisational focus, and continuous learning rather than static certification.

This environment creates the conditions for Secure by Operations to evolve into Secure by Continuity. Organisations that treat the new rules as a catalyst for integrated resilience, rather than as separate compliance burdens, will be better placed to withstand compound shocks.

Continuity in a 3°C World

As the climate warms and global instability accelerates, critical infrastructure will experience compounding stress: heatwaves, floods, grid instability, migration pressures, cyber operations by state and criminal actors, and physical sabotage. These are not distant scenarios; they are emerging features of the operating baseline.

Secure by Continuity positions organisations to cope with this environment by focusing on early signals of degradation, coordinated response rhythms, cross-value-chain accountability and the ability to maintain stability under accelerated pressure. In this sense, continuity becomes a backbone of societal resilience, not only an internal objective for individual operators.

Closing Perspective

Secure by Design protects the technology. Secure by Operations protects the environments in which that technology runs. Secure by Continuity protects society.

The future of critical infrastructure will depend on whether its stewards – suppliers, integrators, operators and authorities – see themselves not as separate entities but as interdependent custodians of continuity. The work discussed in this webinar is one part of that larger strategic shift.

About ERPI and PerilScope

The European Risk Policy Institute (ERPI) is an independent strategic institute dedicated to advancing risk-policy thinking, continuity governance and systemic-resilience strategies across Europe and globally. ERPI develops frameworks, advisory methodologies and futures analysis to support governments, international institutions, critical-infrastructure operators and private-sector leaders in navigating accelerating cyber-physical, climate and geopolitical pressures.

ERPI's work builds on the Strategic Risk Policy® doctrine of the Australian Risk Policy Institute (ARPI) and extends it into the 3°C World Strategic Risk Policy® (3CWSRP®) framework — a forward-looking approach designed for a century defined by convergence, interdependence and non-linear risk.

PerilScope is ERPI's analytical and strategic-foresight platform. It interprets global developments through a resilience lens, connecting operational realities with strategic horizons. PerilScope editions integrate geopolitical signals, climate risk, cyber-physical threats, regulatory shifts, systemic fragility and narrative intelligence.

Together, ERPI and PerilScope provide a coherent architecture for understanding the world not only as it is, but as it is becoming — enabling organisations to move beyond compliance toward strategic resilience and long-term continuity.