



ENCORE WEBINAR PRESENTATION
9 SEPTEMBER 2026
Originally presented at OTCS '26

SPONSORED by ISAGCA
OT Cyber Insurance and Risk
Transfer: Right-Sizing Coverage
Using Evidence, Not Guesswork

Rébiah Bardot-Girard, AXA XL
José Seara, DeNexus



International Society of Automation
Setting the Standard for Automation™

© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

ISA GLOBAL
CYBERSECURITY
ALLIANCE

ISASecure

OT Cyber Insurance and Risk Transfer: Right-Sizing Coverage Using Evidence, Not Guesswork



Rébiah Bardot-Girard
Head of Cyber Risk
Consulting Services, **AXA XL**



José Seara
Founder and CEO,
DeNexus

**This workshop is
sponsored by**



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.



**ISA GLOBAL
CYBERSECURITY
ALLIANCE**

OT Cyber Insurance Is Being Bought on Instinct, Not Evidence



Coverage sized by benchmarking peers,
not by actual loss exposure



Exclusions and sub-limits discovered
after a claim — not before



Underwriters pricing on gut feel
because OT data is opaque



Boards approving retention levels
without understanding what they're retaining

"The question is no longer whether to buy cyber insurance. It's whether what you've bought actually covers your risk."

Three Forces Are Converging — Evidence Is the Differentiator

01



Hard Market Pressure

OT-specific exclusions are expanding. Premiums are rising. We are seeing 15–25% premium differentials between organizations that bring quantified evidence and those that don't. Evidence is now a negotiation lever.

02



Boards Need Numbers

Your board asks four questions after every incident: Were we safer? How much safer? Within risk appetite? What was the ROI? Your underwriter asks the same four. Neither is satisfied with a heat map.

03



OT Loss Is Now Visible

Clorox: \$356M in disclosed losses (2023 10-Q). Colonial Pipeline: \$4.4M ransom, operations halted. JLR: production stopped across multiple plants. OT cyber loss is no longer hypothetical — it is actuarial.



Three Decisions. One Sequence. Infinite Clarity.



DECIDE 01

Mitigate

Reduce probability or impact before transferring risk

- High-likelihood, quantifiable scenarios
- Controls with measurable risk reduction
- Mitigation roadmap linked to underwriting outcomes



DECIDE 02

Retain

Set retention levels based on scenarios you can afford to self-insure

- Scenarios below your retention threshold
- Risks where insurance cost > expected loss
- Operational disruptions under recovery budget



DECIDE 03

Insure

Transfer residual tail risk after mitigation and retention are defined

- Catastrophic / low-frequency scenarios
- Scenarios exceeding retention appetite
- Regulatory and contractual requirements

The sequence matters: mitigate first, set retention second, insure the residual — not the other way around.



What Underwriters and Boards Actually Respond To



Portfolio View

Asset inventory mapped to business process criticality. Not a technology list — a revenue-at-risk view. Which OT systems, if compromised, stop production?



Quantified Loss Scenarios

3–5 named scenarios (e.g., ransomware on DCS, supply chain compromise, remote access exploit) with estimated direct loss, recovery cost, and downtime.



Control Effectiveness Evidence

Not a controls checklist. A demonstrated link between controls in place and reduction in scenario probability or impact — expressed in dollars.

What NOT to bring

- ✗ A maturity score or framework compliance certificate
- ✗ A list of security tools deployed
- ✗ A qualitative risk heat map
- ✗ Last year's pen test report
- ✗ IT-centric metrics applied to OT environments

DeNexus produces all three evidence elements automatically — portfolio view, quantified scenarios, and control effectiveness —



What We Actually See — And What Changes the Conversation

What Creates Friction

- No asset inventory — we're pricing blind
- IT-only metrics presented as OT risk
- Framework scores with no loss translation
- Limits set by broker benchmark, not exposure
- No explanation of OT network architecture

What We Ask For (and rarely get)

- Which systems stop production if compromised?
- What's the realistic recovery timeline per system?
- What controls are in place — and tested?
- Has segmentation been validated post-deployment?
- What third-party access exists to OT networks?

What Changes the Conversation

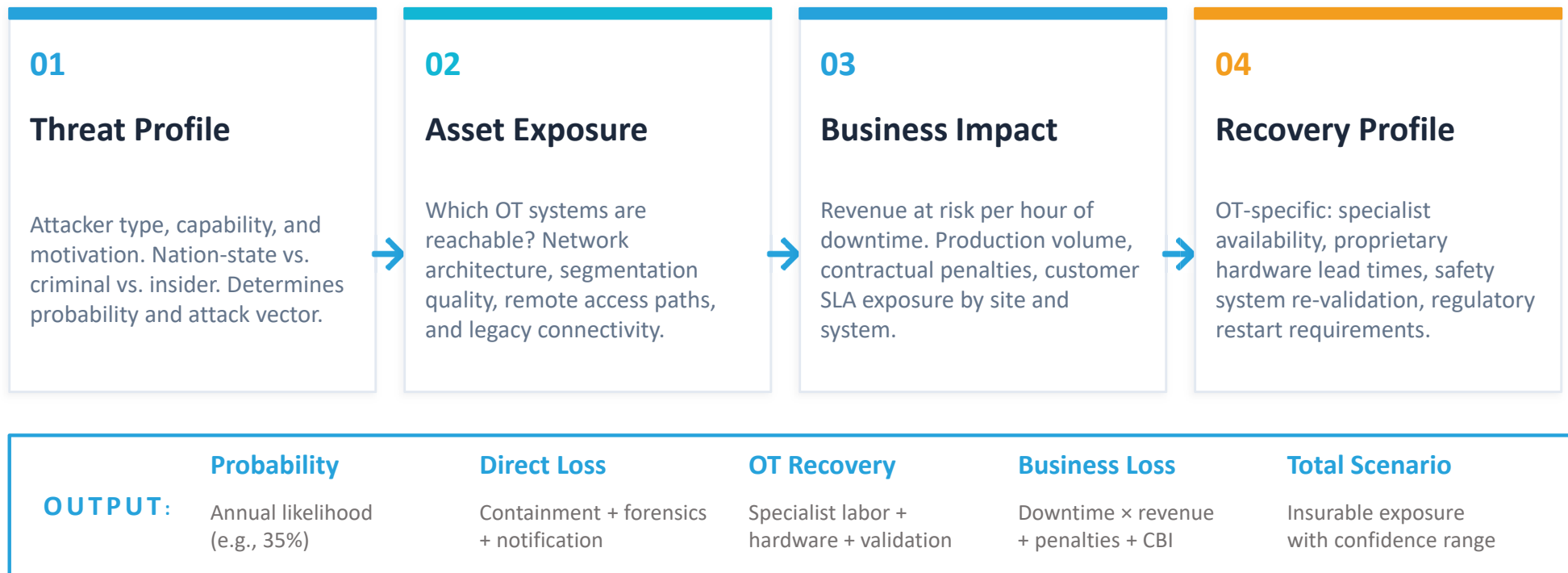
- Quantified loss scenarios with named assumptions
- OT asset map linked to revenue exposure
- Control effectiveness expressed in \$ impact
- Mitigation roadmap with timeline and owner
- Policy review showing you've closed prior gaps

"The best submissions we receive read like a risk management strategy, not an insurance application." — AXA XL Underwriter



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

From OT Architecture to Financial Loss: The Four-Input Method



Ransomware on DCS — Step by Step

€800M Manufacturer, Primary Facility

STEP 1

Define the threat

Criminal ransomware group. Financially motivated. Entry via spear-phishing of engineering workstation. Known OT capability — deploys OT-specific payload post-access.

Annual probability: 35%

STEP 2

Map the blast radius

Engineering workstation has IT/OT boundary access. DCS historian reachable via flat network segment. 3 production lines share the historian. All 3 lines halt on DCS encryption.

Systems affected: 3 of 5 production lines

STEP 3

Calculate business loss

€800M annual revenue. Primary facility = 60% of output. 3 affected lines = 70% of primary facility. Downtime revenue loss: $€800M \times 60\% \times 70\% \div 365 = €916K/day$.

Downtime loss: ~€916K/day

STEP 4

Add OT recovery costs

OT specialist: 2 engineers $\times$ 3 weeks $\times$ €3K/day = €126K. Hardware replacement: €80K. DCS vendor re-commissioning: €95K. Safety system re-validation: €120K. Total OT recovery: €421K.

OT recovery: ~€421K (fixed cost)

T1 — IR + forensics: €0.38M | T2 — OT disruption/downtime: €16.5M | T3 — OT recovery: €0.42M | 18 days • TOTAL: €17.3M



How to Size Coverage Using OT Loss Scenarios

Scenario	Probability (Annual)	Direct Loss	Recovery Cost	Total Exposure	Decision
Ransomware on DCS (Primary Site)	35%	\$6.2M	\$3.1M	\$9.3M	INSURE
Remote Access Compromise	22%	\$1.8M	\$0.9M	\$2.7M	RETAIN
Supply Chain Software Implant	8%	\$14.5M	\$6.2M	\$20.7M	INSURE
Insider Threat — Config Manipulation	18%	\$0.4M	\$0.3M	\$0.7M	MITIGATE
Total Insurable Exposure: \$30.0M Recommended Coverage Limit: \$25M Retention: \$2M					



Linking Mitigation Roadmaps to Better Quantify Outcomes

BEFORE MITIGATION

Ransomware on DCS

Annual Probability: 35%

Expected Annual Loss: \$3.26M

Scenario Total Exposure: \$9.3M



AFTER MITIGATION (network segmentation + OT EDR)

Same Scenario, Improved Position

Annual Probability: 18% ↓49%

Expected Annual Loss: \$0.99M ↓70%

Scenario Total Exposure: \$5.5M ↓41%

\$235K/year premium savings · \$300K mitigation investment · 15-month payback · before counting avoided loss reduction



The Minimum Viable Submission: What's In It and How to Build It

01 Executive Summary (1 page)	02 OT Asset & Exposure Map (2 pages)	03 Scenario Analysis (1 page / scenario)
Risk appetite statement Board-approved retention level and rationale	Site inventory Each site: OT systems, connectivity, revenue at risk per day	Scenario definition Threat actor + attack vector + affected systems
Top 3 scenarios Named, with total exposure and decision (insure/retain/mitigate)	Network architecture summary Segmentation status, remote access inventory, IT/OT boundary controls	Loss build Downtime loss + OT recovery + forensics + third-party
Coverage ask Limit, retention, endorsements requested	Critical path analysis Which systems halt production — and what the financial impact is	Probability basis Source data / methodology / confidence level
Year-over-year delta What changed in your risk profile since last renewal	Third-party access log All vendor/integrator access paths with current status	Control state What's in place — and what it does to probability and impact

Full Evidence Pack Checklist available as leave-behind — includes section templates, field definitions, underwriter review notes.



The Framework Is Universal. The Scenarios Are Not.

Energy & Power

Top scenario: Grid destabilization via SCADA compromise

Typical exposure: **€20–80M+**

Recovery range: **4–12 weeks**

⚠ War exclusion applies to nation-state attribution — explicitly common in energy targeting

Manufacturing

Top scenario: Ransomware halting production lines

Typical exposure: **€5–25M**

Recovery range: **2–6 weeks**

⚠ Sub-limit for OT recovery frequently triggered — proprietary hardware costs misclassified as IT

Oil & Gas

Top scenario: Process control manipulation / safety system targeting

Typical exposure: **€15–100M+**

Recovery range: **6–20 weeks**

⚠ Environmental liability from process disruption often uninsured under cyber policy

Rail & Maritime

Top scenario: Navigation / signaling system compromise

Typical exposure: **€8–40M**

Recovery range: **3–10 weeks**

⚠ Liability to third parties (passengers, cargo) often requires separate marine/rail rider



Your Evidence Pack Pays Twice: One Build.

NIS2 Article 21	Cyber Resilience Act	COVERED BY YOUR EVIDENCE PACK
✓ Risk analysis and information system security policies	✓ Security by design and default	✓
✓ Incident handling and business continuity	✓ Vulnerability management throughout lifecycle	✓
✓ Supply chain security including vendor risk	✓ Incident reporting to ENISA	✓
✓ Vulnerability handling and disclosure	✓ Security documentation for conformity assessment	✓
✓ Use of multi-factor authentication and encryption	✓ Software bill of materials (SBOM) for connected products	✓

Key insight: The evidence pack you build for your insurer — scenarios, portfolio view, control effectiveness — satisfies NIS2 Article 21 and CRA conformity in the same workflow. One build, two audiences. If your security team is producing separate documentation for each, that is a process problem worth fixing before the next renewal cycle.



What You Can Do on Monday



This week

Run the three-decision test

Take your top 5 OT assets. Ask: if each were compromised, what's the financial impact? Assign each to Mitigate / Retain / Insure. The gaps become obvious.



This month

Audit your current security posture

Map your OT controls to your top 3 scenarios. For each: Are recovery timelines documented? Is third-party access inventoried? Gaps will be spotted by your underwriter



Before renewal

Build your evidence pack

Assemble the three elements: portfolio view, 3–5 quantified scenarios, control effectiveness. Use our checklist (next slide) as your starting structure.



Budget cycle

Link mitigation to premium

For every security investment in your roadmap, estimate the scenario impact and calculate the insurance cost reduction. Present this to your CFO, not just your CISO.

Take-home: Evidence Pack Checklist + OT Loss Scenario Template — scan the QR code.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

WHY THIS PARTNERSHIP EXISTS

A Two-Sided Problem. One Connected Solution.

The Operator's Problem

You know your OT environment is underinsured — but you can't prove by how much.

Your board wants a number. Your broker wants a submission.
Your insurer wants evidence. You have a maturity score and a heat map.

The gap isn't awareness. It's translation — from OT reality to financial language that moves coverage.



The Underwriter's Problem

You want to write OT cyber — but you can't price what you can't see.

Submissions arrive without asset inventories, without OT network context, without loss scenarios. You're underwriting narrative, not risk.

The gap isn't appetite. It's data — structured, quantified, OT-native evidence that your actuarial models can consume.

DeNexus produces the evidence. AXA XL acts on it. What follows is how each side works.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

DeNexus - Quantify. Reduce. Transfer.

QUANTIFY + MITIGATE

DeRISK™ CRQ

Translate OT cyber exposure into financial risk currency. Simulate mitigation projects before you spend the money.

AEL · VaR · Loss curves · Mitigation ROI · Evidence pack

300+ deployments

REDUCE

DeRISK™ QVM

Every CVE ranked by expected dollar loss — not CVSS. Identify the 1–2% of vulnerabilities driving 90% of actual risk.

\$ per CVE · ATT&CK mapping · Remediation ranking · ROI per patch

200+ deployments

TRANSFER

DeRISK™ UWA Agentic

Five AI agents deliver full actuarial underwriting output in 10–20 minutes. The insurer side of the evidence chain.

EL · MFL · Loss curves · Premium indication · Audit trail

GA · May 2026

The sequence matters: quantify your exposure, reduce what you can, transfer the residual — not the other way around.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

The Evidence Engine — and the Mitigation Simulator

What It Does

- Translates OT cyber exposure into AEL and VaR — facility by facility, bottom-up to portfolio
- Powers the three decisions: which risks to mitigate, which to retain, which to insure
- Simulates mitigation projects before you spend — CapEx/OpEx inputs, ROI output per project
- ML-powered MRS recommends highest risk-reduction / highest-ROI projects automatically
- Produces the evidence pack underwriters and boards both accept

Under the Hood

- URMS engine — proprietary deterministic probabilistic model (NoA + APA + LEI + CoEXP)
- 50 million simulations per site per assessment cycle
- DNX CSF control framework — inspired by ISA/IEC 62443, native to OT
- Integrations: Dragos · Claroty · Nozomi · Forescout · Tenable · PANW · Fortinet
- Outputs: AEL, VaR, loss exceedance curves, mitigation report, what-if scenarios

300+ deployments · US & EU · 4 sectors

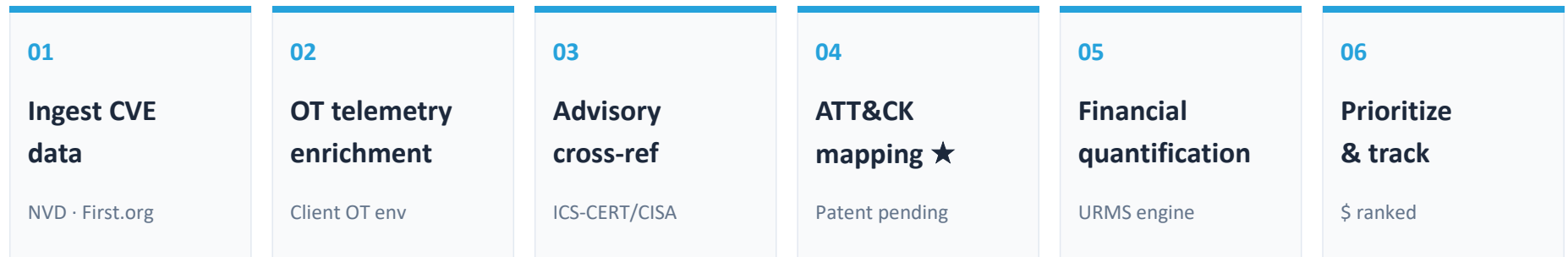


Every CVE in Dollars, Not Scores

1–2%

of vulnerabilities drive 90% of actual risk.
QVM finds them — in dollars.

The 6-Stage Enrichment Pipeline



200+ deployments · Patent-pending CVE → ATT&CK for ICS auto-mapping

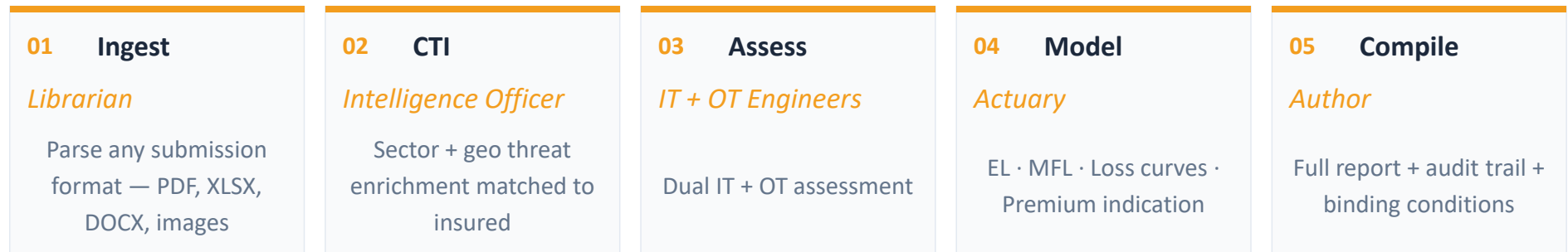


Augment Your Underwriting Team with OT Cyber Specialist Capability — Without Hiring One

10–20 min

vs. 10–30 hours manual

Five-Agent Pipeline + Orchestrator Agent



→ Sound of Silence = risk signal → 28 regulatory requirements mapped → Pre-trained on 10+ questionnaires → Replaceable actuarial model

GA · May 2026 · Agentic AI — not a co-pilot · Human always in the loop





X^L Insurance

Cyber Risk Consulting Services

Proactive services

2026



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Building better security, day in, day out

At AXA XL, we believe that effective cyber risk management involves more than just reacting to incidents, we focus on prevention and resilience.

Our Cyber Risk Consulting team guides you through four key phases:

Prevent by using predictive analytics and risk assessments to identify potential threats.

Prepare by implementing proactive monitoring and cybersecurity education to strengthen your organization. Then,

Protect by reinforcing your defenses against attacks.

Prevail by enhancing your cyber resilience to minimize disruption and recover quickly. Together.

Four pillars for elevating your security maturity

A comprehensive approach to safeguarding your business at every stage, delivered via our Cyber Risk Consulting team.



Prevent

We continuously assess your security maturity, uncover emerging risks and help you shape a proactive cyber strategy that keeps you ahead of threats.

- Continuously rating your cyber security performance
- Managing compliance risks across IT & OT systems
- Advising strategically on emerging threats
- Safeguarding against data breaches at every opportunity



Prepare

We work with you to identify vulnerabilities, anticipate attacks and equip your people and systems to stay ready for whatever comes next.

- Delivering robust training and awareness programmes
- Hardening cyber defences against evolving attacks
- Monitoring threats and data leaks in real time



Protect

We work with you to defend your critical assets, evolving protections as risks change and equipping you with insights and tools to strengthen your security posture.

- Detecting, monitoring and blocking attacks as they unfold
- Managing identity and access in a secure way
- Identifying and remediating vulnerabilities the moment they appear



Prevail

We help you respond and recover quickly, turning every incident into an opportunity to emerge stronger.

- Running diagnostics to uncover gaps
- Leading fast, expert-led incident responses
- Coaching teams through crisis management exercises
- Driving faster recovery and building lasting



End-to-end cyber expertise

AXA XL Cyber Risk Consulting is a specialised division dedicated to proactively anticipating threats, managing cyber risks, and reducing cyber exposure across the entire policy lifecycle.

As part of our ongoing commitment to delivering excellent client service, our team provides an extensive range of risk mitigation services and discounted access to leading cyber security.

Several proactive services are included in cyber policies on a complimentary basis.



Operational Technology (OT)

Services for the Industrial sector

Our value proposition for 360° OT security is grounded in widely recognized standards such as the IEC 62443 series and is developed in partnership with key players. Our strategy offers advantages such as leveraging our expertise and creating synergies, sharing responsibilities, optimizing resources, and providing clients with access to innovative services and solutions.

In partnership with: **Deloitte.** IDENEXUS™



Prevent

OT cyber governance

OT risk management & compliance

Industrial on-site audit in accordance with industry standards

Prepare

Tailored cyber-OT training & awareness

OT Intrusion tests and vulnerability assessment

Protect

OT inventory management and mapping of OT networks

Maritime inventory audit and management

OT SOC monitoring – Implementation and management of a SOC monitoring solution

Prevail

OT incident response



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Operational Technology (OT)

Prevent services

OT Onsite Industrial Audit

Overview

Identify strengths and areas for improvement, prioritize necessary controls, and provide a comprehensive view of the cybersecurity maturity level of the industrial environment

What value provide to our client's risk?

- Identification of the most critical assets.
- Identification of risks in the environment and vulnerabilities affecting the assets.
- Documenting the current state to serve as future reference points for determining the security status and level of each asset.
- Compliance with regulations and an overview of the security compliance or maturity level compared to other companies in the same sector.

Location

- France/Morocco

How it works

- **Review of documentation:** Collect the relevant deliverables concerning cybersecurity. Analyse the documentation related to industrial systems. Understand the topology and architecture of IT and OT networks.
- **Site visits:** Conduct interviews to identify the level of cybersecurity maturity on-site based on a dedicated framework. Examine local facilities and physical security controls. Identify vulnerabilities present in industrial systems (workstations, IT/OT firewalls, MES, DCS).
- **Summary of strengths and gaps:** Establish risk scenarios. Formalize recommendations for identified non-conformities. Provide details on findings and general recommendations.

Deliverables

- Summary of interviews
- Maturity level of sites based on the framework
- Audit report

Supported by

Deloitte.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Operational Technology (OT)

Prepare services

OT Awareness and Training

Overview

Improve the level of knowledge and expertise in cybersecurity for managerial and operational staff involved in industrial environments.

What value provide to our client's risk?

- Provide employees with an overview of industrial cybersecurity by training them in best security practices
- Enhance industrial cybersecurity skills of employees with access to critical systems by aiming to provide them with the necessary tools and knowledge to manage cybersecurity risks and incidents.
- Train employees to identify vulnerabilities in industrial systems, implement effective protection measures, and respond appropriately in case of an incident.

Location

- France/Morocco

How it works

- **Content preparation for the targeted audience:** Conduct meetings to understand awareness needs and target teams. Conduct a study/interviews to understand employee habits and identify risky behaviours. Define and validate awareness and training materials.
- **Industrial Cybersecurity Awareness:** Facilitate awareness sessions using examples from their ecosystem. Engage participants through quizzes and practical exercises. Enable internal trainers to independently deliver the awareness program using the provided.
- **Enhancement of Industrial Cybersecurity Skills:** Present the principles, standards, and vulnerabilities of critical components, protocols, and networks in industrial environments. Explain secure configurations, network segmentation, and access management. Present real case studies and incident simulations.

Deliverables

- Awareness support materials
- Training support materials

Supported by

Deloitte.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Operational Technology (OT)

Prepare services

OT Vulnerability Assessment

Overview

Identify and exploit vulnerabilities in systems in the industrial environment to assess their level of security and criticality to operations and enable the implementation of corrective measures

What value provide to our client's risk?

- Proactive identification of vulnerabilities and security gaps in the industrial environment and interconnections with IT.
- Mitigation of operational and financial risks from potential cyber attacks.
- Analysis of detection and incident response capabilities through conducted penetration tests.
- Identification of the attack surface of the industrial environment.
- Providing recommendations related to identified vulnerabilities.

Location

- France/Morocco

How it works

- **State of Ecosystem:** Collect the results of penetration tests and risk analyses conducted previously. Conduct an inventory of all critical objects and examine the associated access levels. Review existing policies, standards, and procedures.
- **Penetration Testing on Industrial Systems:** Network scan of accessible equipment and analysis of exposed services. Review of communication protocols used and attempts at interception. Execution of test scenarios defined according to the sensitivity of the assets present and their resilience.
- **Report of tests and attack surface:** Represent relevant attack paths based on identified vulnerabilities. Formalize the analysis report including vulnerabilities, attack scenarios, and associated risks. Present the test results by detailing the criticality of identified vulnerabilities and actions to be taken.

Deliverables

- Penetration test report
- Documentation of evidence

Supported by

Deloitte.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Operational Technology (OT)

Protect services

Maritime Inventory Management and Security Audit

Overview

Identify assets, assess compliance level with regulations, and mitigate associated risks for the company and its clients, at sea and on shore.

What value provide to our client's risk?

- Obtain a view on the level of regulatory compliance (e.g., NIS2, E26-E27, ISPS, etc.).
- Exhaustive inventory of physical and software assets on each vessel, including versions and any identified vulnerabilities.
- Photos that can serve as a future reference to determine the exact location of each asset on board the vessel, as well as its configuration (connections, attached devices, serial numbers, etc.).
- A cartography of the onboard IT system and the links between its various components.

Location

- France/Morocco

How it works

- **Preparation for vessel visit** and analysis of documentary prerequisites. Formalization of the data exchange protocol. Planning of interviews and vessel visits with various stakeholders.
- **Asset analysis and compliance level:** Mapping of IT/OT flows and assets on vessels. Assessment of the cyber maturity level of each vessel. Reporting of the most critical identified points. Concluding presentation for each vessel.
- **Presentation and validation of findings:** Consolidation of results across all fleet. Deployment of dashboards for tracking identified assets by vessel. Presentation per vessel of IT/OT system hierarchies. Closure presentation with different stakeholders.

Deliverables

- Input for CMDB, inventories, updated handbooks
- Dashboard of discovered assets
- Final executive report

Supported by

Deloitte.



Operational Technology (OT)

Protect services

Study, Implementation, and Management of solutions

Overview

Build, configuration and run of security solutions tailored to industrial environments.

What value provide to our client's risk?

- Automated asset discovery and classification
- Continuous monitoring to detect unauthorized changes or assets.
- Segmentation of OT networks to prevent lateral movement of threats.
- 24/7 monitoring of OT networks to detect OT-specific threats.
- Protection of OT endpoints against malware, ransomware, and unauthorized access.
- Behavioural analysis to detect unusual activity on critical endpoints.

Location

- France/Morocco

Supported by

Deloitte.

How it works

- **Review of solutions:** Understanding of the current situation and challenges through architecture review and conducting interviews. Comprehensive review of market solutions and in-depth evaluation of 2 shortlisted solutions based on identified needs. Validation of the chosen solution that best meets the needs.
- **Solution implementation (Build):** Definition of functional and technical architecture, target governance, solution implementation plan, and tracking indicators. Configuration of the solution to meet the needs. Establishment of necessary connections between the solution and the ecosystem.
- **Solution management (Run):** Start of solution operations. Service stabilization. Continuous review of the solution's performance. Monitoring through operational governance bodies. Adjustment of tracking indicators and configuration if needed.

Deliverables

- Study report
- Continuous reports on the functioning of the solution



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Operational Technology (OT)

Prevail services

OT SOC

Overview

Integration of OT Security Operations, which ensure the secure and reliable functioning of industrial systems, with the OT SOC, responsible for real-time threat monitoring, incident detection, and response to cyberattacks.

What value provide to our client's risk?

- **Reduced Downtime:** Proactive monitoring and rapid response prevent cyber incidents from escalating into costly physical production halts.
- **Complete Visibility:** Automated asset discovery eliminates security "blind spots" by identifying and tracking every device on the OT network.
- **Regulatory Alignment:** Continuous compliance mapping reduces the risk of legal penalties and safety failures by meeting standards.

Location

- France/Morocco

How it works

- **Monitoring & Detection:** Integration into Deloitte's existing SOC. 24/7 monitoring of OT networks to detect cyber threats specific to OT systems. Integration with threat intelligence feeds for continuous improvement of playbooks and detection rules
- **Incident Response:** Real-time incident response using SIEM and IDS/IPS solutions. Prioritization and escalation of incidents based on the impact on operations, with defined workflows. Forensic analysis and root cause investigation on OT devices and networks.
- **Endpoint Protection:** Protection of OT endpoints against malware, ransomware, and unauthorized access. Behavioural analysis to detect unusual activities on critical endpoints. Centralized management of OT-specific endpoint security tools.

Deliverables

- 24/7 Monitoring & Alerting
- Asset & Vulnerability Reports
- Incident Response & Remediation

Supported by

Deloitte.



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.

Thank You

Questions & Discussion

To continue the conversation:

→ Request a DeRISK CRQ scoping conversation

[QR Code]

→ Obtain your OT cyber insurance readiness assessment

→ Get the Evidence Pack Checklist + Scenario Template

Scan for Evidence Pack

"OT cyber risk is quantifiable. Your next renewal can be different."

DE^NEXUS™



© Copyright International Society of Automation (ISA) 2026. All rights reserved. Content provided as part of the ISA OT Cybersecurity Summit (17-18 June) — Prague, Czech Republic. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by means, electronic, mechanical, photocopying, recording or otherwise, without the publisher's prior written permission.