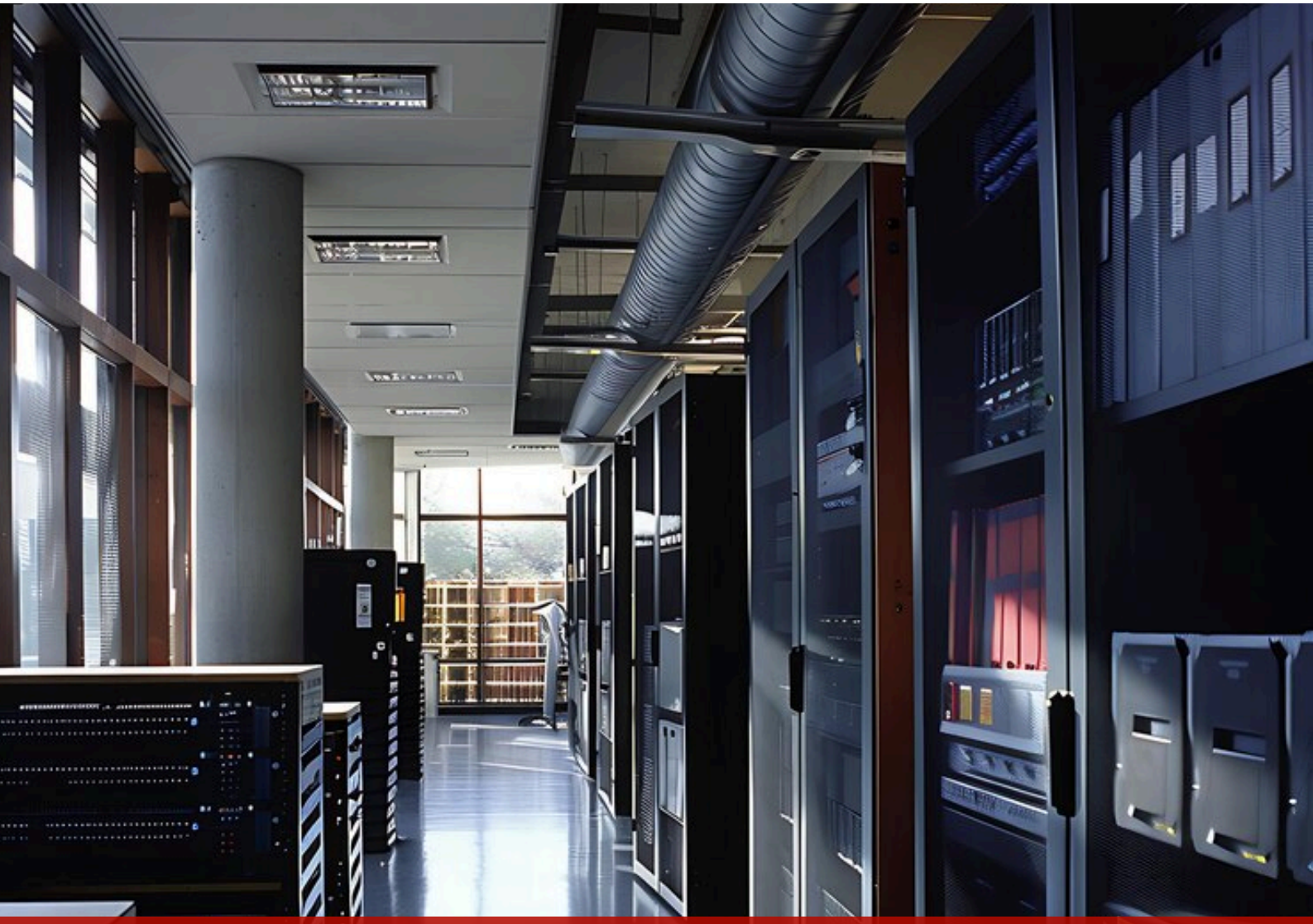
ÆGIS

TRUST THE EDGE



INTEGRATING IT AND OT SECURITY

Advancing Cybersecurity Across Industrial and IT Ecosystems

DAVIDE BERETTA

INCIDENT RESPONSE SPECIALIST

WWW.AEGIS-OT.COM

AEGIS

PREFACE

Today's industrial enterprises face an expanded risk surface as OT networks converge with IT infrastructure. Operational environments that once relied on physical segmentation and implicit trust must now contend with sophisticated adversaries, legacy constraints, and cloud-integrated architectures.

ÆGIS presents this expanded technical briefing to help enterprise defenders, engineers, and decision-makers align on an updated model for modern cybersecurity across interconnected domains.

SECTION I — CONVERGENCE AS ATTACK SURFACE: AN ENGINEERING PERSPECTIVE

The traditional IT/OT divide is no longer viable. Manufacturing execution systems (MES), historians, and SCADA environments now route data to cloud analytics platforms and centralized dashboards. This increases productivity—but also introduces bidirectional threat vectors.

Technical Factors:

- OT devices often use insecure or proprietary protocols (e.g., Modbus, DNP3, BACnet).
- Systems designed with physical safety, not cybersecurity, in mind are now routable via TCP/IP.
- Vulnerability management is hindered by limited patch cycles, vendor constraints, and system criticality.
- Remote access, frequently introduced during the pandemic for business continuity, remains largely ungoverned.

Result: Operational environments become attractive lateral movement zones after an initial IT compromise.

SECTION II — VULNERABILITY ≠ EXPLOITABILITY: WHY CVSS MISLEADS IN ICS

A vulnerability's severity in IT does not directly translate to criticality in OT. In fact, ÆGIS research has shown that over 60% of CVEs affecting industrial systems do not result in materially increased process risk.

Critical Considerations for OT Risk Assessment:

- Is the vulnerable component in the critical path of a physical process?
- Can the vulnerable device be exploited remotely?
- Would exploitation cause functional disruption, safety risks, or just a nuisance alert?

Shift in Thinking: Prioritize threats based on **process impact analysis** , not just CVSS scores. Security decisions must be made in partnership with engineering.

Case Insight: ÆGIS documented a case in which a high-CVSS-rated buffer overflow in an HMI posed minimal risk because the HMI had no control capability. Conversely, a low-rated flaw in a protocol stack enabled replay attacks on a PLC with direct control over boiler pressure—highly consequential.

SECTION III — ADVANCED ADVERSARIES: WHAT ÆGIS SEES IN THE FIELD

From 2023–2025, ÆGIS observed a notable increase in:

- Nation-state operators moving beyond espionage to pre-positioning for kinetic disruption.
- Ransomware operators targeting industrial companies for extortion, using OT shutdowns as leverage.
- Supply chain compromises at the firmware and hardware level (e.g., embedded backdoors in IIoT devices).

TTPs Include:

- Living-off-the-land via remote management tools (TeamViewer, RDP, VNC)
- Lateral movement via Active Directory trust relationships to engineering workstations
- Deployment of ICS-aware malware frameworks
- Hiding in engineering logs or exploiting trust in USB engineering tools

Example Case: An attacker exploited a misconfigured engineering workstation to alter HMI logic and trigger an unplanned shutdown at a critical infrastructure facility. Dwell time: 9 months. Discovery occurred only after physical process anomalies prompted investigation.

SECTION IV — FROM DETECTION TO CONTAINMENT: A MORE PRACTICAL RESPONSE MODEL

Borrowing IT's 1-10-60 response model for detection, investigation, and remediation is aspirational—but often unrealistic in OT. Instead, ÆGIS promotes the **0-Detect, 0-Contain, X-Remediate** model for ICS:

- **0-DETECT:**
  Aim for early, passive anomaly detection using context-aware baselining.
- **0-CONTAIN:**
  Pre-stage containment plans with segment isolation, fail-safes, and manual overrides.
- **X-REMEDIATE:**
  Accept that remediation timelines will vary, but plan them as if safety and uptime are both top-tier objectives.

Incident Drill: ÆGIS simulations show that the average response time in OT—without pre-planning—is over 36 hours. With structured containment workflows, it drops to under 4.

SECTION V — PHYSICS-AWARE SECURITY: THE FORGOTTEN LAYER

Cybersecurity in ICS must account for the physical consequences of digital actions.

Examples:

- Manipulating a setpoint for an exothermic reaction can cause an explosion.
- Interfering with a centrifuge's RPM sensor may cause imbalance and mechanical failure.

Security teams must partner with process engineers to:

- Map digital assets to physical consequences.
- Simulate "what if" scenarios for cyber-initiated process deviations.
- Implement alarms not just for IT events, but for anomalous physical readings triggered by cyber means.

Bottom Line: Understand the control loop. Secure the logic layer, not just the network.

SECTION VI — WHERE TO START: AN ÆGIS-PROVEN MATURITY PATH

INVENTORY EVERYTHING

Include sensors, actuators, protocols, software versions, and interdependencies.

ESTABLISH VISIBILITY

Use passive ICS protocol analysis and anomaly detection—don't scan or probe.

THREAT HUNT REGULARLY

Deploy experienced analysts to trace dormant adversaries or misconfigurations.

INTEGRATE ENGINEERING AND SECURITY

Establish change management procedures for logic changes.

BUILD A KNOWLEDGE EXCHANGE

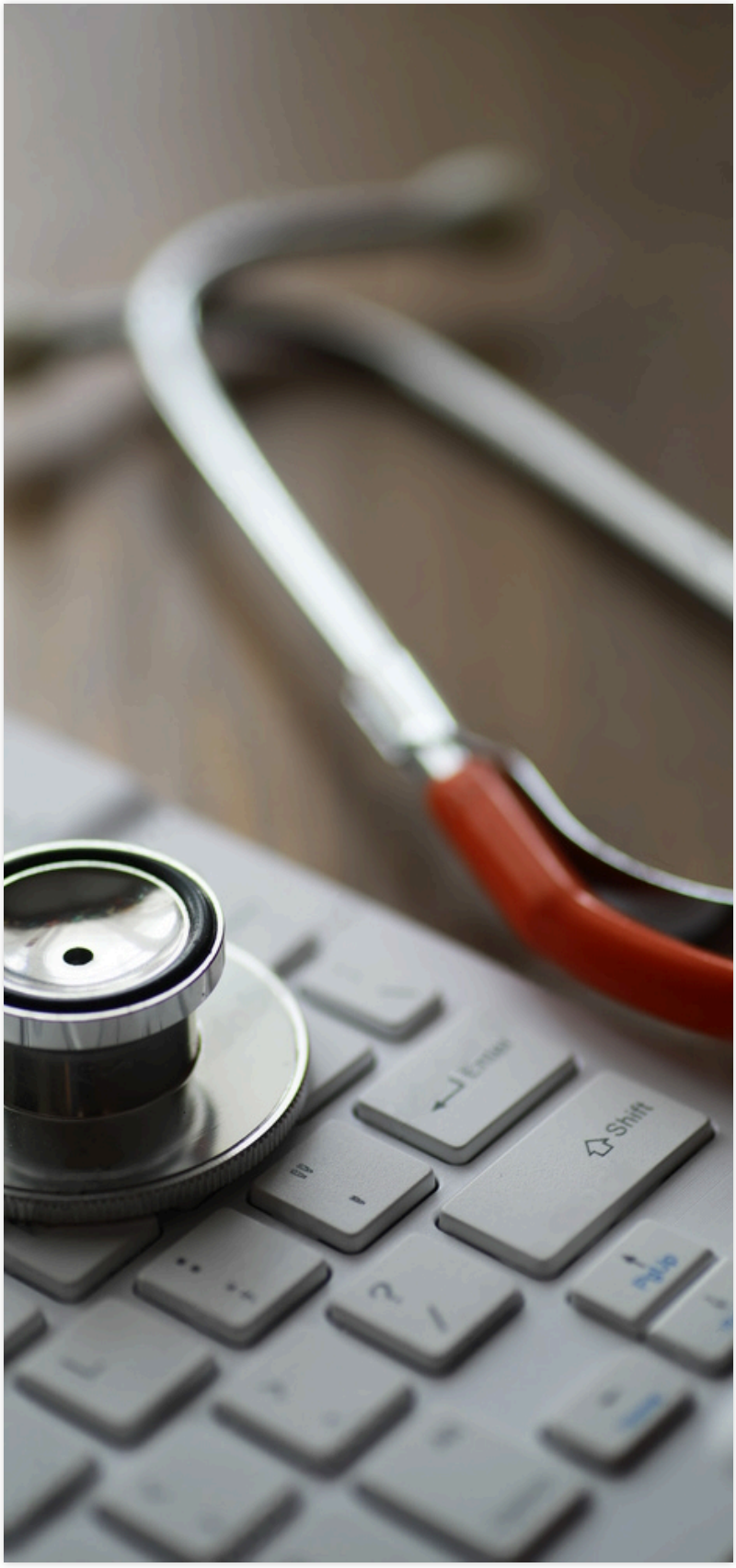
Cross-train engineers in cyber principles and analysts in industrial logic.

FORMALIZE OPERATIONAL-CYBER COMMITTEES

Governance matters. Create a joint oversight mechanism for safety and security decisions.

DEVELOP INCIDENT PLAYBOOKS

Tailored not only by asset type, but by process consequence.



ÆGIS Services often begin with a passive, zero-disruption visibility deployment, followed by a red team emulation of ICS-specific adversary behaviors.

SECTION VII — TECHNICAL DEFENSE IN DEPTH: REAL CONTROLS THAT WORK

Network Layer:

- Deep packet inspection with OT protocol support (e.g., Modbus, EtherNet/IP)
- Industrial demilitarized zones (IDMZs) and strict firewall rules
- VLAN separation of engineering workstations and controllers

Host Layer:

- Application whitelisting (e.g., only allow certified engineering tools)
- Firmware integrity validation on PLCs and RTUs
- Secure boot and cryptographic signatures for runtime integrity

Logical Layer:

- Role-based access with enforced separation of duties
- Logging and tamper detection for logic uploads and firmware changes
- Multi-factor authentication for logic deployment

Process Layer:

- Independent safety instrumented systems (SIS)
- Process anomaly alarms cross-referenced with cyber alerting
- Manual override switches and mechanical safeties

Bonus Tip: Include OT cyber risks in your business continuity planning—not just disaster recovery.

SECTION VIII — FUTURE SHIFTS: PREDICTING THE NEXT THREE YEARS

ÆGIS anticipates these key developments:

CONVERGENCE OF SIEM AND HISTORIAN DATA

Correlated analytics will detect both cyber and process anomalies.

WIDER USE OF DIGITAL TWINS

For sandboxed threat simulation and attack path modeling.

AUTOMATED LOGIC VALIDATION

ML-based systems will flag unusual PLC logic patterns before deployment.

INCREASED REGULATORY OVERSIGHT

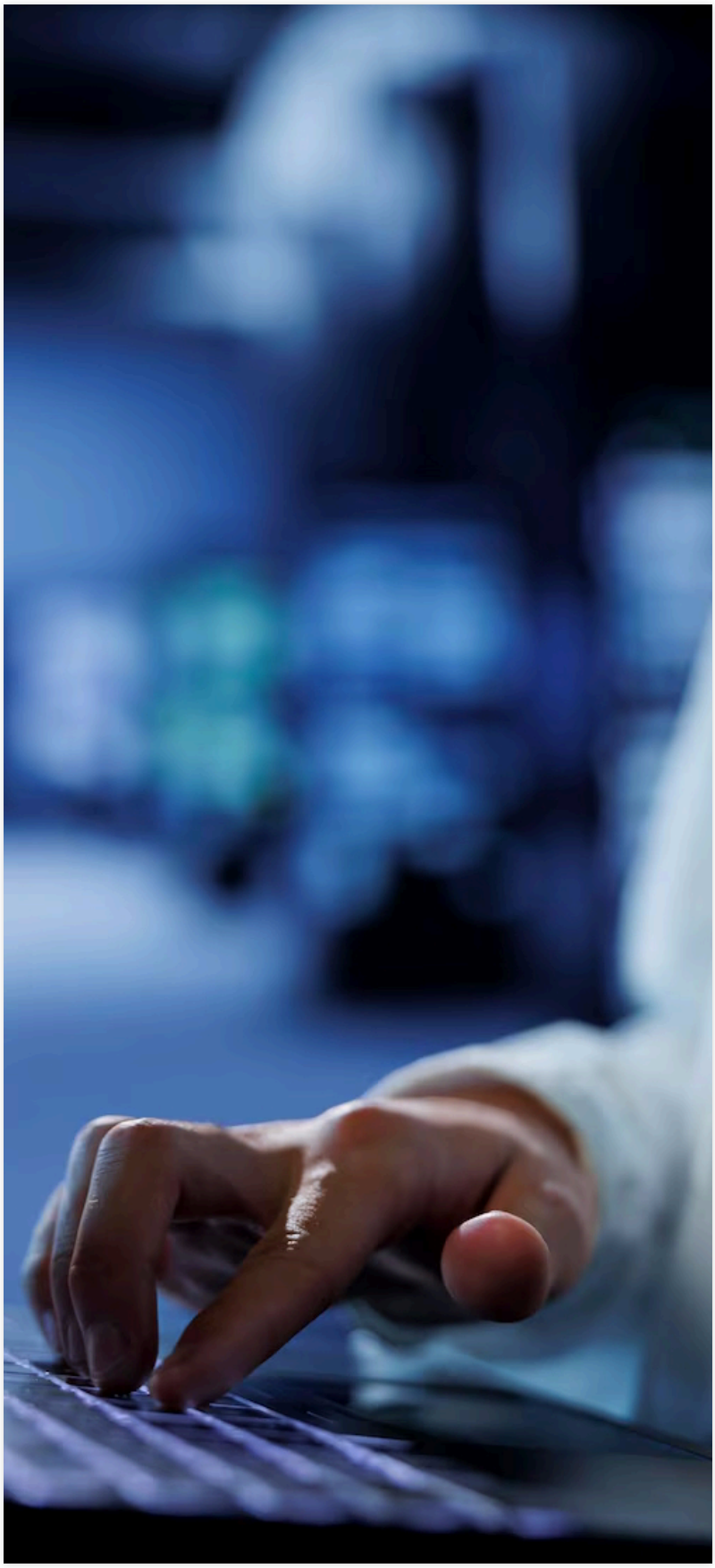
Expect NIS2-style mandates to include industrial-specific controls.

AI-DRIVEN ADVERSARIES

Script kiddies with ChatGPT-assisted malware creation will become more effective and dangerous.

OT-SPECIFIC CYBER RANGES

Companies will invest in virtualized labs for red/blue team exercises tailored to industrial processes.



FINAL THOUGHT — THE ÆGIS POSITION

Cybersecurity at the IT/OT boundary is no longer optional.

The industry must treat cybersecurity as a function of operational resilience—not a technical feature, not a compliance check, but a strategic imperative embedded in the business of making, moving, or distributing goods and services.

ÆGIS continues to build the methodologies, tools, and human partnerships that make this shift achievable—one system at a time.

To learn more or engage ÆGIS team for a readiness consultation or assessment, contact us.

ÆGIS
TRUST THE EDGE

ABOUT ÆGIS

Ægis was born from a clear mission — to bring enterprise-grade cybersecurity into the heart of operational technology. In a world where OT networks are increasingly connected, exposed, and targeted, protecting critical infrastructure is no longer optional. It's a strategic necessity. Ægis is more than a product. It's a platform built from the ground up to secure complex, distributed, real-time environments — power plants, energy transport networks, automation systems, and industrial control infrastructure. Our team combines deep field experience in cybersecurity, OT engineering, and infrastructure resilience, delivering a platform that reflects the realities of operational risk, compliance, and performance.

CONTACT

www.aegis-ot.com

info@aegis-ot.com

Aegis

THANK YOU