ÆGIS

TRUST THE EDGE

IT-ORIGINATED THREATS MITIGATION IN OT

A Modern Framework for Industrial Organizations

PIERFELICE ROCCO

SECURITY RESEARCHER

WWW.AEGIS-OT.COM

AEGIS

INTRODUCTION

The growing interconnection of Operational Technology (OT) with Information Technology (IT) is transforming industrial environments. Whether it's manufacturing, energy, transportation, or critical infrastructure, the convergence is unlocking new capabilities — but also exposing new vulnerabilities. ICS (Industrial Control Systems) environments were traditionally isolated and proprietary, but digital transformation is introducing connectivity, cloud integration, and remote access. These benefits come with expanded attack surfaces and higher stakes.

Unlike IT systems, where a breach might result in data loss or financial fraud, attacks on OT systems can disrupt physical processes, damage machinery, threaten worker safety, and impact public well-being. The need for a dedicated, structured approach to ICS/OT cybersecurity has never been more urgent. This article outlines a modern, defensible cybersecurity architecture tailored to the unique needs of industrial organizations — based on our work at ÆGIS across diverse critical infrastructure sectors.

1. DEFENSIBLE ARCHITECTURE: THE BACKBONE OF ICS/OT CYBERSECURITY

A defensible architecture refers to the design of systems in a way that limits potential damage, facilitates monitoring, and simplifies response. For OT environments, this goes beyond traditional IT security tools — it requires contextual awareness of physical processes and operational constraints.

At ÆGIS, we've found that building defensibility into ICS environments isn't just about adding tools — it's about reshaping how systems are designed, maintained, and monitored from the ground up.

KEY PRINCIPLES OF DEFENSIBLE ICS/OT ARCHITECTURE:

A. COMPREHENSIVE ASSET IDENTIFICATION AND INVENTORY

Understanding what you have is the first step in protecting it. Many industrial sites struggle with undocumented or legacy devices that may be running outdated software. A complete and current asset inventory, including hardware, firmware, operating systems, communication protocols, and network topology, is essential.

- Passive scanning and active querying (where safe) can help build this inventory.
- Integrate asset data with vulnerability databases for risk prioritization.

We at ÆGIS often start engagements with asset discovery — it's shocking how many systems run unmonitored for years.

B. NETWORK SEGMENTATION AND ZONE-BASED DESIGN

One of the most effective strategies is segmenting networks into zones based on function, criticality, and trust level.

- Implement "zones and conduits" architecture (as per IEC 62443).
- Create a Demilitarized Zone (DMZ) between IT and OT to reduce cross-contamination.
- Enforce unidirectional gateways or firewalls to control data flows, especially from lower trust zones to higher trust areas.

This approach limits lateral movement by attackers and contains breaches within defined boundaries.

C. SECURE REMOTE ACCESS AND VENDOR MANAGEMENT

Remote access is increasingly necessary, especially post-COVID, but it is a significant vector for attacks.

- Use multi-factor authentication (MFA) and least-privilege access models.
- Segment vendor access, log all sessions, and enforce time-bound permissions.
- Consider jump servers and session recording for high-privilege accounts.

At ÆGIS, we advocate for strict controls around third-party access — some of the most damaging incidents we've investigated originated from unmanaged vendor connections.

D. CONTINUOUS MONITORING, DETECTION, AND LOGGING

ICS/OT environments require visibility into both cyber and physical parameters.

- Deploy network detection and response (NDR) solutions tailored for industrial protocols like Modbus, DNP3, or OPC.
- Monitor for anomalies such as unusual command sequences or data rates.
- Log system and security events centrally and retain logs in a tamper-evident system.

ÆGIS strongly recommends investing in visibility — you can't respond to what you can't see.

E. INCIDENT RESPONSE PLANNING AND RECOVERY

Industrial systems can’t always afford downtime — which makes incident response planning critical.

- Develop playbooks for various scenarios (malware, insider threat, ransomware, misconfigurations).
- Conduct tabletop exercises and simulate attacks without disrupting production.
- Have offline backups and clearly documented restoration procedures.

We help organizations define response paths that minimize disruption while protecting safety and integrity.

2. TACKLING COMMON INDUSTRIAL CYBERSECURITY CHALLENGES

Despite growing awareness, many industrial sites are still at early stages of cybersecurity maturity. Common pain points include:

A. LEGACY SYSTEMS AND OUTDATED SOFTWARE

Many OT environments rely on equipment designed decades ago — systems not built with security in mind.

- Replace or isolate legacy components.
- Use virtual patching or application-layer firewalls when updates are not feasible.

When ÆGIS conducts risk assessments, we often find that legacy PLCs or RTUs are still in production — some without any vendor support. Securing them requires tailored approaches.

B. LIMITED OT SECURITY EXPERTISE

Unlike IT, OT has traditionally prioritized availability and reliability over confidentiality and integrity.

- Cross-train engineering teams on security principles.
- Build hybrid teams that include both IT security and OT domain experts.

We believe the future of ICS security lies in interdisciplinary collaboration — something we actively promote in client engagements.

C. THIRD-PARTY RISKS

Vendors, integrators, and contractors often have extensive access but may not follow strict security practices.

- Enforce vendor risk management policies.
- Require contractual security obligations and compliance with industry standards.

At ÆGIS, we recommend embedding security clauses in all vendor contracts and conducting periodic access reviews.

3. SECURITY CULTURE AND HUMAN FACTORS

Technology alone can't secure ICS environments. Human awareness and accountability are equally critical.

- Conduct regular training tailored to different roles: engineers, operators, maintenance, and executives.
- Promote a “see something, say something” culture.
- Ensure personnel understand how to recognize phishing, social engineering, and unauthorized changes.

According to a recent SANS ICS survey, over 60% of incidents in OT environments involved either human error or insider actions. We at ÆGIS always emphasize that cybersecurity is as much a people issue as it is a technical one.

4. ALIGNING WITH INDUSTRY STANDARDS AND FRAMEWORKS

Security frameworks provide a structured, scalable path for organizations to build maturity.

KEY STANDARDS:

IEC 62443

Focused on control system cybersecurity, defining roles, security levels, and lifecycle processes.

NIST SP 800-82

Offers detailed guidance for securing ICS environments.

NERC CIP

(for energy): Compliance-focused framework for critical infrastructure protection.

MITRE ATT&CK FOR ICS

Maps adversarial tactics, techniques, and procedures (TTPs) specific to OT.

At ÆGIS, we align our services with these standards to ensure our clients' security programs are defensible and auditable.

5. THE ROLE OF EMERGING TECHNOLOGIES

Cybersecurity for ICS is evolving rapidly. New tools are being developed specifically for OT environments:

- **AI AND MACHINE LEARNING**
  Used for anomaly detection and predictive maintenance.
- **DIGITAL TWINS**
  Simulate physical processes to detect deviations and assess vulnerabilities without risk.
- **ZERO TRUST ARCHITECTURES**
  Though challenging in OT, elements of zero trust — like micro-segmentation and identity verification — are being adapted for industrial use.

ÆGIS is actively piloting AI-based behavioral detection tools in high-stakes environments, and the results are promising — especially when paired with expert oversight.

CONCLUSION

The digital transformation of industrial operations is accelerating — but so is the threat landscape. ICS and OT environments can no longer rely on isolation or obscurity for protection. Instead, they need a proactive, layered, and context-aware cybersecurity strategy.

By building a defensible architecture, addressing known challenges, fostering a security culture, and aligning with industry frameworks, industrial organizations can move from reactive defense to resilient security. This transformation isn't just technical — it's strategic, cultural, and operational.

At ÆGIS, we're proud to help organizations chart this course. We believe that securing industrial systems means protecting not just data, but lives, environments, and economies.

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