Executive Overview

Independent IT/OT Cybersecurity Architecture & Advisory for industrial, manufacturing and operational technology environments.

Practical cybersecurity for industrial operations

Aegis helps organisations understand exposure, prioritise remediation and strengthen operational resilience across the IT/OT boundary.

CORE PROPOSITION

Secure Critical Operations

Reduce cyber risk. Strengthen resilience. Improve security governance.

Operational resilience

Security architecture that protects production availability, safety and business continuity.

Executive clarity

Board-ready summaries, prioritised roadmaps and evidence-led recommendations.

Industrial focus

Designed for complex IT/OT estates where controls must align with plant realities.

Version 2.0 | June 2026

Public overview for website download

info@aegisindustrialsecurity.com | UK 0208 0589606 | aegisindustrialsecurity.com

What Aegis Delivers

Focused advisory services that convert fragmented technical risk into clear decisions, delivery priorities and governance actions.

01 IT/OT cybersecurity architecture

Target-state models for enterprise and industrial networks, including zones, conduits and secure integration patterns.

02 OT security assessments

Current-state reviews that identify exposure, control gaps and practical improvement actions.

03 Network segmentation & firewall review

Assess rulebases, trust boundaries, conduits, remote access and excessive access across IT/OT paths.

04 Vulnerability & exposure management

Prioritise exposure using operational context, asset criticality, exploitability and remediation practicality.

05 Cyber resilience & incident readiness

Review backup, recovery, OT incident scenarios and operational continuity dependencies.

06 Governance & executive reporting

Translate technical findings into maturity narratives, accountable actions and board-ready summaries.

Industrial Network Segmentation & Firewall Risk Review

A focused, bounded first engagement to identify excessive access, weak segmentation, insecure conduits, legacy protocol exposure and firewall governance gaps.

01 Review scope

- Firewall rulebase analysis and high-risk rule identification
- Purdue model, zone and conduit alignment
- Legacy protocol, remote access and exposure review

02 Client deliverables

- Executive report and stakeholder readout
- Prioritised remediation roadmap
- Technical findings appendix and risk reduction recommendations

03 Commercial value

A tangible review directly linked to risk reduction, audit readiness, operational resilience and accountable remediation planning.

Delivery approach

Understand
Objectives, constraints and architecture

→

Assess
Risk pathways, segmentation and governance

→

Prioritise
Risk-ranked remediation roadmap

→

Improve
Advisory support for implementation

→

Sustain
Governance, maturity and continuous improvement

Typical delivery: small environments 1-2 weeks | medium environments 2-4 weeks | larger or multi-site engagements scoped by complexity.

Framework Alignment

Aegis uses recognised security frameworks as operating references, then translates them into practical controls, evidence and execution plans.

ISA/IEC 62443	Primary industrial security reference for zones, conduits, security levels and OT-specific governance.
NIST CSF	Executive-friendly structure for risk framing, maturity and resilience reporting.
ISO/IEC 27001	Governance, risk treatment, policy and security management alignment.
MITRE ATT&CK for ICS	Threat-informed mapping for adversary behaviours and control validation.
Purdue Model	Reference model for segmentation, trust boundaries and IT/OT demarcation.
TISAX	Relevant for automotive and manufacturing supply-chain assurance requirements where applicable.

OPERATING PRINCIPLE — **Controls | Evidence | Roadmap** — Frameworks are mapped into clear evidence, control expectations and improvement actions.

Why Aegis Industrial Security

FOUNDER

Craig Cyrus CISSP

Cybersecurity Architect

Over two decades of experience across IT, cybersecurity and industrial environments. Focus areas include IT/OT cybersecurity architecture, network segmentation, firewall risk review, vulnerability management, cyber resilience and executive-facing security reporting.

01 Industrial context

Recommendations are shaped for production environments, not generic enterprise assumptions.

02 Executive translation

Technical risks are converted into clear decisions, priorities and defensible business narratives.

03 Independent judgement

Advice is not tied to reselling products or pushing a specific technology stack.

04 Practical execution

Outputs support delivery teams, site engineers and accountable leadership.

BUSINESS VALUE

Clearer risk ownership, stronger governance, improved readiness and a prioritised remediation roadmap.

Secure Critical Operations

Reduce cyber risk. Strengthen resilience. Improve security governance.

Start with a focused conversation to confirm the business driver, scope and priority outcomes. Aegis will then define a proportionate engagement structure, expected deliverables and delivery approach.

01 Initial consultation

A short discovery discussion to establish the business driver, scope and priority outcomes.

02 Focused engagement

Aegis defines the engagement structure, evidence needs, expected deliverables and delivery approach.

03 Practical roadmap

The engagement produces clear findings, decision-ready summaries and accountable next actions.

Request an Initial Consultation

info@aegisindustrialsecurity.com UK 0208 0589606 aegisindustrialsecurity.com

Craig Cyrus CISSP | Cybersecurity Architect