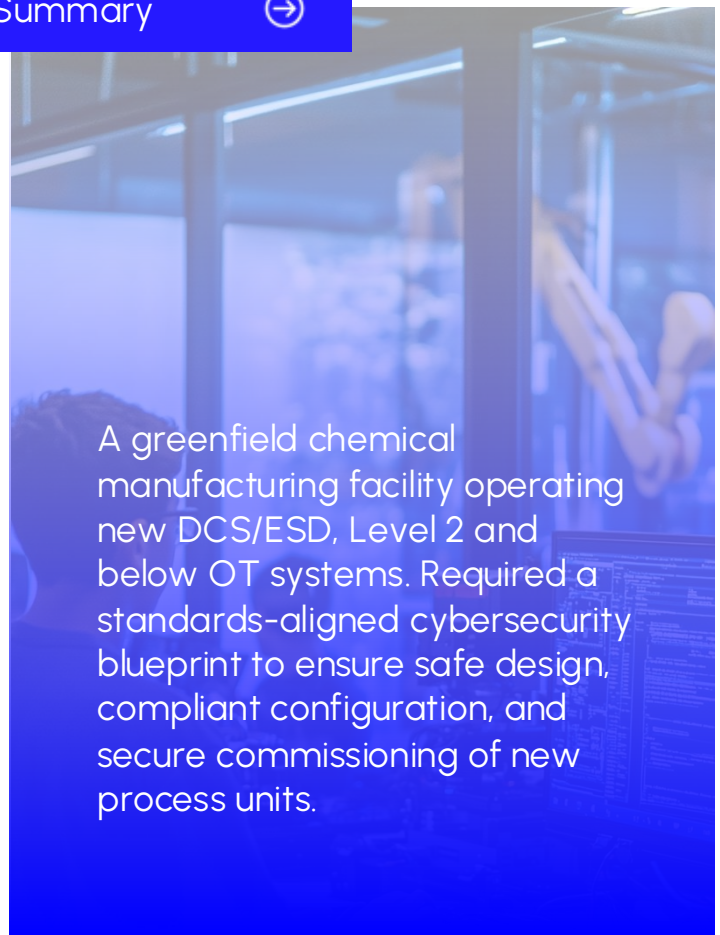
Use Case 2

Greenfield OT Cyber Assurance & Requirements Framework

Summary



A greenfield chemical manufacturing facility operating new DCS/ESD, Level 2 and below OT systems. Required a standards-aligned cybersecurity blueprint to ensure safe design, compliant configuration, and secure commissioning of new process units.

Business Issue

The client needed to:

- Validate OT architecture
- Assess cyber risks
- Establish Security Levels (SL-T and CyberSL)
- Define cybersecurity requirements for engineering and implementation

Without a structured framework, the project risked misaligned safeguards, insecure system configuration, and compliance gaps affecting safety and reliability

Use Case 2

Greenfield OT Cyber Assurance & Requirements Framework

Our Approach

01 Validate Architecture & Segmentation

Confirmed OT design, zones, conduits, and asset inventory.

02 Identify Assets & Criticality

Mapped DCS/ESD assets to process and safety impact.

03 Conduct CyberPHA DLRA

Assessed threats, vulnerabilities, and credible scenarios.

04 Evaluate Cyber Risk

Calculated inherent/residual risk and prioritized mitigations.

05 Verify Security Levels

Set SL-T and confirmed achievable CyberSL per ISA/IEC 62443.

06 Define 62443 Requirements

Developed CSRS and safeguard recommendations.

07 Deliver & Validate

Issued reports/specs and verified secure implementation

08 Oversee Implementation

Validated secure configuration during commissioning to ensure compliance with design requirements.

Use Case 2

Greenfield OT Cyber Assurance & Requirements Framework

Value to Customer / Issues Resolved

01 Standards-aligned OT architecture and segmentation model

02 Full visibility into credible cyber threats and vulnerabilities

03 Clear Security Level (SL-T & CyberSL) definition for each OT zone

04 Structured mitigation roadmap reducing engineering and operational risk

05 Cybersecurity embedded in design, procurement, FAT/SAT, and commissioning

06 Reduced likelihood of cyber-induced process disruptions or safety impacts

Outcome

ARISTA CYBER

The client received a **comprehensive OT cybersecurity assurance package** for its greenfield units, ensuring DCS/ESD systems met required Security Levels and were implemented securely. The DLRA provided visibility into risks, validated safeguards, and defined actionable requirements—resulting in a **safer, more resilient, and fully compliant OT environment** ready for reliable operations.