SECURING INDUSTRIAL SAFETY AND RELIABILITY

Bridging Functional Safety (ISA 84) and Cybersecurity (ISA/IEC 62443)

Koniag Cyber (KCS) helps industrial organizations protect people, processes, and production by integrating process safety and cyber resilience.

We partner with leading integrators and technology providers to deliver end-to-end protection — from Safety Instrumented Systems (SIS) integrity to secure automation networks across plants, terminals, and transportation assets handling hazardous chemicals and other critical operations.

As part of the Koniag family of companies, Koniag Cyber builds on over 50 years of experience meeting client needs across commercial and government sectors — delivering trusted solutions that strengthen operational safety, regulatory compliance, and digital transformation initiatives.

Core Capabilities

CYBERSECURITY RISK & COMPLIANCE

- Perform **ISA/IEC 62443 Gap Assessments** and **Cyber-PHA/LOPA** reviews.
- Integrate cybersecurity into **Process Safety Management (PSM)** and **Risk Management Plans (RMP)**.
- Deliver actionable roadmaps that align with **ISA 84**, **CFATS**, and **EPA/OSHA** requirements.

OUTCOME

Clear visibility of cyber-physical risk and compliance confidence.

SECURE CONTROL SYSTEM ARCHITECTURE

- Design **zone & conduit segmentation** using the Purdue Model.
- Harden **Safety Instrumented Systems (SIS)** and **control networks** to ensure functional independence.
- Implement secure **remote access**, **firewalls**, and **data-diode isolation**.

OUTCOME

Reduced attack surface and maintained process integrity.

OT ASSET VISIBILITY & THREAT MONITORING

- Deploy **industrial anomaly detection** for PLC, HMI, and SIS networks.
- Enable **24×7 OT SOC monitoring** and incident alerting.
- Manage vulnerabilities, patches, and change tracking across legacy and modern systems.

OUTCOME

Early detection and faster response to cyber-physical threats.

SYSTEM HARDENING & CONFIGURATION ASSURANCE

- Secure PLC, HMI, and engineering workstation configurations.
- Apply least-privilege and secure-by-design settings.
- Validate system integrity through baseline checks and firmware signing.

OUTCOME

Reliable, tamper-resistant control environments.

INCIDENT RESPONSE & RECOVERY

- Develop and exercise **ICS-specific incident response plans.**
- Conduct **joint cyber + safety drills** simulating ammonia release scenarios.
- Validate backups and recovery procedures for control systems.

OUTCOME

Rapid recovery while maintaining safety compliance.

INTEGRATED LIFECYCLE SUPPORT

- Embed cybersecurity in every phase of the **Safety Lifecycle**—from design to decommissioning.
- Support FAT/SAT, validation, and operations with cybersecurity oversight.
- Provide continuous improvement through maturity tracking and audits.

OUTCOME

Sustainable, measurable security improvement over time.

TRAINING & AWARENESS

- Tailored **ISA/IEC 62443 practitioner and operator training.**
- Hands-on **incident response and cyber-safety workshops.**
- Guidance on policy, governance, and supplier risk management.

OUTCOME

Empowered teams and consistent safe-secure culture.

Koniag Cyber complements **process safety and automation** expertise with **industrial cybersecurity depth**, delivering unified protection across both safety and security domains.

Safety + Security = Resilience

Together, we help clients achieve compliance, continuity, and confidence.

Industrial Cyber Resilience
OT Security
ISA/IEC 62443 Implementation

info@koniagcyber.com
www.koniagcyber.com