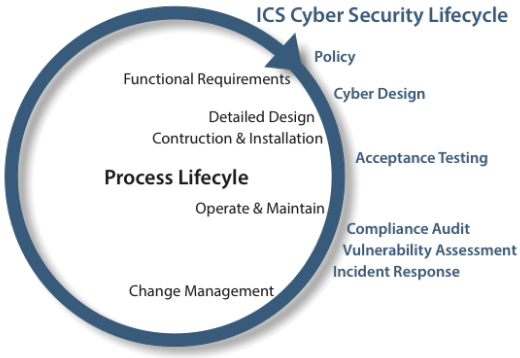
Kenexis Industrial Cyber Security

Industrial Network Security, Performance & Reliability Services

Background

Industrial Control System protocols are different that Ethernet protocols and were created originally as serial communications before the wide spread use of Ethernet networking. They support proprietary inter-process communications and were built to provide reliable deterministic communications before Ethernet security was a consideration. Consequently, many lack means of authentication or integrity checking and are vulnerable.



Our Security Services are staffed by seasoned industrial control system experts and our designs are built on a solid industrial control system network design with secure communication and reliability as defined in ISA/IEC 62443 and other standards as required by industry or region. Our designs provide secure and reliable industrial networks that will serve your business well with better visibility, secure remote connectivity, and less unexplained downtime. Kenexis offers industrial cyber security services designed around your process lifecycle to assist your organization with establishing a secure and reliable industrial network throughout the system's lifecycle.

Policy service is designed to help your organization develop an industrial control system security philosophy including responsibilities, risks, policies, and procedures. All of which are assessed against standards and regulations applicable to your industry and region. Your established policy will drive security focused behavior, budgeting decisions, and accountability.

Cyber Design service creates your industrial secure network design. We assess critical areas/process, risks, subsequent threat vectors and develop a secure logical network design with layers of protection and isolated traffic flows that a system integrator can use to develop a detailed design.

Acceptance Testing verifies that the detailed design as built, meets the security functions defined in the cyber design. These test can be performed onsite for systems/equipment constructed and installed locally or performed offsite where the skid is built. These test are designed to prevent the introduction of vulnerabilities into your system. Report includes analysis & recommendations.

Compliance Audit service verifies the awareness and compliance. Periodically it is good practice to test both policy awareness and policy compliance. We will work with your team to develop questionnaires and interview using a variety of methods. Report includes analysis & recommendations.

Vulnerability Assessment evaluates the ICS network for security, performance, and reliability. Prior to assessment, we will review network architecture, assets, technologies, data flows, and previous

Kenexis Industrial Cyber Security

Industrial Network Security, Performance & Reliability Services

assessments including risks assessments like HAZOP. Vulnerability testing includes passive and active scanning for device discovery and service enumeration as well as vulnerabilities. Data aggregation and collation is followed by in depth analysis using a variety of tools and Kenexis Dulcet Analytics. We identify vulnerabilities and rank them, remove false positives, and develop prioritized recommendations. Our final report includes asset inventory, vulnerabilities discovered & severity ratings, recommendations, comparisons, overview of tools utilized and findings including all raw data.

Incident Response service will help you develop a plan or provide assistance during an incident. Our incident response focuses on remediating the problem as quickly as possible and not specifically on forensics even those we use forensics techniques.

EXPERIENCE developed from working in the process industry and manufacturing, with the military, vendors, educational institutions and standards organizations worldwide. Our investigators have many years of experience in the development, design, and operation of industrial control systems, building automation systems, and many different embedded controllers and protocols.

Kenexis Regulation & Standards Experience:
ISA/IEC 62443 (ISA-99) Security for Industrial Automation and Control Systems
ISA-TR84.00.09 Security Countermeasures Related to Safety Instrumented Systems (SIS)
ISO/IEC 27000 Information Technology Security Techniques
NERC CIP North American Electric Reliability Corporation
NIST Cybersecurity Framework

Kenexis Cyber Participation:
International Society of Automation (ISA)
ISA Safety & Security Division Director
ISA99 Co-Chair (ISA62443)
ISA Instructors & Authors

Kenexis Cyber Certifications:
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
Certified Automation Professional (CAP)
Global Industrial Cyber Security Professional (GICSP)
Certified Ethical Hacker (CEH)

Kenexis Industry Experience:
Oil & Gas; Upstream, Midstream, & Downstream
Chemical; Petrochemical, Pharmaceutical
Power Generation; Nuclear, Gas, Coal, Hydro
Municipalities; Water & Wastewater
Manufacturing; Automotive, Pharma, Metal, Food & Beverage
Buildings; Automation, Energy
Transit; Rail, Shipping, Terminals
Government; Research

About Kenexis

Kenexis is an independent engineering consulting firm providing a range of services that are geared toward identifying the risks posed by process plants and manufacturing facilities and then assisting in the implementation of technical safeguards to mitigate those risks. Kenexis services fall into four main categories:

Our services help our clients to comply with appropriate regulations and standards, and benchmark their performance and processes against industry best practices. These services allow our clients to have best in class safety, security, and reliability.