Assuring Safe, Reliable, and Secure Industrial Operations

Kenexis Security Corporation provides industry leading process protection strategies combining safety and security to provide end-users with the key information they need to assure the safe, reliable, and efficient operation of their facilities.

Cyber security, industrial networking, change management, safety faults and failures, government regulatory efforts such as 6 CFR 27 CFATS and NERC CIP-002—CIP-009, and other concerns are driving an increased awareness that asset owners need to protect their industrial processes from cyber security threats.

Kenexis Security Corporation provides industry leading process protection strategies combining safety and security to provide end-users with the key information they need to assure the safe, reliable, and efficient operation of their facilities.
Common Questions about Industrial Security
- Is Our Process Safe?
- Is Our Process Secure?

These questions can only be answered if you have a balanced and thorough understanding of:
- Device Vulnerabilities
- Industrial Networking
- Process Safety
- Process Intelligence Applications (OEE, LIMS, ERP, MES, etc)
- Disaster Recovery and Incident Response
- Industry Standards
- Regulatory Requirements

The Approach to Industrial Security
- Utilize Industry Standards and Regulatory Requirements (ISA-84, ISA-99, ISA-18, ISA-95, etc)
- Team members must be experienced in automation, safety, networking, and security
- Leverage the concept of a “Security Assurancr Level (SAL)” - a streamlined model that ranks possible process impacts from quality, stoppage, safety, regulatory, and other concerns and balances the capabilities of the entire system to prevent and mitigate these impacts.
- Validate the implementation against security and safety requirements