

Assuring Safe, Reliable, and Secure Industrial Operations



**PLAN**



**PREPARE**



**DEFEND**



**RESPOND**

# INDUSTRIAL SAFETY AND SECURITY ASSURANCE STRATEGIES

**KENEXIS SECURITY CORPORATION** <http://www.kenexis.com/security>

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.

## **KENEXIS Security Corporation**

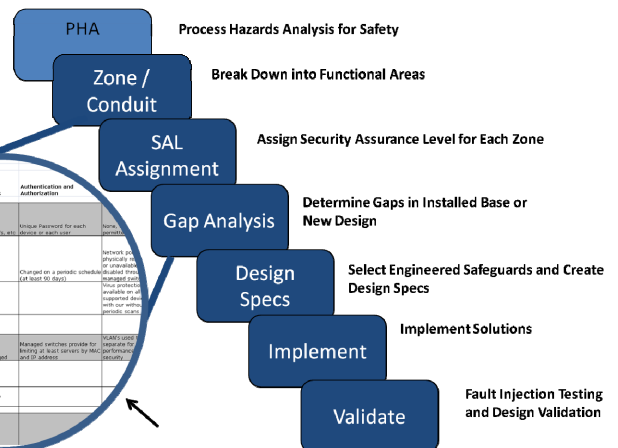
2929 Kenny Road  
Suite 225  
Columbus, OH 43221

Phone: 614.451.7031  
Fax: 614.451.2643  
E-mail: [info@kenexis.com](mailto:info@kenexis.com)

**KENEXIS**  
Copyright © 2008 Kenexis Security Corporation

# KENEXIS

## Security for Process Control



<http://www.kenexis.com/security>  
[info@kenexis.com](mailto:info@kenexis.com)

### 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:

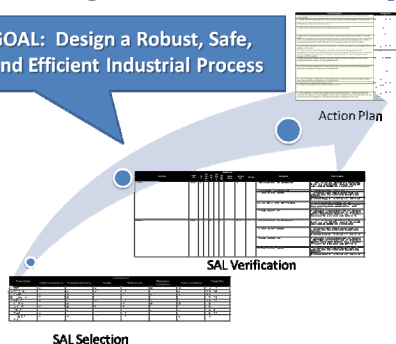
- Device Vulnerabilities
- Industrial Networking
- Process Safety
- Process Intelligence Applications (OEE, LIMS, ERP, MES, etc)
- Disaster Recovery and Incident Response
- Industry Standards
- Regulatory Requirements

### 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 Assurance 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

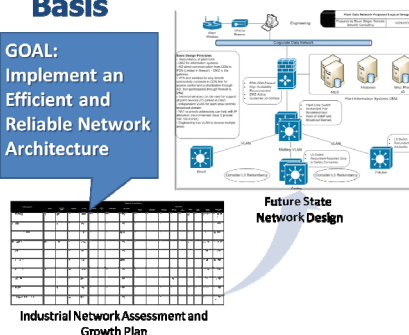
### Design Basis for Security

GOAL: Design a Robust, Safe, and Efficient Industrial Process



### Industrial Network Design Basis

GOAL: Implement an Efficient and Reliable Network Architecture



### Industrial Security Training

**Introduction to Industrial Ethernet Networking**

- Overview of OSI, Network Devices, Topologies and Design
- LAB: Packet Analysis, Traffic Analysis, and Troubleshooting
- 12 hours

**Introduction to Industrial Security**

- Emerging Legislation and Standards (CRAFTS, NERC CIP, ISA-99, etc)
- Industrial Security Risk Management Practices and Technologies
- Lab: Attack Trends and Methods, Scenario Modeling, Attack Simulation
- 12 hours

**Advanced Industrial Cyber Security**

- Cost of Capital, ROI for Security, Business Case
- Advanced Design for Security (OEE, LIMS, MES, Historians, PHA, SIS, etc)
- Lab - SAL Selection and Verification, Network Analysis
- 16 Hours - 2 days

## Strategies for Industrial Automation and Process Control