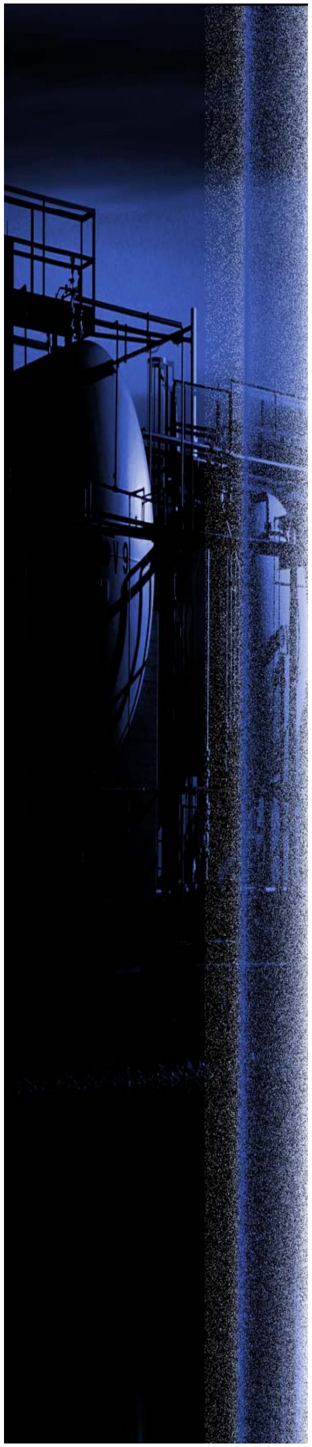

KENEXIS
Industrial Security Services

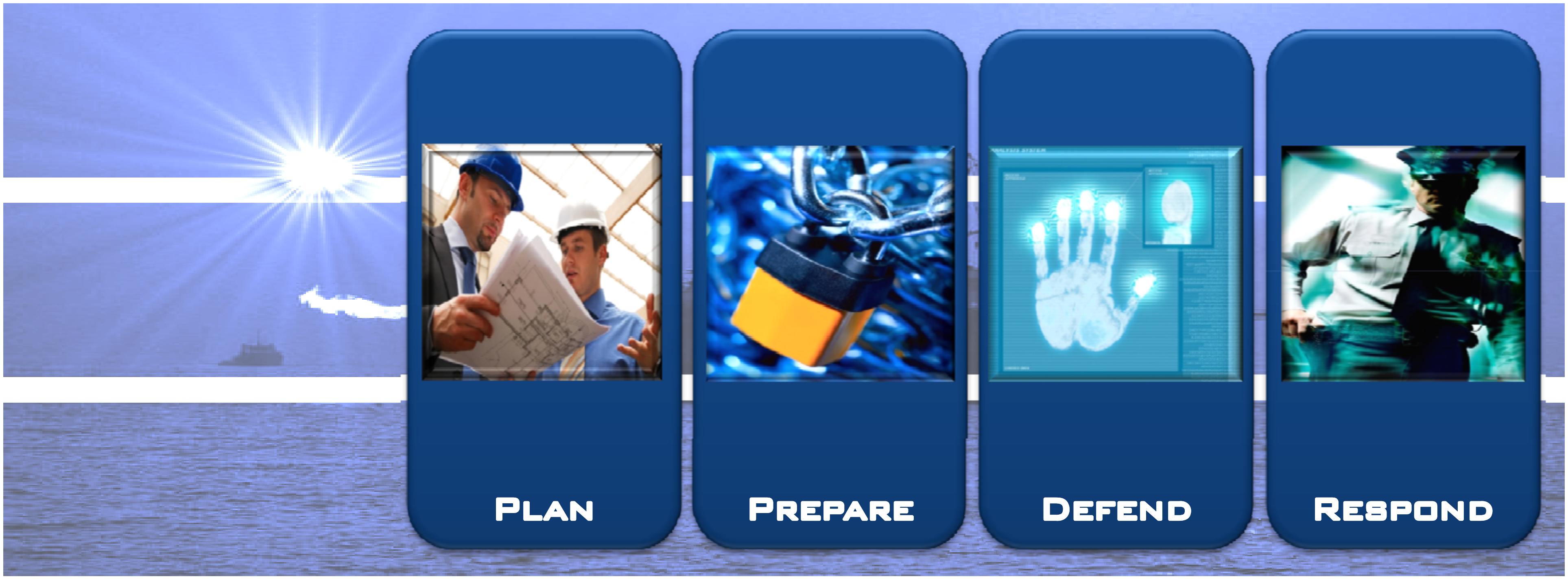


Today's Presenter

Bryan L Singer, CISM, CISSP, CAP

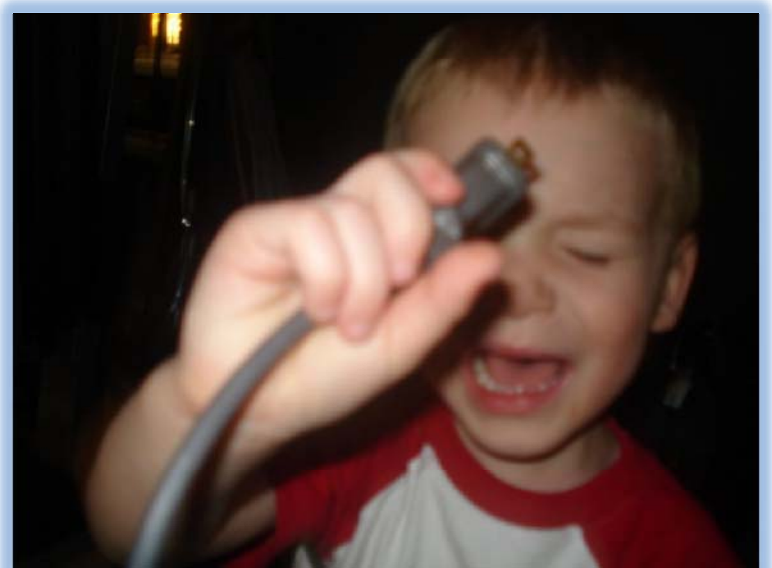
- Vice President, Kenexis Security Corporation
- Chairman ISA-99 Industrial Automation and Control Systems Security
- Chair ISA-84/99 JWG for Safety and Security
- Appointee to NERC CIP SAR and Drafting Team
- DHS PCSF former board member and current governing board

KENEXIS



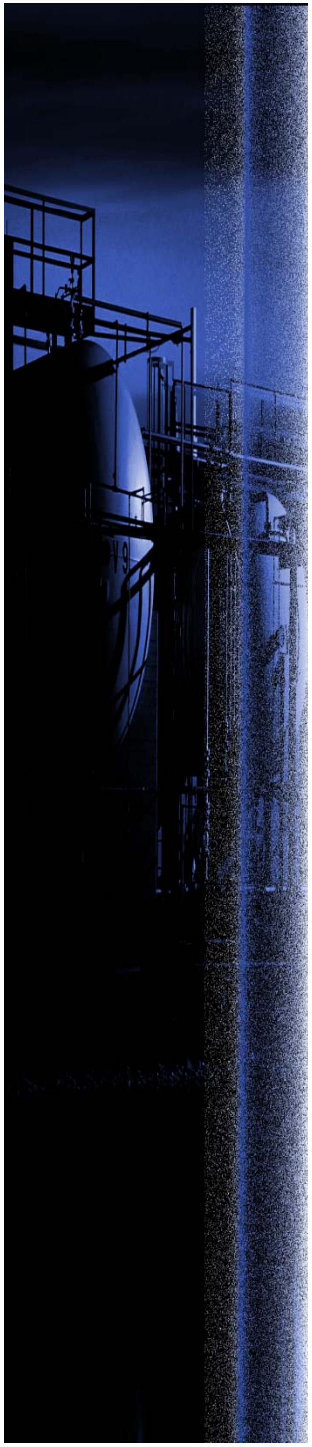
INDUSTRIAL SAFETY AND SECURITY

When Technology Goes Awry

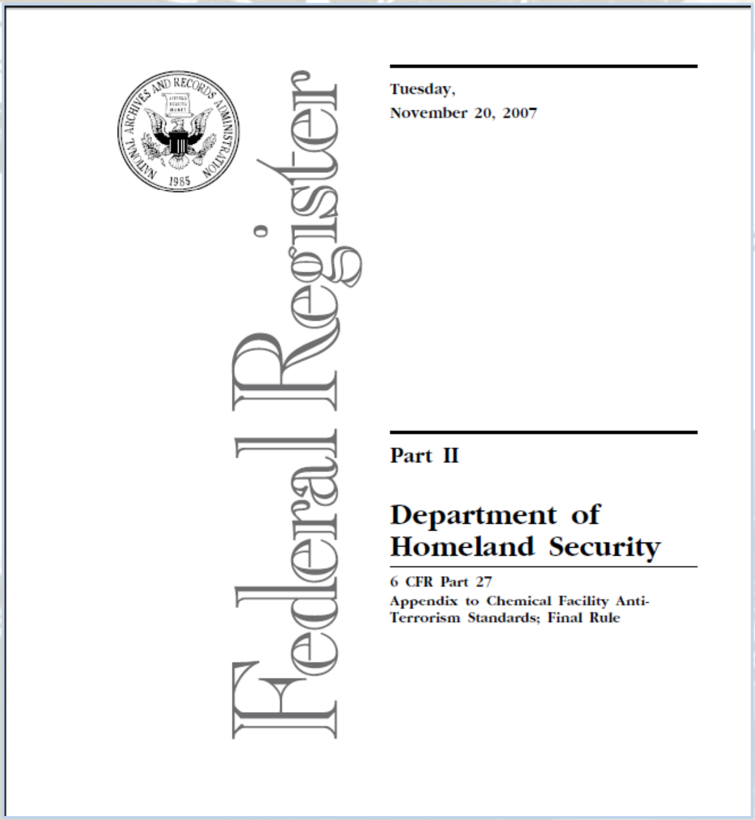


- In process control, we now unite the logical and the physical
- Under attack, bad things can happen!
- Safety systems are just as vulnerable as any other component
- These systems are exposed to external attack if they are networked

KENEXIS



6 CFR 27 A: CFATS Regulations



Federal Register

Tuesday,
November 20, 2007

Part II

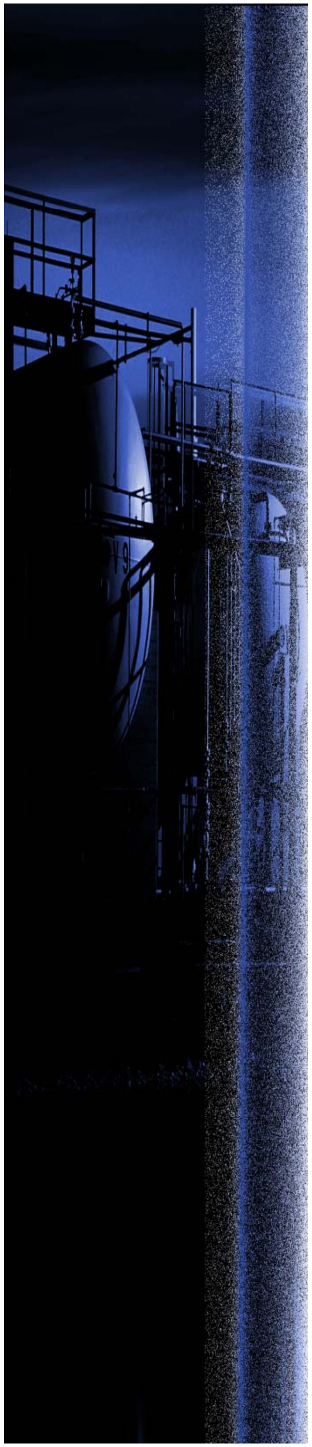
Department of Homeland Security

6 CFR Part 27
Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule

Chemical Facility Anti-Terrorism Standards (CFATS) 6 CFR 27.230(a) covered facilities must satisfy the performance standards identified in this section. <…>

Each covered facility must select, develop, and implement measures designed to: **(8) Deter cyber sabotage, including by preventing unauthorized onsite or remove access to critical process controls, SCADA systems, and other sensitive computerized systems.**

KENEXIS



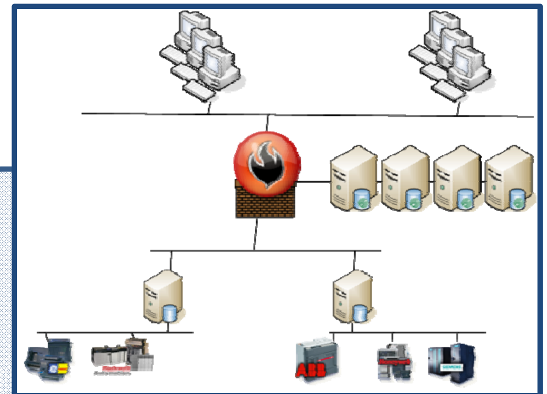
Requirements for Industrial Security

- Solution Providers and Project Personnel MUST understand process control, IT security, and have a solid understanding of system such as OEE, CBM, LIMS, MES, ERP, etc
- Vulnerability Methodology must include issues centric to process control devices, not just PCs and Servers
- A KEEN knowledge of the process and safety requirements is REQUIRED

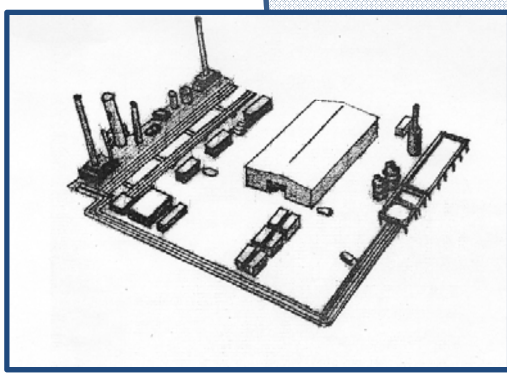
KENEXIS

Where Should We Focus?

Devices



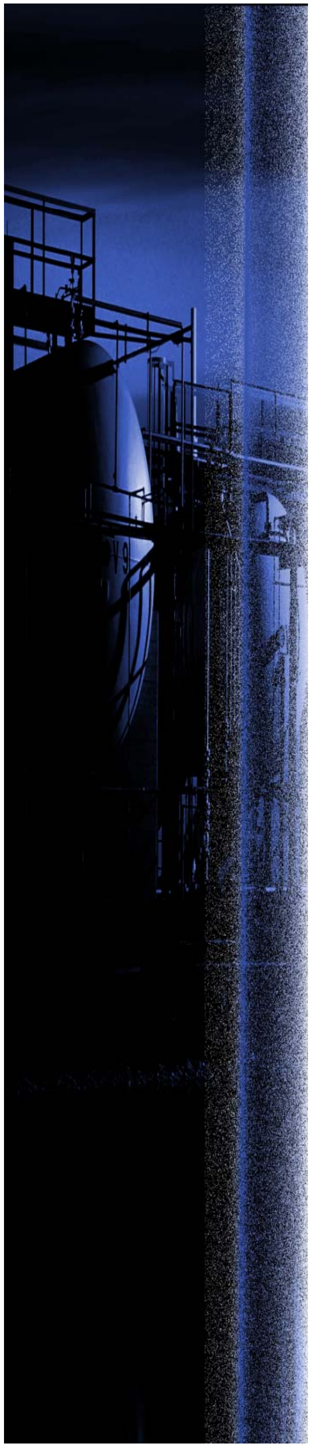
Network and Infrastructure



Process

- Too much attention often paid to device issues (US-CERT, ISCI, etc)
- Objective of most industrial attacks is widespread damage or outages
- These are most easily exploited in process and network issues!

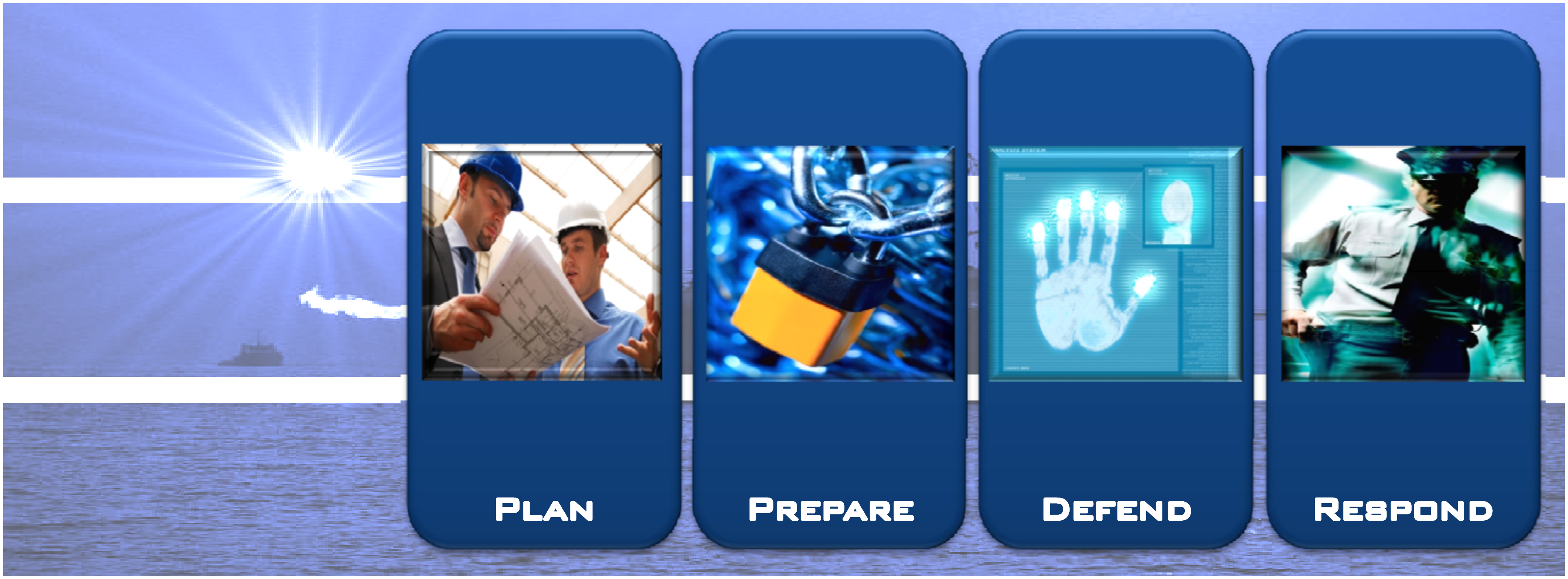
KENEXIS



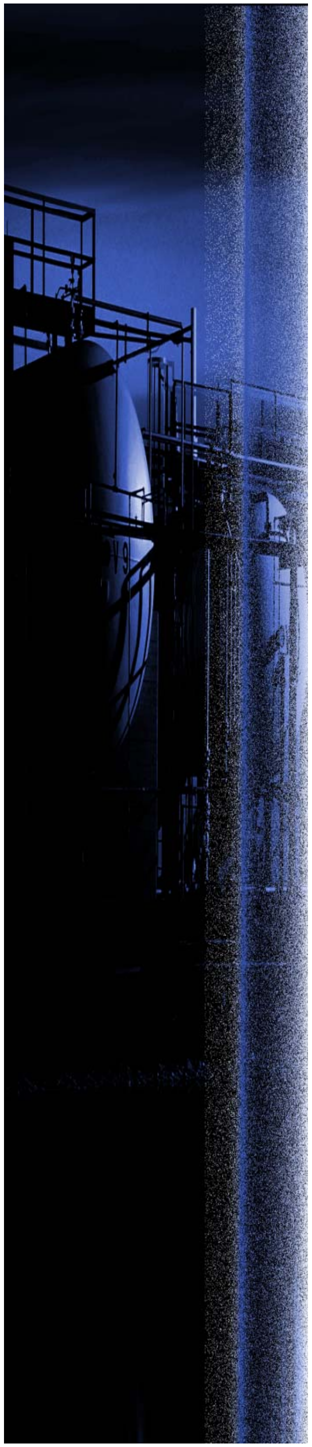
Vulnerability Taxonomies in Process Control

Vulnerability Type	Technical Skill	Process Knowledge	Desired Outcomes
Network and Infrastructure	Moderate	Low	•Deny, Disrupt, Deter Communications •Shutdowns • Passive Reconnaissance • Active Damage widespread
Devices and Endpoint Vulnerabilities	Mod-High	None-Low	• Viruses, worms, etc to disable workstations • "Bastion Hosts" to own an endpoint device for bot-nets, etc • "Trojan Horse" to control single workstations • Damage Limited to possibly widespread
Process Vulnerabilities	Limited	Extensive	• Catastrophic shutdowns and failures • Permanent System Damage • Retribution

KENEXIS



THE KENEXIS SECURITY PROCESS



The Industrial Security Process

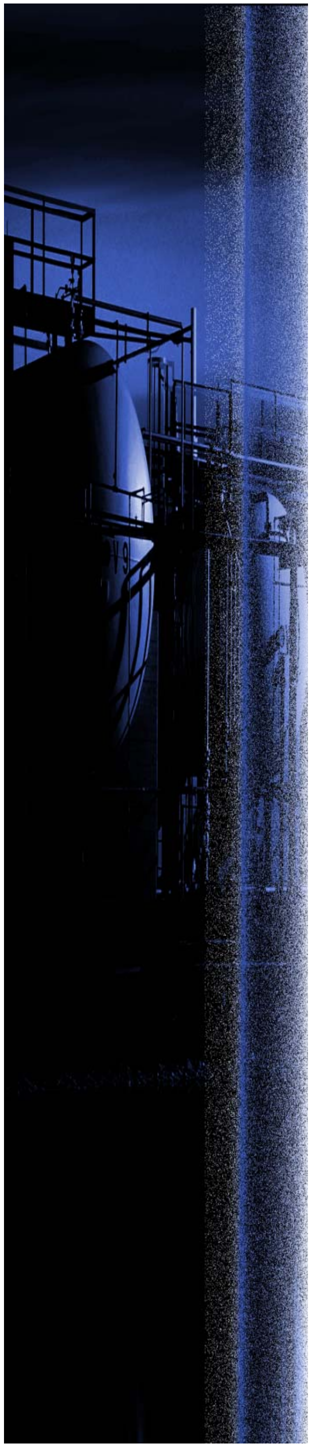
Plan
- PHA for Security
- SAL Determination
- Engineered Safeguard Selection and Design Basis
- CFATS, NERC CIP, NIST 800, ISA-99, ISA-84, ISA-95 Analysis
- Incident Response and Disaster Recovery Planning

Prepare
- Implementation Verification
- Fault Injection and Resilience Testing
- Change Management

Defend
- Failure and Incident Analysis
- Training and Awareness
- Periodic System Review

Respond
- Incident Response and Recovery
- Forensics and Investigation

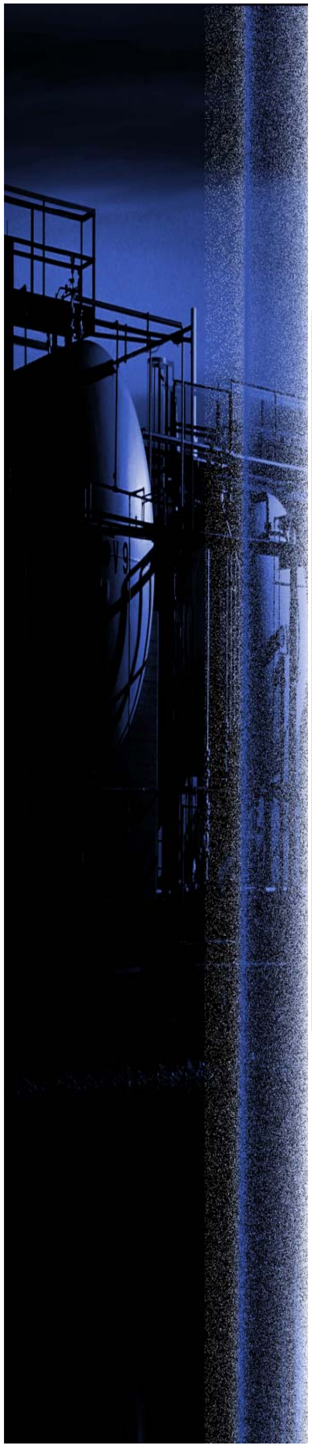
KENEXIS



It's Not ALL About the Firewall!!

- Engineered Safeguards For Process Control
  - Safety Instrumented Systems
  - Alarm Systems
  - Fire and Gas Systems
  - Relief Devices / Vent and Disposal Systems
  - Facility Siting / Temporary Refuge
  - Other Passive and Active Mitigation Measures
  - Machine Safeguarding

KENEXIS



Out of the Box Thinking for Industrial Security

Preventative
- Industrial Networking
- Safety and SIS
- Process and Automation Design
- Industrial Security Controls
- Intelligent Process Control
- Physical Security

Detective
- OEE
- CBM
- LIMS
- Historians
- MES
- ERP
- Firewalls
- IDS
- Alarm and Event Management
- Guard Plans
- Cameras and Monitoring

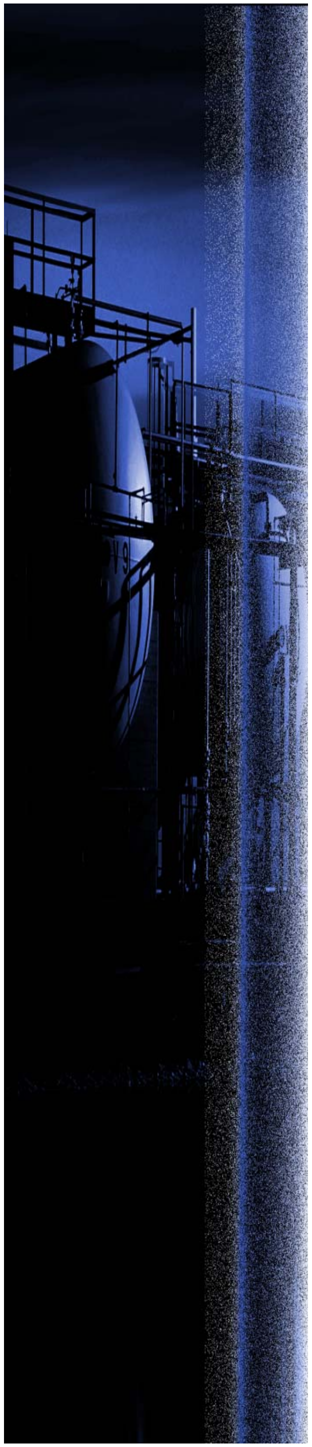
Reactive
- Incident Response
- Disaster Recovery
- Process Architecture and Design
- Fail-Safes
- Emergency Response and Coordination
- Pressure Relief Valves
- Redundancy and Failover for Processors
- Redundancy and Failover for Industrial Network

Risk Control Types for Defense in Depth

Leverages Existing Networks and Process Intelligence Applications

Security in Industrial Settings Requires Elements of Each!

KENEXIS



Protect The Device, or the System?

Device Security Features and Resilience

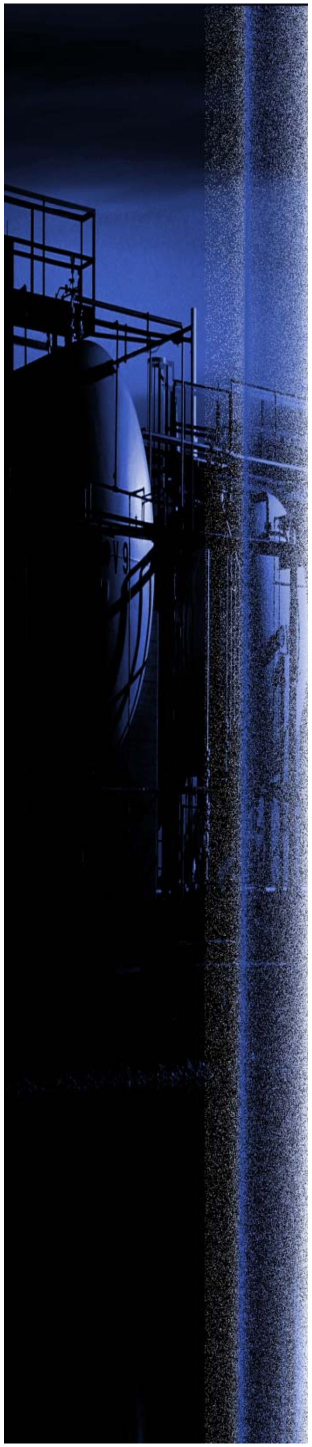
Demonstrates Compliance to

Process Architecture, Engineering Standards, Safety, and Security

Provide Performance Requirements

Follow a Process Similar to ISA-84, IEC 61508 Safety!

KENEXIS



Introducing Security Assurance Levels

Security Assurance Level 1 - Basic

- Minimal System Protection Measures
- Little to No Damage

Security Assurance Level 2 - Moderate

- Basic Authentication, Configuration Management, Network Protection, etc – Little to No Redundancy
- Damage limited to process interruptions or stoppages, minor safety, no public confidence, etc

Security Assurance Level 3 - Significant

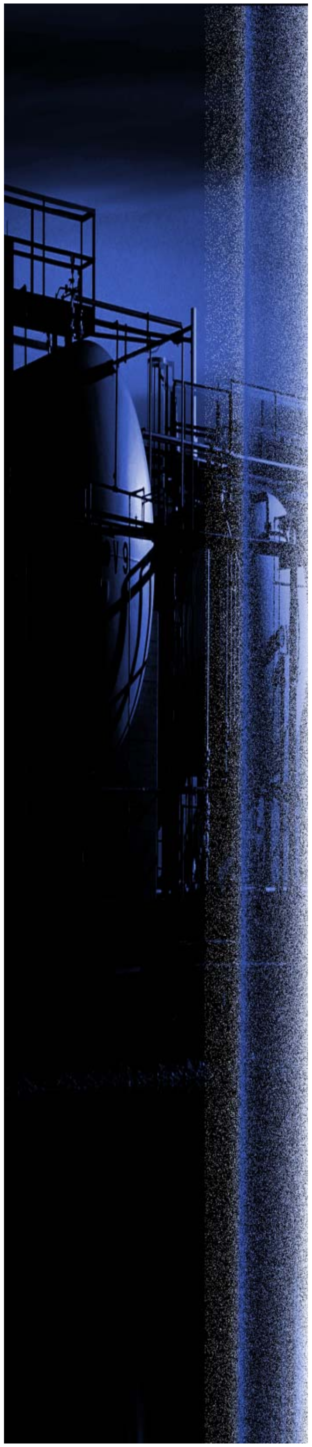
- Some redundancy in network and controls, availability, predominate SIS or similar controls, consistent authentication, strong policies and awareness
- Safety up to death and dismemberment, major stoppages, public confidence loss, quality loss, etc

Security Assurance Level 4 – Extreme

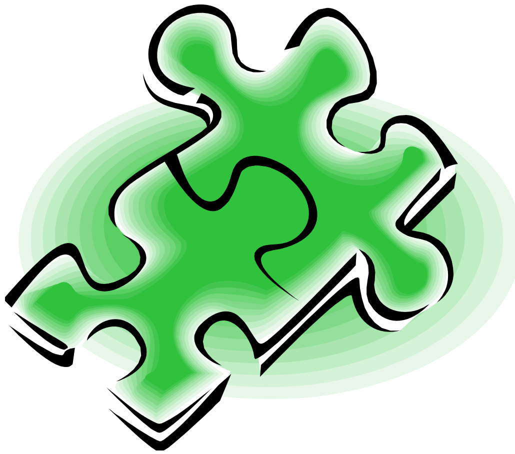
- Extensive redundancy in network and controls, heavy protection in SIS, strong authentication, heavy awareness
- Mass casualty or catastrophic failure scenarios, irrecoverable

- Emerging Definitions in ISA-99
- Focuses on IMPACT and protection required
- Deals with systematic faults, intentional or unintentional

KENEXIS



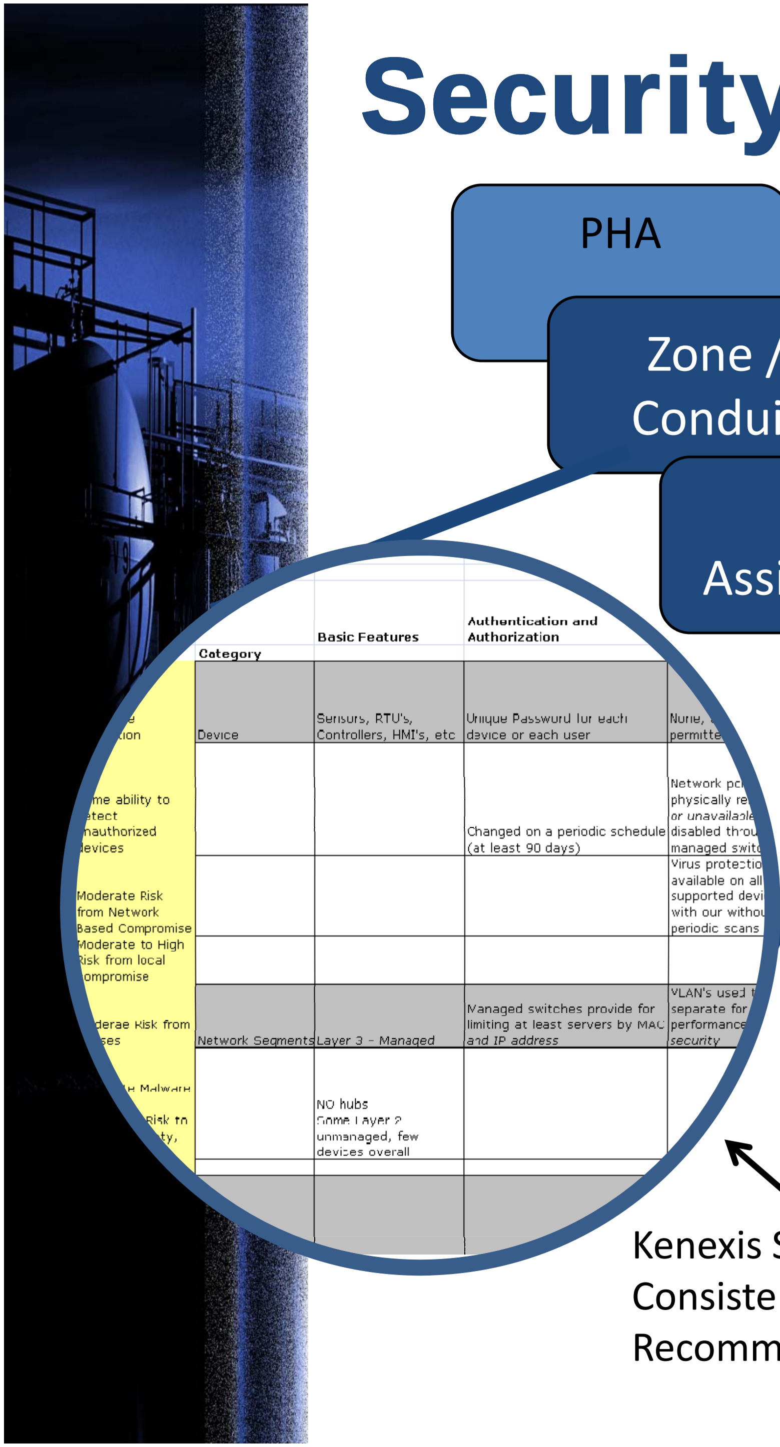
SIL Versus SAL



- **Safety Integrity Levels Common in Process**
  - Process Hazards Analysis Determines Hazards and Likelihood
  - Likelihood categorized by dangerous hardware failures per hour
  - Does not deal with intentional!
- **Security Assurance Levels**
  - Completes the picture
  - Deals with impact
  - Full picture of intentional and unintentional faults and failures that result in SYSTEMIC failures

KENEXIS

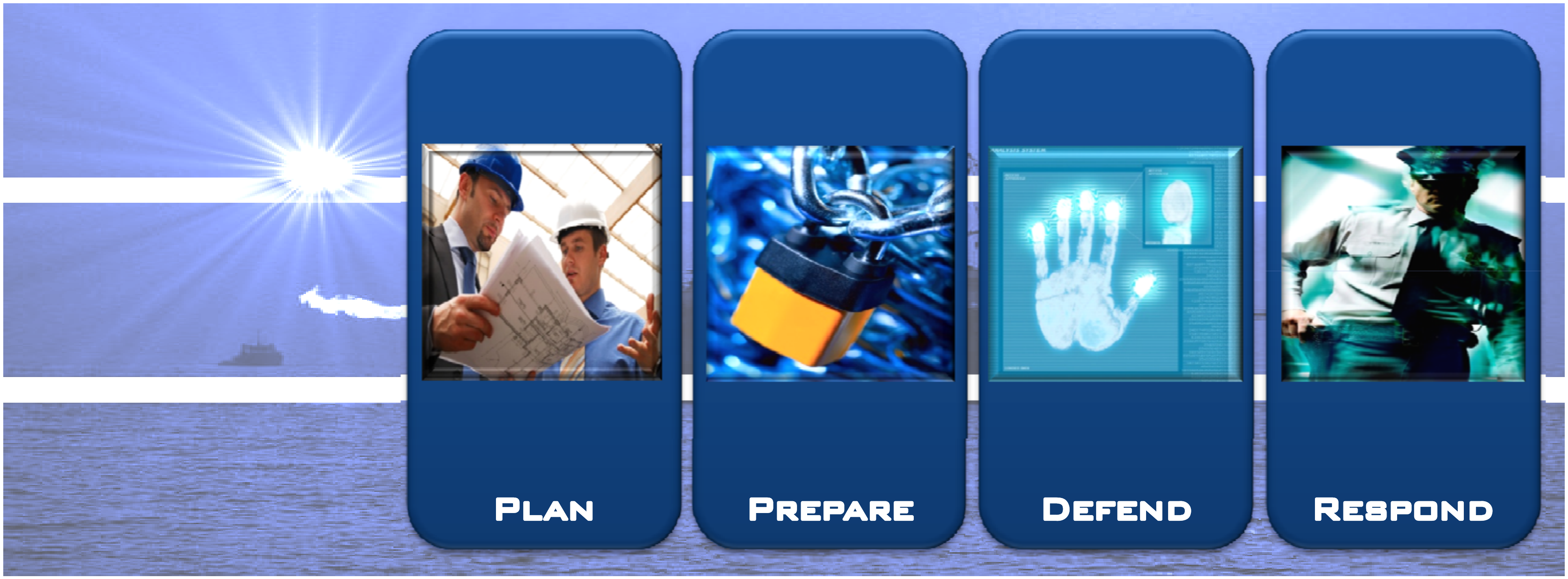
Security for Process Control



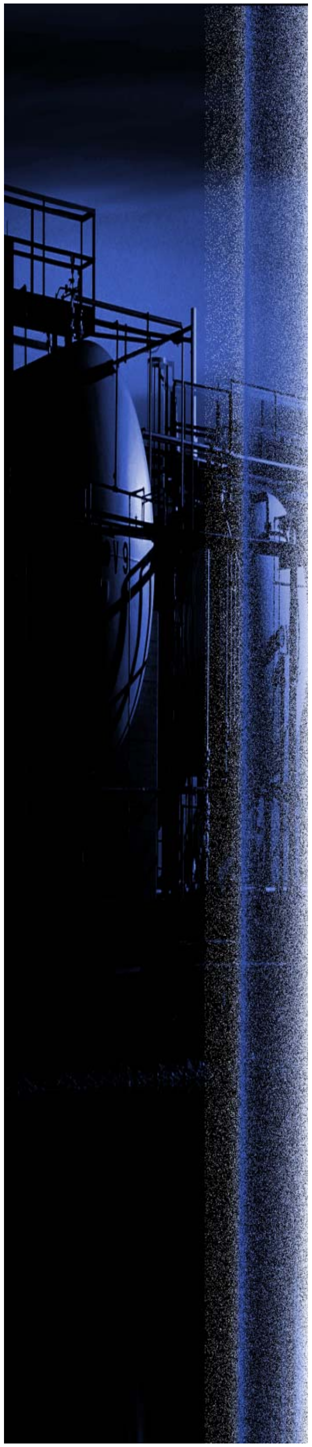
- **PHA** — Process Hazards Analysis for Safety
- **Zone / Conduit** — Break Down into Functional Areas
- **SAL Assignment** — Assign Security Assurance Level for Each Zone
- **Gap Analysis** — Determine Gaps in Installed Base or New Design
- **Design Specs** — Select Engineered Safeguards and Create Design Specs
- **Implement** — Implement Solutions
- **Validate** — Fault Injection Testing and Design Validation

Kenexis SAL Worksheets for Consistent Analysis and Recommendations

KENEXIS

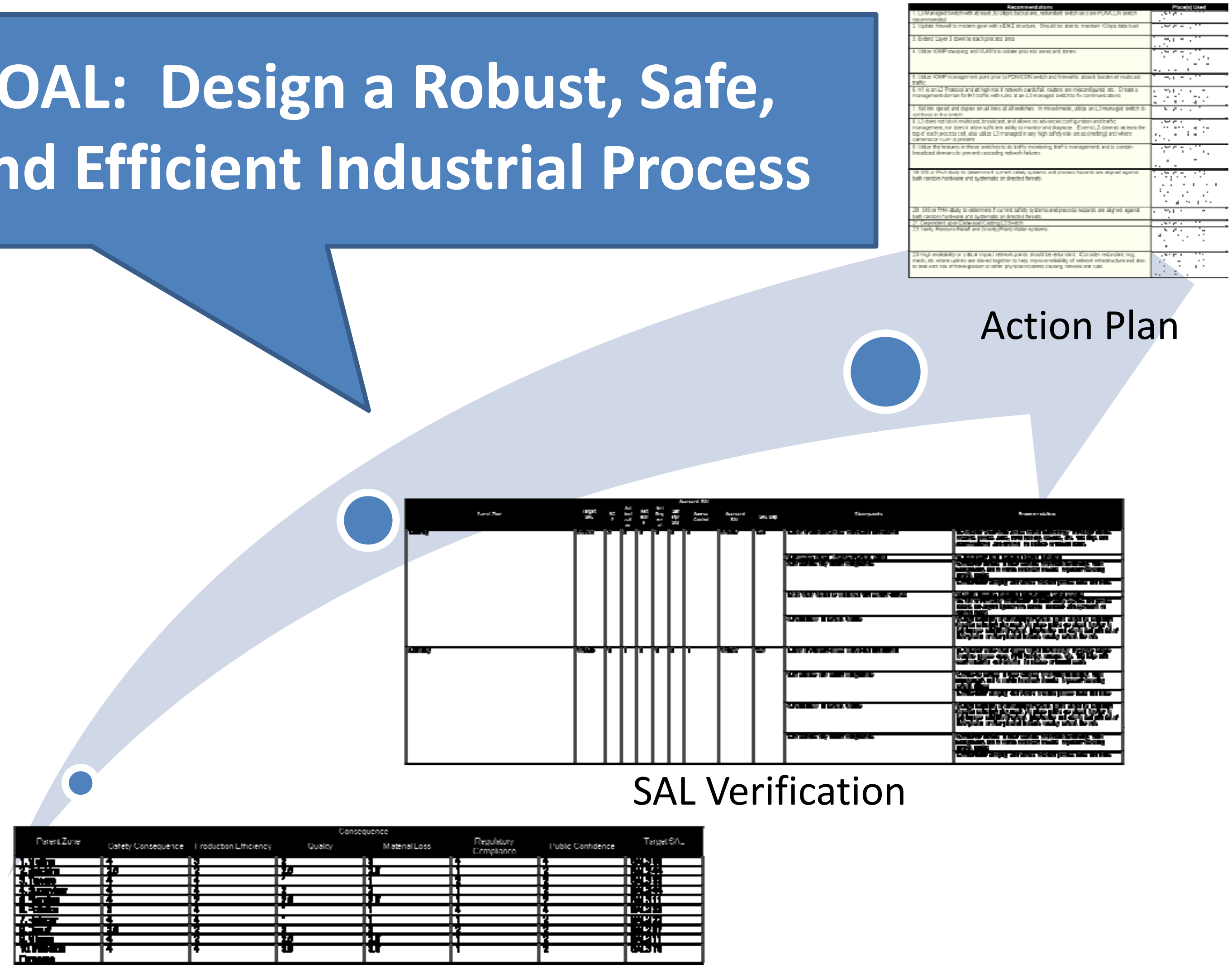


DESIGN BASIS FOR SECURITY

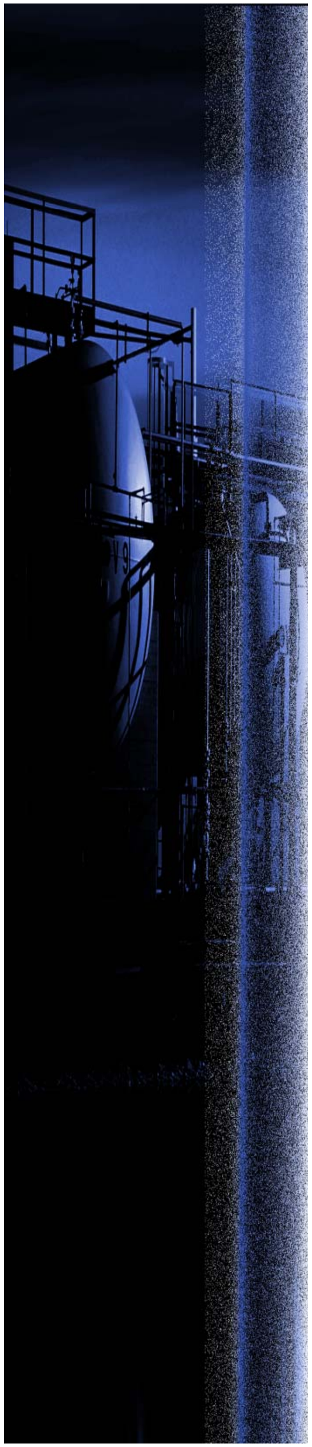


Design Basis for Security

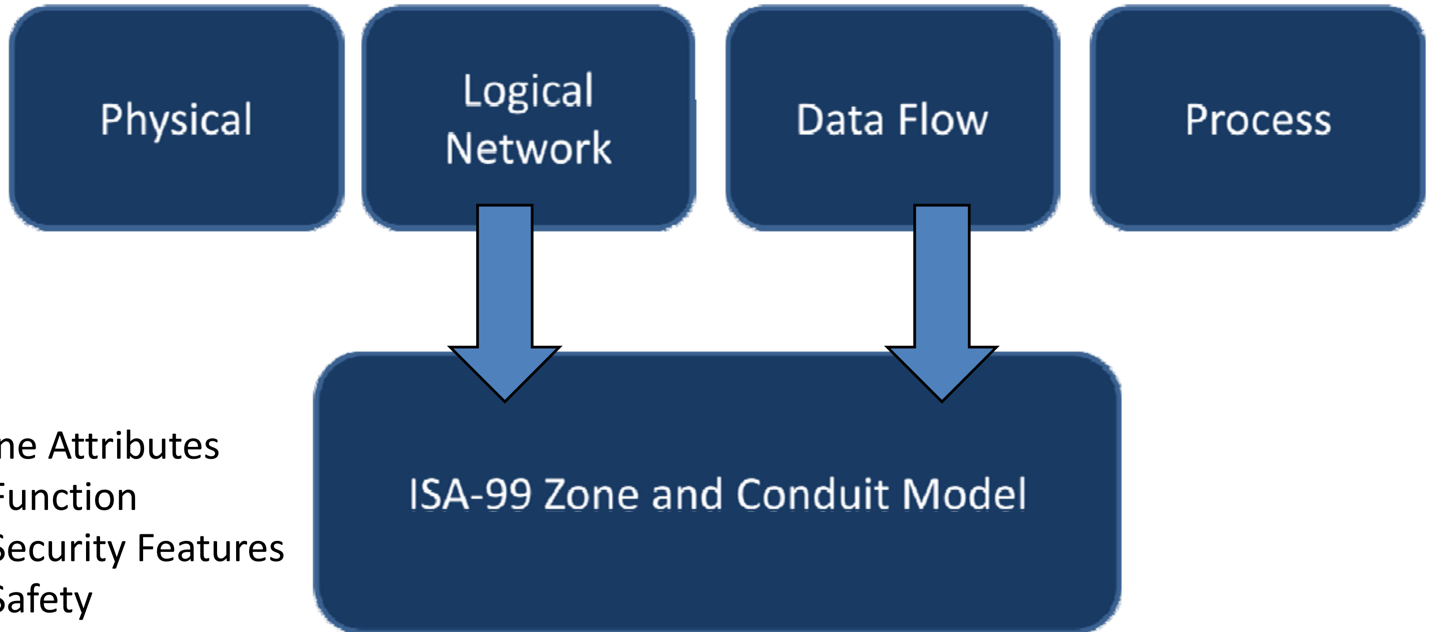
GOAL: Design a Robust, Safe, and Efficient Industrial Process



KENEXIS



Step 1 Zone and Conduit Modeling



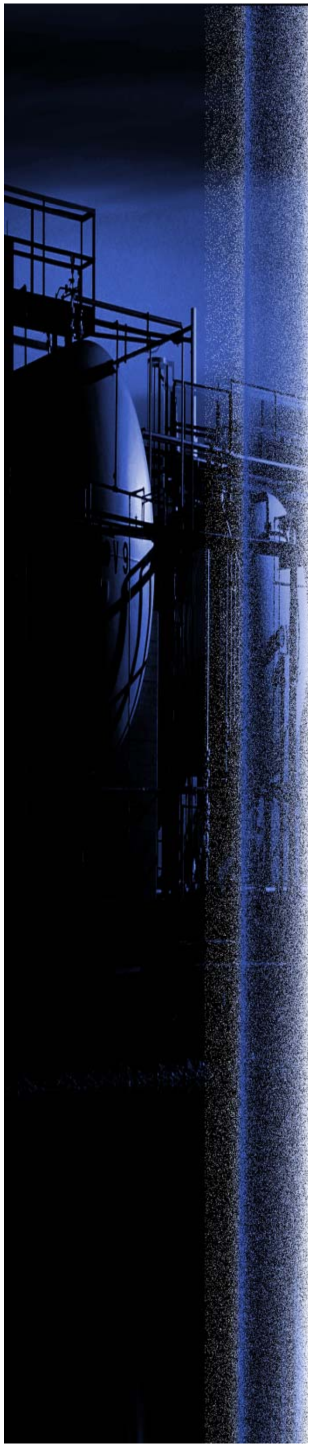
Zone Attributes

- Function
- Security Features
- Safety
- Efficiency
- Maintenance
- Quality
- Regulatory Compliance
- Parent Zone

A Logical Representation of the Environment – ranked by security requirements

SAL requirements determined by zone

KENEXIS

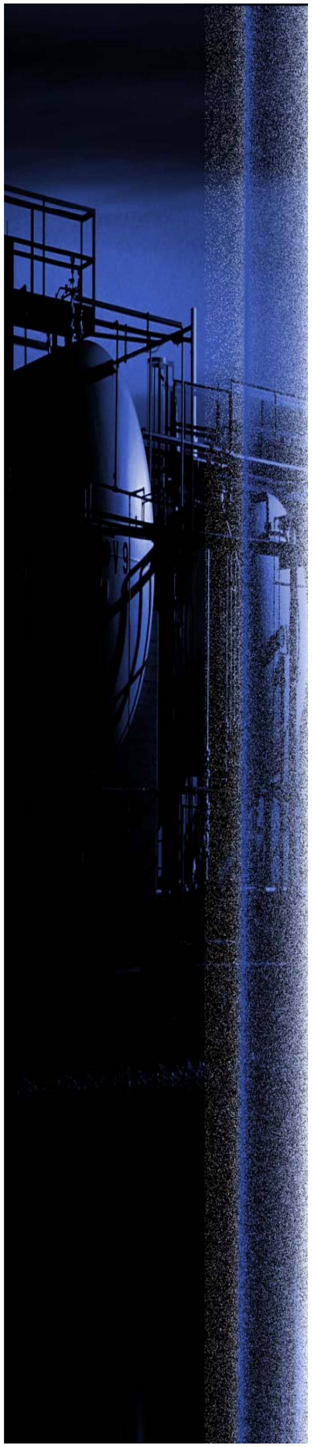


Step 2 - SAL Selection

	Consequence						
Parent Zone	Safety Consequence	Production Efficiency	Quality	Material Loss	Regulatory Compliance	Public Confidence	Target SAL
1. Melting	4	3	2	3	4	4	SAL3.89
2. Batching	2.5	2	2.5	2.5	1	2	SAL2.44
3. Towers	4	4	1	1	2	2	SAL3.33
4. Supervisor	4	4	2	2	1	2	SAL3.44
5. Blending	4	2	2.5	2.5	1	2	SAL3.11
6. Pollution	3	4	1	1	4	4	SAL3.33
7. Robicon	4	4	1	1	1	2	SAL3.22
8. Desulf	2.5	2	3	3	2	2	SAL2.67
9. Mixers	4	2	2.5	2.5	1	2	SAL3.11
10. Induction Furnaces	4	4	3.5	3.5	1	2	SAL3.78

- Customer Determines Impact Categories and Severity
- Customer Provides Weighting Factors to Respective Categories
- Kenexis calculates weighted average to provide projected/target Security Assurance Level

KENEXIS

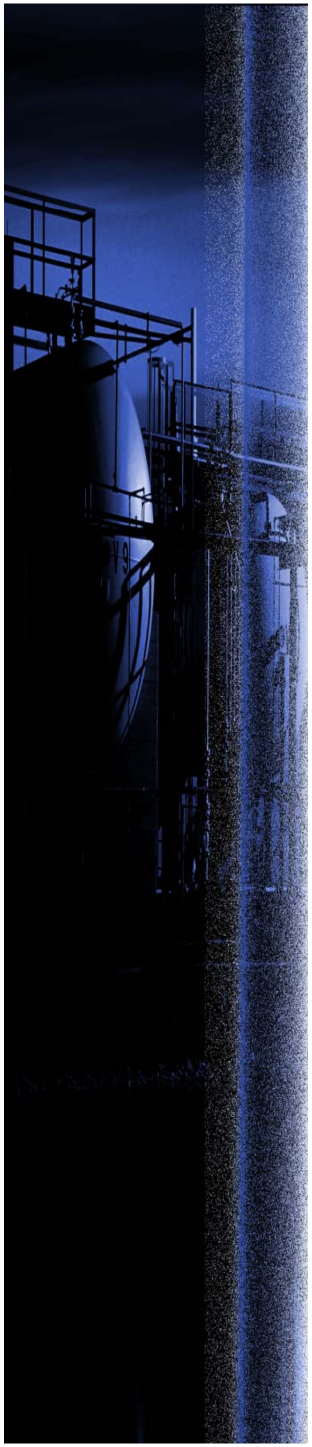


Step 3 - SAL Verification

Parent Zone	Target SAL	Assessed SAL						Assessed SAL	SAL Gap	Discrepancies	Recommendations
		BCP	Authorization	Network	Net Segment	Safety/SIS	Access Control				
1. Melting	SAL3.89	3	2	2	2	2	2	SAL2.17	1.72	1. Lack of sufficient access control and authorization	11. Consider some other access control methodology like badge readers to various process areas, RFID tracking, cameras, etc. This helps with event correlation and detection for adverse or harmful events
										2. Excessive burden / Usage of network switch	21. Dependent upon Delavaud Casting L2 Switch
										3. L3 switches only default configurations	9. Utilize the features in these switches to do traffic monitoring, traffic management, and to contain broadcast domains to prevent cascading network failures
											4. Utilize IGMP snooping and VLAN's to isolate process areas and zones
										4. SIS Study Should be conducted with security analysis	22. Verify Pressure Relief and Gravity(Plant) Water systems
											20. SIS or PHA study to determine if current safety systems and process hazards are aligned against both random hardware and systematic or directed threats
										5. Redundancy in Network Comms	23. High availability or critical impact network points should be redundant. Consider redundant ring, mesh, etc where uplinks are slaved together to help improve reliability of network infrastructure and also to deal with risk of fire/explosion or other physical incidents causing network line cuts
2. Batching	SAL2.44	2	1	2	2	2	1	SAL1.67	0.78	1. Lack of sufficient access control and authorization	11. Consider some other access control methodology like badge readers to various process areas, RFID tracking, cameras, etc. This helps with event correlation and detection for adverse or harmful events
										2. L3 switches only default configurations	9. Utilize the features in these switches to do traffic monitoring, traffic management, and to contain broadcast domains to prevent cascading network failures
											4. Utilize IGMP snooping and VLAN's to isolate process areas and zones
										3. Redundancy in Network Comms	23. High availability or critical impact network points should be redundant. Consider redundant ring, mesh, etc where uplinks are slaved together to help improve reliability of network infrastructure and also to deal with risk of fire/explosion or other physical incidents causing network line cuts
										4. L3 switches only default configurations	9. Utilize the features in these switches to do traffic monitoring, traffic management, and to contain broadcast domains to prevent cascading network failures
											4. Utilize IGMP snooping and VLAN's to isolate process areas and zones

- Kenexis Evaluates Existing Infrastructure and Planned Architecture against SAL Calculations Worksheets
- SAL GAP identified with a list of discrepancies and Recommendations for Remediation

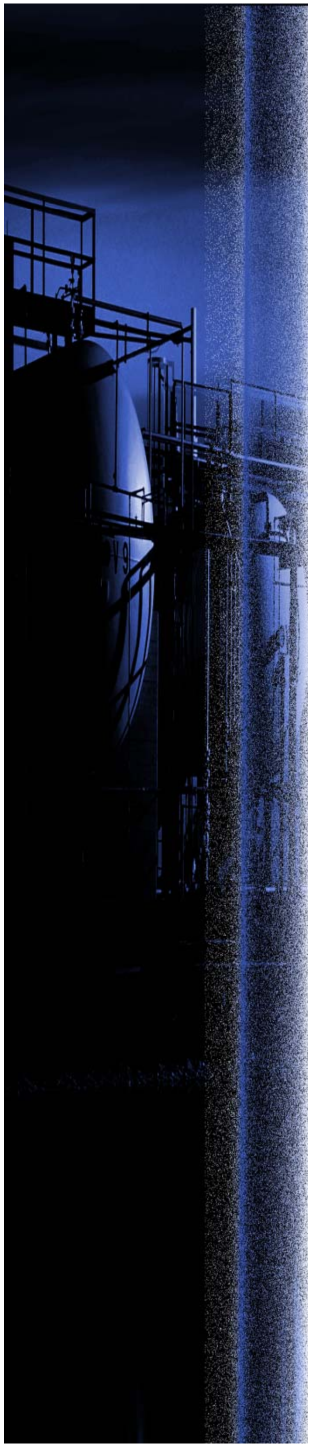
KENEXIS



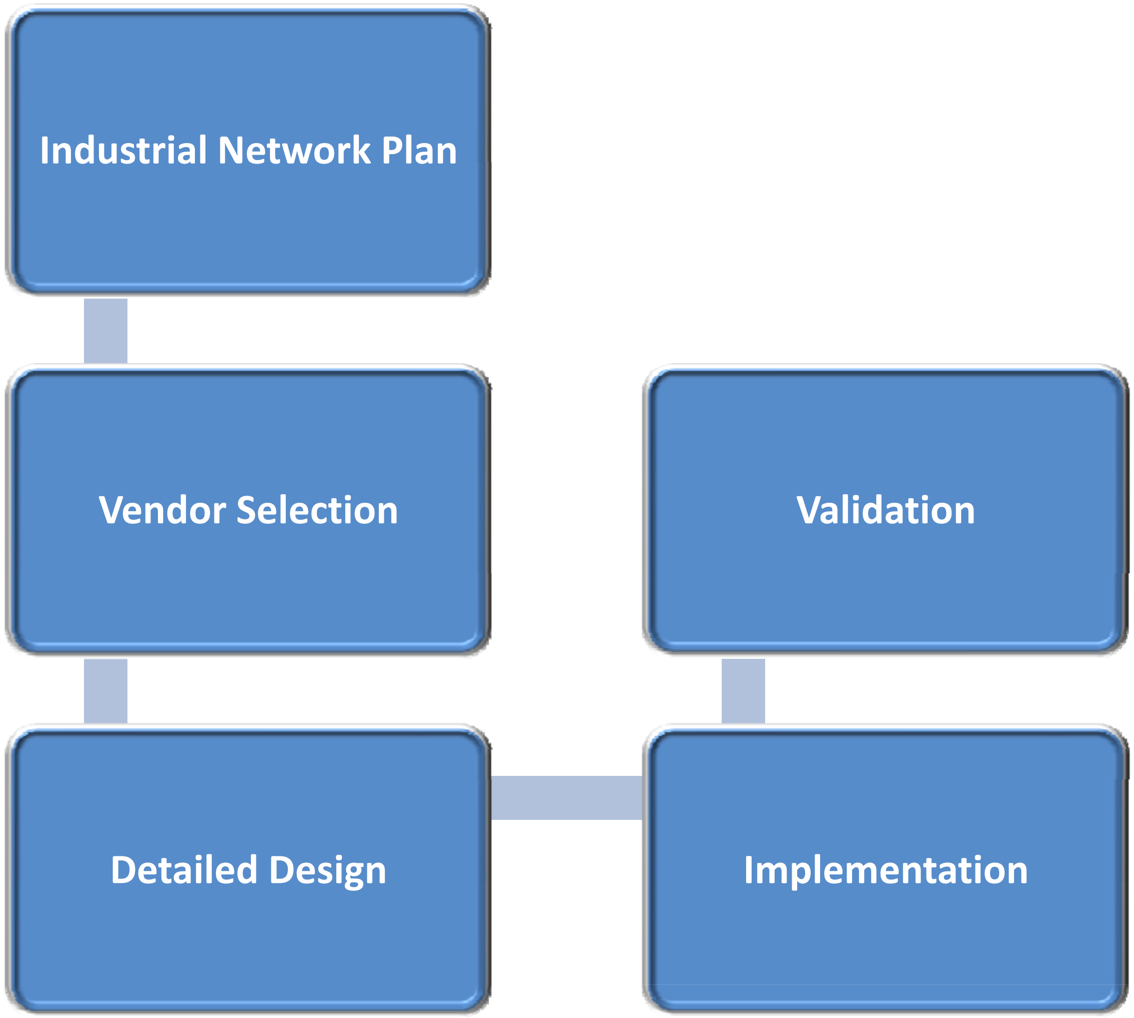
Step 4 – Recommendations and Action Plan

Recommendations	Place(s) Used
1. L3 Managed Switch with at least 20 Gbp/s backplane, redundant switch as core PDN/CDN switch recommended	Discrepancies: 2.1.1.1, 2.2.1.2
2. Update firewall to modern gear with a DMZ structure. Should be able to maintain 1Gbps data load	Discrepancies: 2.1.1.2
3. Extend Layer 3 down to each process area	Discrepancies: 2.1.1.1, 2.2.1.2
4. Utilize IGMP snooping and VLAN's to isolate process areas and zones	Discrepancies: 2.1.1.3, 3.1.1.3, 3.2.1.2, 3.2.1.4, 3.3.1.2, 3.3.1.3, 4.1.1.4, 4.2.1.4, 4.3.1.4
5. Utilize IGMP management point prior to PDN/CDN switch and firewall to absorb burden of multicast traffic	Discrepancies: 2.1.1.3
6. H1 is an L2 Protocol and at high risk if network cards fail, routers are misconfigured, etc. Create a management domain for H1 traffic with rules at an L3 managed switch to fix communications	Discrepancies: 2.1.1.4, 4.1.1.2, 4.1.1.3, 4.2.1.2, 4.2.1.3, 4.3.1.2, 4.3.1.3
7. Set link speed and duplex on all links at all switches. In mixed mode, utilize an L3 managed switch to set these in the switch	Discrepancies: 2.1.1.7
8. L2 does not block multicast, broadcast, and allows no advanced configuration and traffic management, nor does it allow sufficient ability to monitor and diagnose. Extend L3 down to at least the top of each process cell, also utilize L3 managed in any high safety risk areas (melting) and where cameras or VOIP is present	Discrepancies: 1.6.1.2, 2.1.1.5, 4.1.1.3, 4.1.1.4, 4.2.1.3, 4.2.1.4, 4.3.1.3, 4.3.1.4
9. Utilize the features in these switches to do traffic monitoring, traffic management, and to contain broadcast domains to prevent cascading network failures	Discrepancies: 2.1.1.6, 3.1.1.3, 3.2.1.2, 3.2.1.4, 3.3.1.2, 3.3.1.3, 4.1.1.3, 4.2.1.3, 4.3.1.3
19. SIS or PHA study to determine if current safety systems and process hazards are aligned against both random hardware and systematic or directed threats	Discrepancies: 1.6.1.4, 1.10.1.4, 1.11.1.3, 1.13.1.3, 1.14.1.4, 1.15.1.4, 1.16.1.4, 3.4.1.2, 3.5.1.2, 3.6.1.2, 3.7.1.2, 3.8.1.3, 3.9.1.3, 3.10.1.2, 4.1.1.5, 4.2.1.5
20. SIS or PHA study to determine if current safety systems and process hazards are aligned against both random hardware and systematic or directed threats	Discrepancies: 1.1.1.4, 3.1.1.4
21. Dependent upon Delavaud Casting L2 Switch	Discrepancies: 3.1.1.2
22. Verify Pressure Relief and Gravity(Plant) Water systems	Discrepancies: 3.1.1.4, 3.4.1.2, 3.5.1.2, 3.6.1.2, 3.7.1.2, 3.8.1.3, 3.9.1.3, 3.10.1.2
23. High availability or critical impact network points should be redundant. Consider redundant ring, mesh, etc where uplinks are slaved together to help improve reliability of network infrastructure and also to deal with risk of fire/explosion or other physical incidents causing network line cuts	Discrepancies: 3.1.1.5, 3.2.1.3, 3.4.1.3, 3.5.1.3, 3.6.1.3, 3.7.1.3, 4.1.1.2, 4.2.1.2, 4.3.1.2

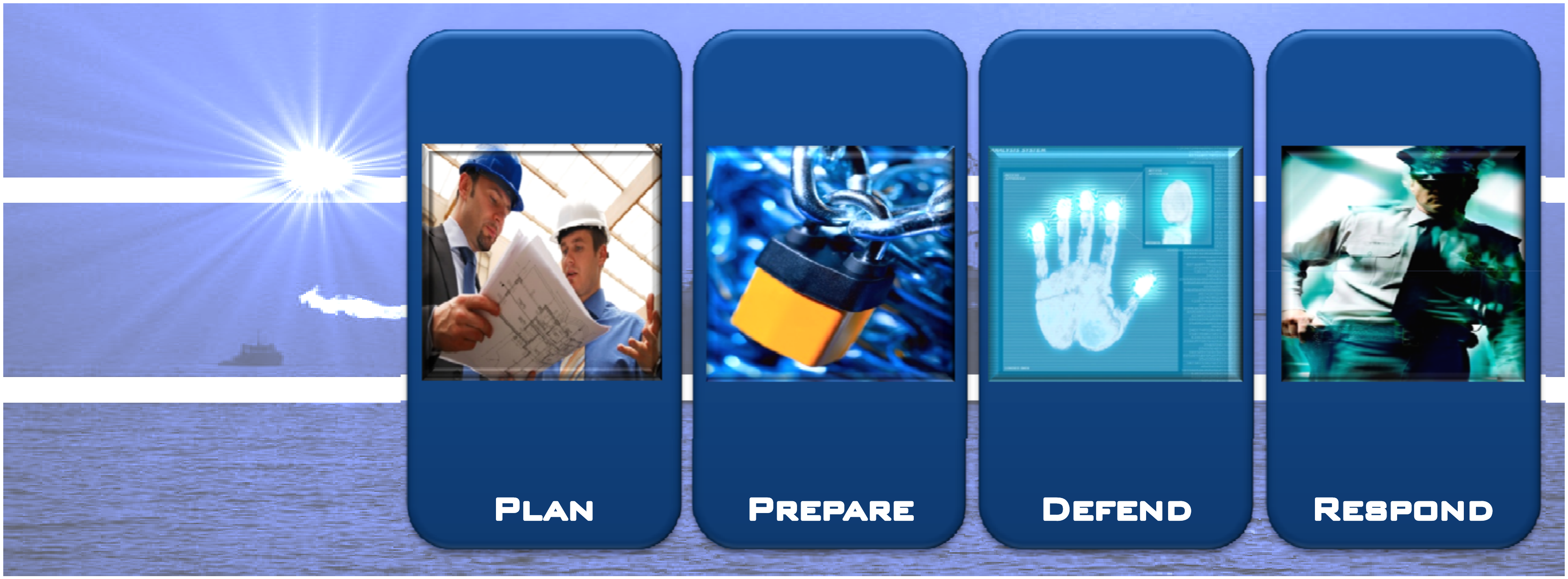
KENEXIS



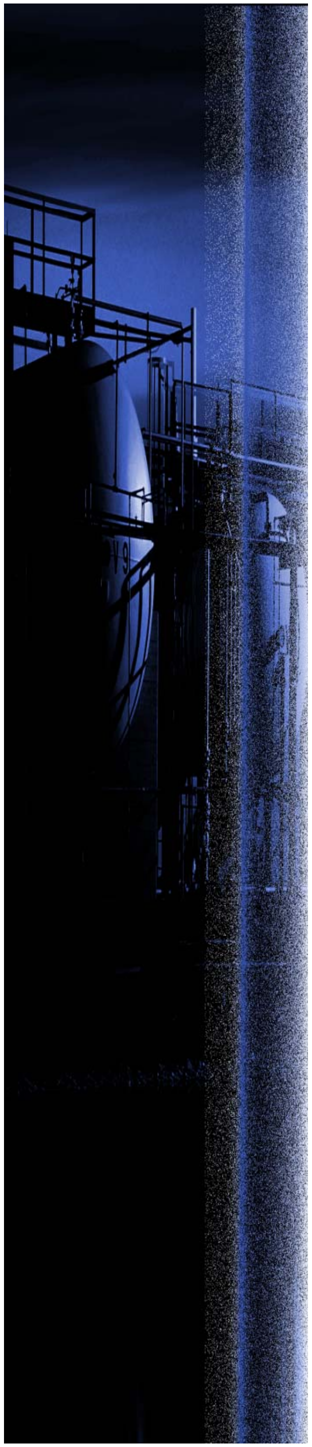
Design Basis: Next Steps



KENEXIS

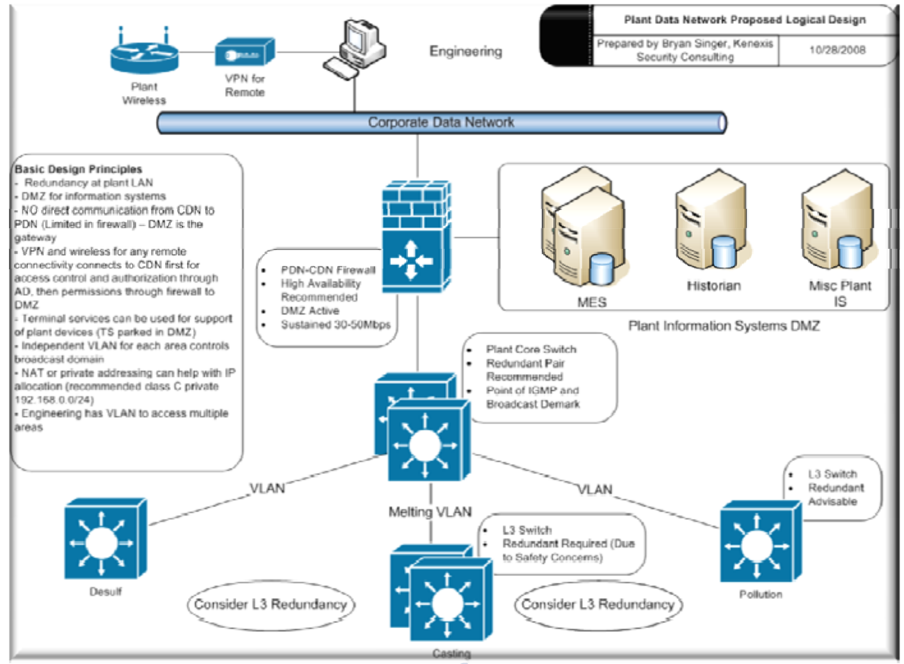


INDUSTRIAL NETWORK DESIGN BASIS



Industrial Network Design Basis

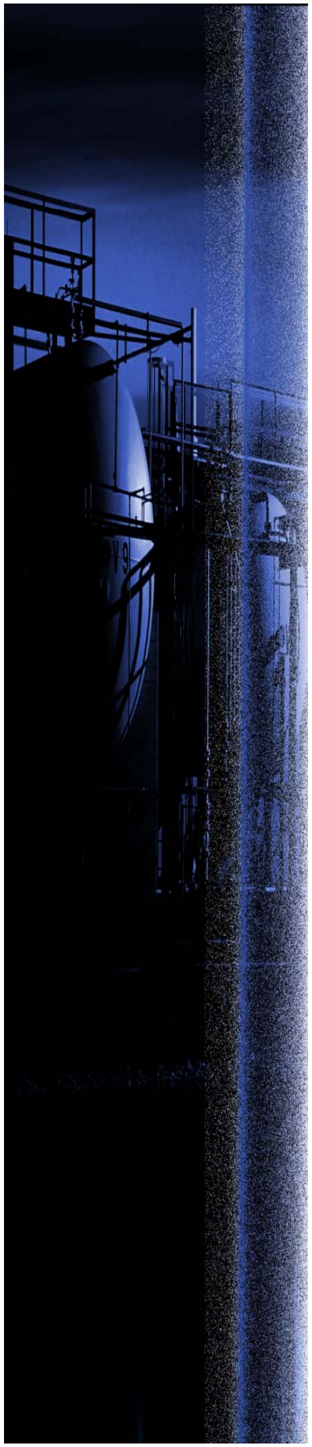
GOAL: Implement an Efficient and Reliable Network Architecture



Future State Network Design

Industrial Network Assessment and Growth Plan

KENEXIS



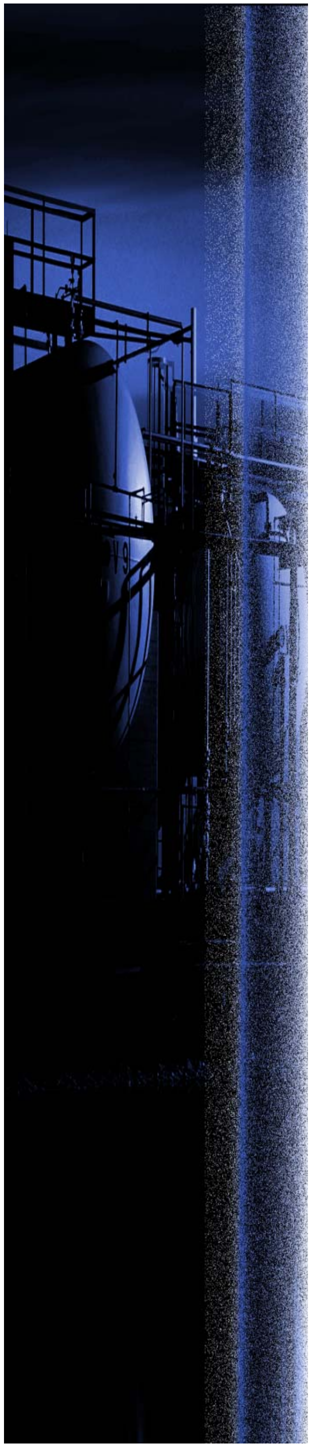
Step 1 Consequence Modeling

	Sensors/Meters	Valves/Actuators	Driver/Motors	Controllers	HMI	DCS/SCADA	Historians/OM Intelligence	MES	ERP	Corporate Network	Plant Network
Sensors/Meters	X	SECQF	SECQRF	ECRQF	ERQF	RQF	RQF	RQF			SECIRQF
Valves/Actuators	SECQF		SECQRF	ECRQF	ERQF	RQF	RQF	RQF			SECIRQF
Driver/Motors	SECQF	SECQF	X	ECRQF	ERQF	RQF	RQF	RQF			SECIRQF
Controllers	SECQF	SECQF	SECQF	X	ERQF	RQF	RQF	RQF			SECIRQF
HMI	SECIRQF	SECIRQF	SECIRQF	SECIRQF	X	RQIF	RQIF	CIRQF			SECIRQF
DCS/SCADA	SECIRQF	SECIRQF	SECIRQF	SECIRQF	ECIRQF	X	RQIF	CIRQF	CIRQF		SECIRQF
Historians/OM Intelligence	ECIRQF	ECIRQF	SECIRQF	SECIRQF	ECIRQF	RQIF	X	CIRQF	CIRQF		ECIRQF
MES***	ECIRQF	ECIRQF	SECIRQF	SECIRQF	ECIRQF	RQIF	IRQF	CIRQF	CIRQF	CIRF	CIRQF
ERP						IRQF	IRQF	D	X	CIRF	CIRQF
Corporate Network**								EECIRQF	EECIRQF	X	
Plant Network	SECIRQF	SECIRQF	SECIRQF	SECIRQF	SECIRQF	SECIRQF	ECIRQF	ECIRQF	ECIRQF		X
* Assumes that HMI is required for process											
** Assumes Generally Accepted Practice of Isolating Process from Corporate or Data Networks											
*** Assumes MES not needed for Production											

S	Safety
E	Efficiency
C	Confidence
I	IP Loss
R	Regulatory
Q	Quality
F	Financial

- Failure of the Plant Data Network has Immediate and Significant Issues
- Industry Average Time to Detect and Recover from Industrial Switch Failure is 3-6 Hours!

KENEXIS

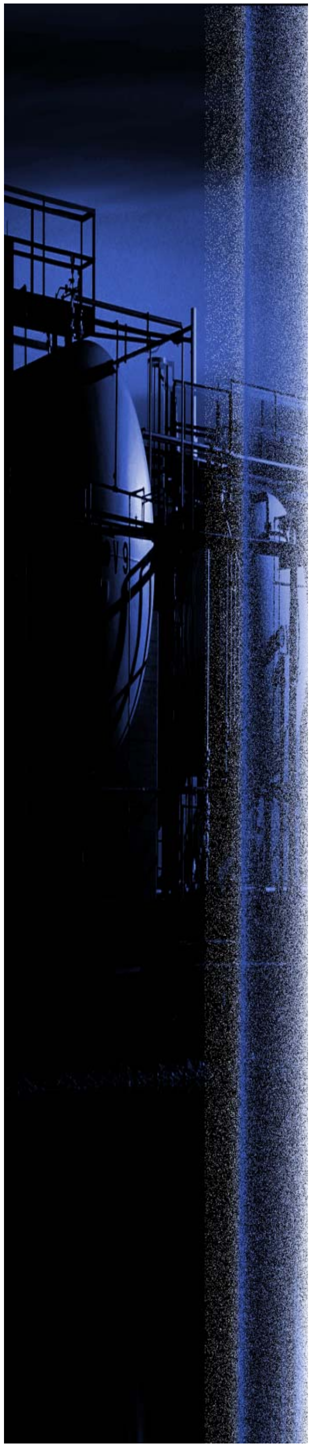


Step 2 Industrial Network Plan

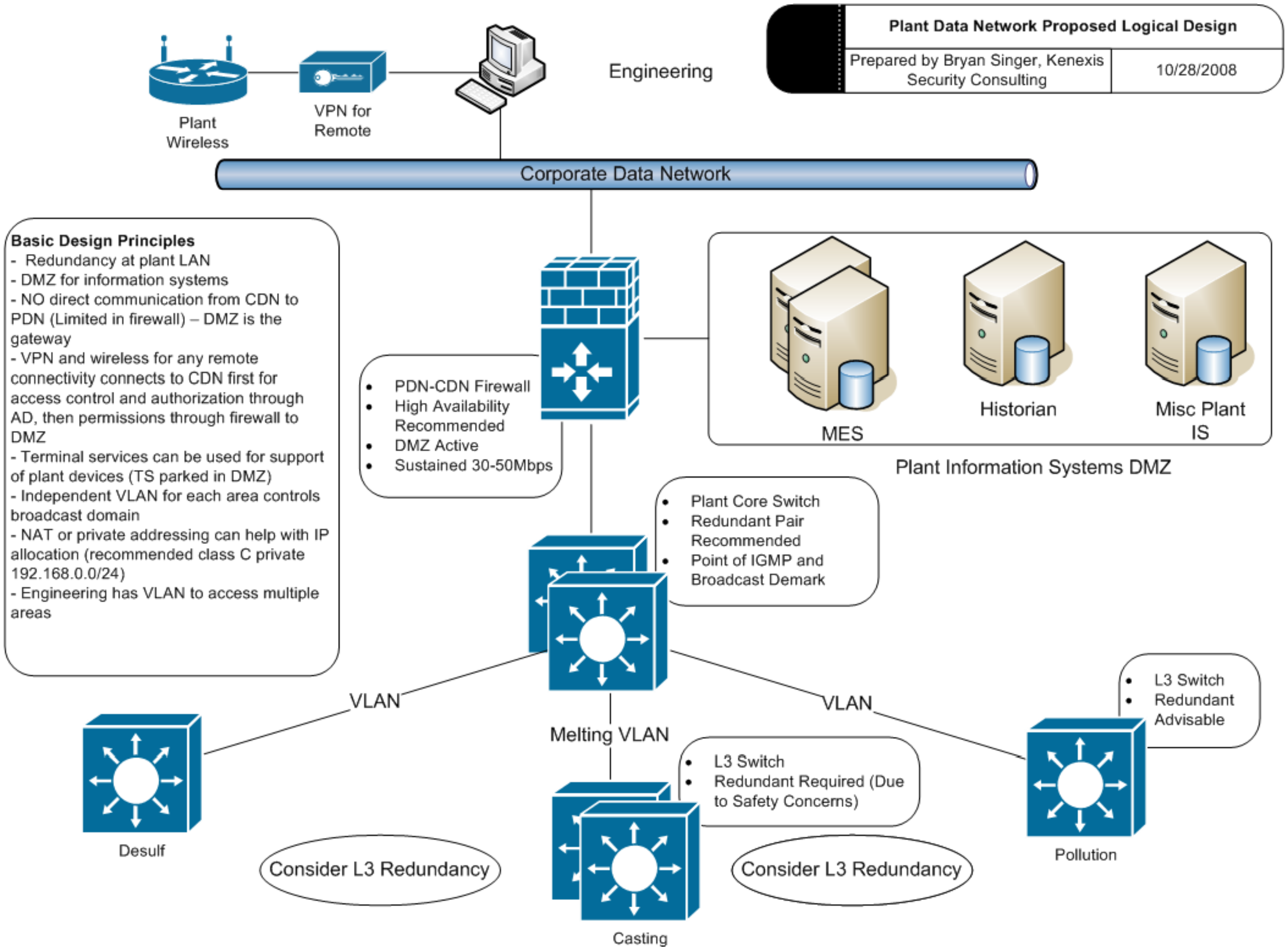
Parent Zone	Network Calculations																
									Target Increase								
	Servers	Workstation Counts	Processors	I/O Count	IP Cameras	Switches	Power Meters	Peak Capacity	Servers	Workstations	Processors	I/O Count	IP Cameras	Switches	Power Meters	Network Increase	Target Network Load
1. Melting	2	26	8	1606	10	1	13	9Mb/s	0	3	0	0	0	2	0	27.80%	11.50Mb/s
2. Batching	1	2	1	262	0	1	0	3Mb/s	0	0	0	0	0	0	0	3.01%	3.09Mb/s
3. Cooling Towers	0	0	2	1241	0	1	0	4Mb/s	1	0	0	0	0	0	0	8.63%	4.35Mb/s
4. Supervisor	4	14	1	2152	0	1	0	9Mb/s	1	3	0	0	0	2	0	22.04%	10.98Mb/s
5. Blend	1	7	1	746	0	1	0	8Mb/s	0	3	0	0	0	0	0	8.54%	8.68Mb/s
6. Pollution	1	3	1	984	0	1	0	4Mb/s	0	0	0	0	0	0	0	7.84%	4.31Mb/s
7. Robicon	2	8	4	1696	0	1	13	7Mb/s	1	0	0	0	0	0	0	15.64%	8.09Mb/s
8. Desulf	1	3	1	496	0	1	0	3Mb/s	0	1	0	650	0	0	0	9.17%	3.27Mb/s
9. Mixers	1	4	2	152	0	1	0	3Mb/s	0	1	0	0	0	0	0	3.39%	3.10Mb/s
10. Induction Furnaces	1	7	2	400	0	1	0	3Mb/s	0	1	1	0	0	0	0	6%	3.18Mb/s

- Inventory of Network Assets, I/O, etc
- Projected Growth and Traffic Loads

KENEXIS

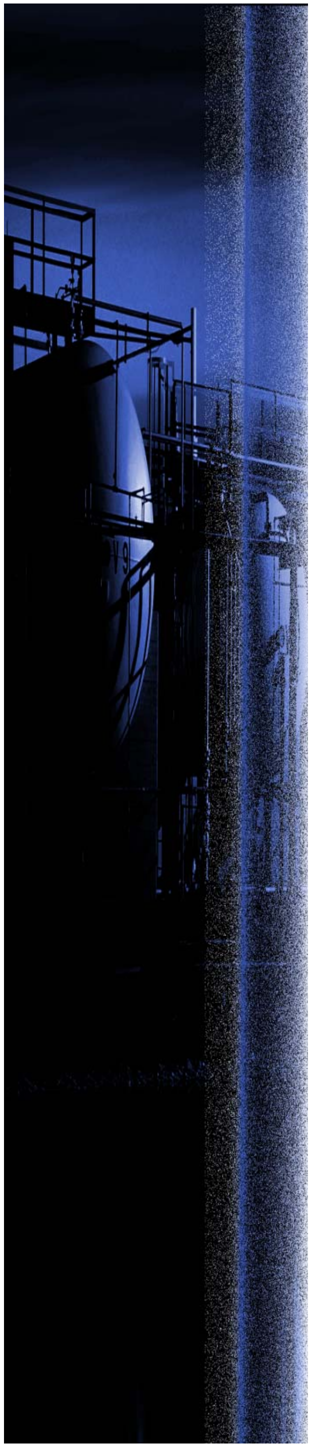


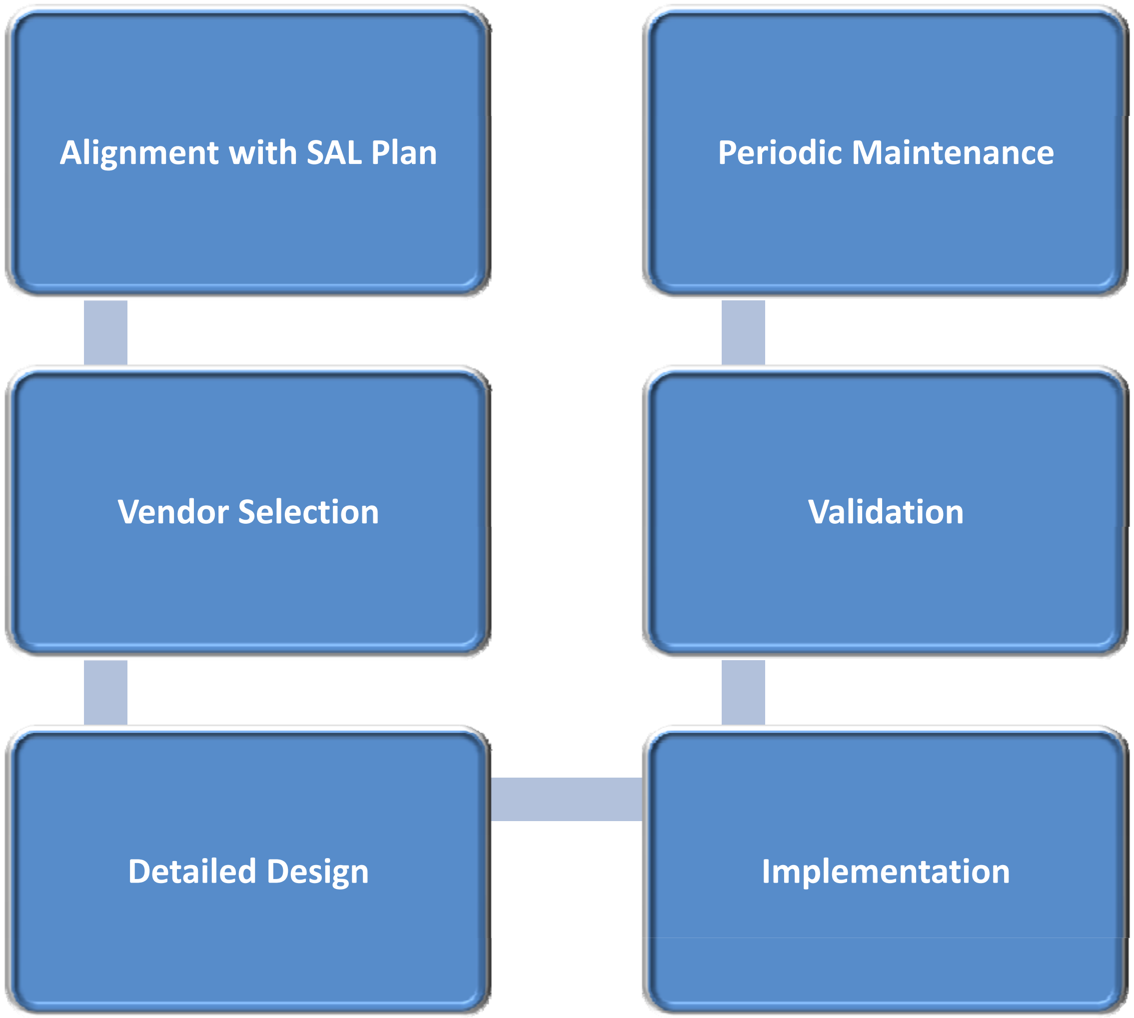
Step 3 – Logical Design



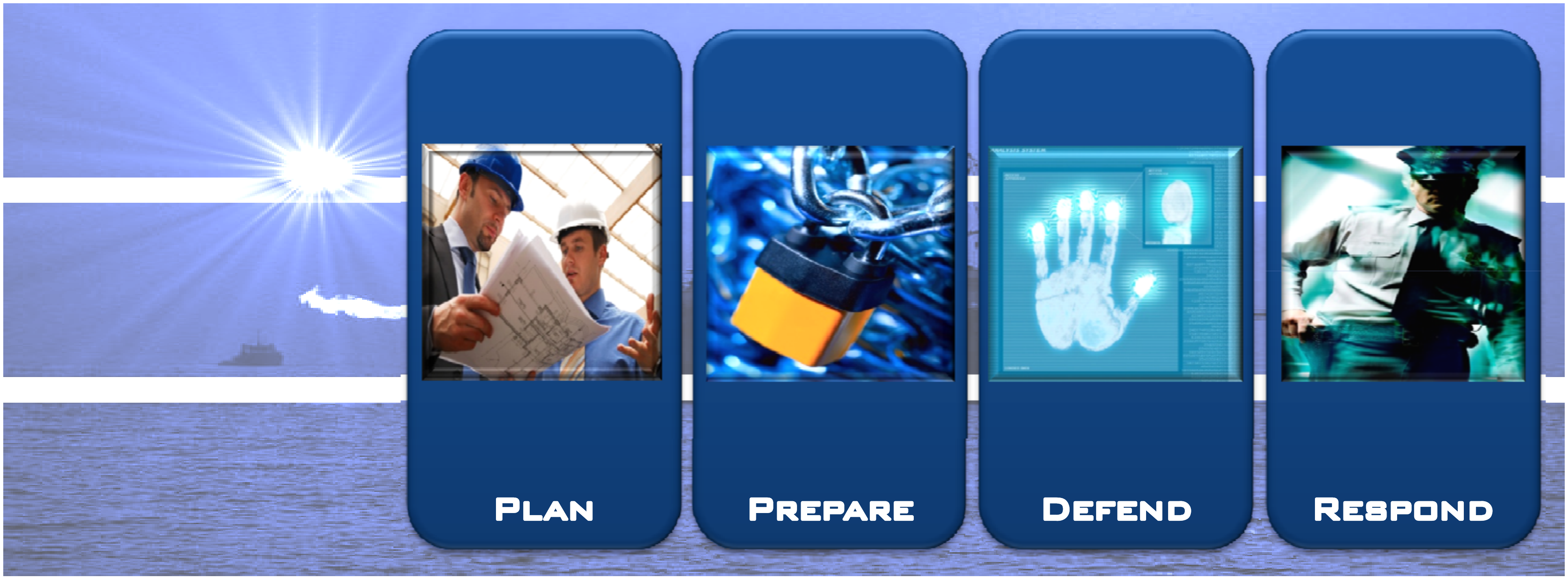
KENEXIS

Industrial Network Design Basis: Next Steps

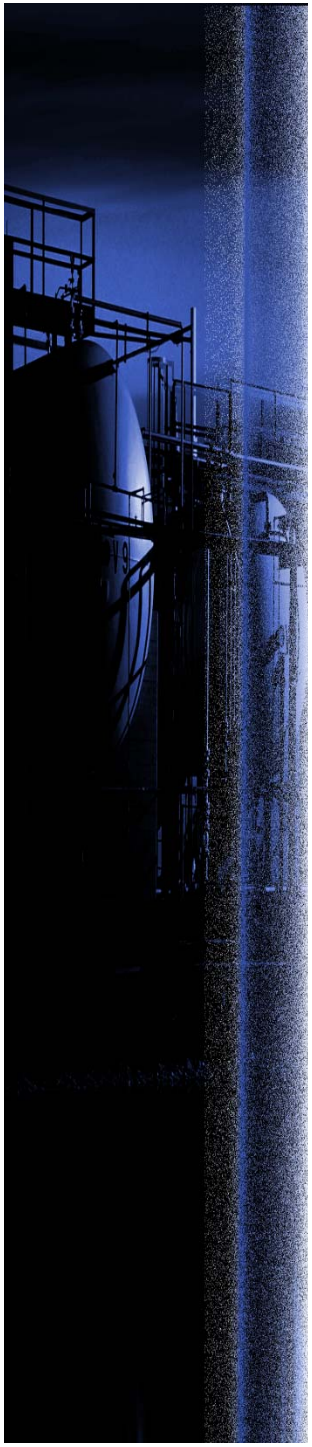




KENEXIS



TRAINING AND AWARENESS



Industrial Security Training Classes

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

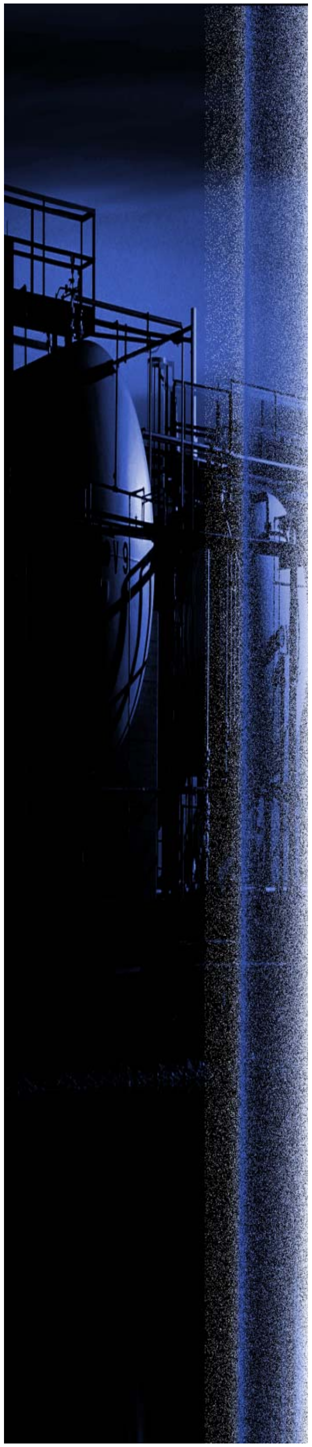
- Emerging Legislation and Standards (CFATS, NERC CIP, ISA-99, etc)
- Industrial Security Risk Management Practices and Technologies
- Lab: Attack Trends and Methods, Scenario Modeling, Attack Simulation
- 12 Hours

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

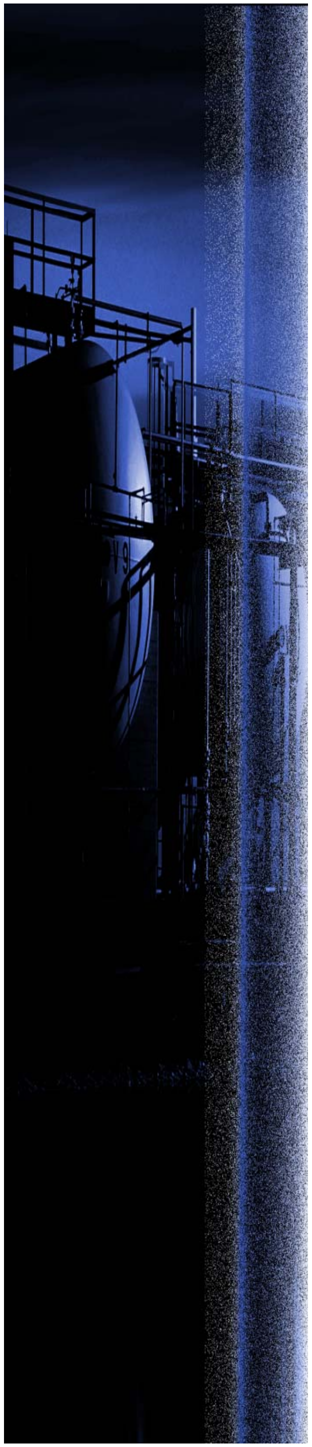
May be combined and consolidated depending on class needs

KENEXIS



Training Class Overviews

- Training Advantages with KENEXIS
  - Partnered with Lofty Perch to Offer Industry recognized and Leading cyber Security solutions such as the Idaho National Labs Training Modules
  - All Instructors are dedicated professionals with at least 15 years of experience
  - Flexible Location Options for convenience and privacy, including onsite
  - Classes may be customized per needs or combined with other service offerings
  - Customer focused and dynamic, classes are more like a workshop experience where real-world experience is leveraged in-line with training



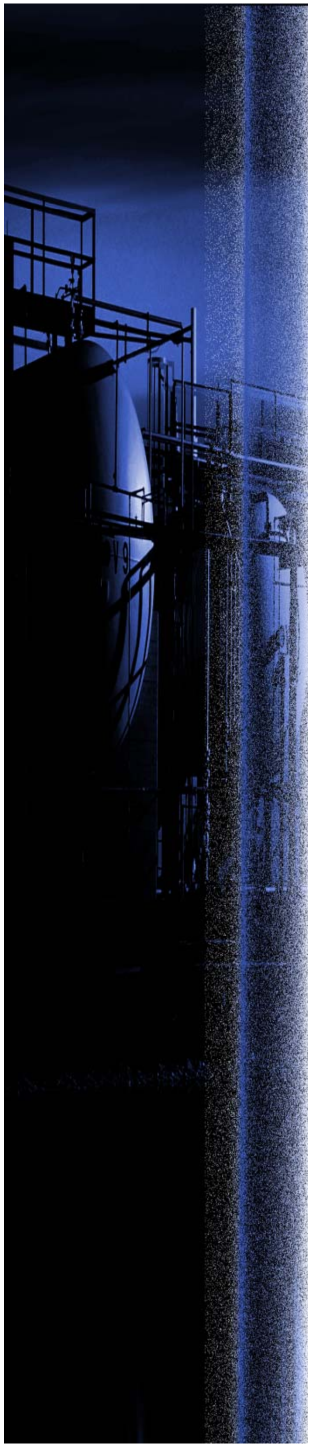
Introduction to Industrial Ethernet Networking

Overview of Networking	
	Introduction to Network Protocols
	OSI 7 Layer
	Overview of Ethernet 802.3
	Overview of Wireless 802.11x
	Industrial Protocol Summary
Network Devices	
	Hubs
	Switches
	Routers
	Bridges
	Firewalls
	Intrusion Detection Systems
	ACL
	VLAN
Lab	
	Packet Capture
	Packet Analysis
	IP Routing Exercise
	IP Network Configurations Exercise
	Industrial Network Topologies and Design
	Network Stress Tools
Network Design and Implementation	
	Physical Media - Fiber, twisted pair, UTP, STP, wireless spectrum management
	Network Topologies (Star, Ring, Mesh, Bus, etc)
	IP Addressing
	Network Security Architectures
	Considerations for Industrial Deployment

Course provides an overview of industrial networking including in depth discussions about networking technologies, topologies, and design.

Class Features:

- 12-16 hours Total Training
- Lab with packet analysis and troubleshooting
- Detailed Analysis of Common Industrial Network Failure Modes



Introduction to Industrial Security

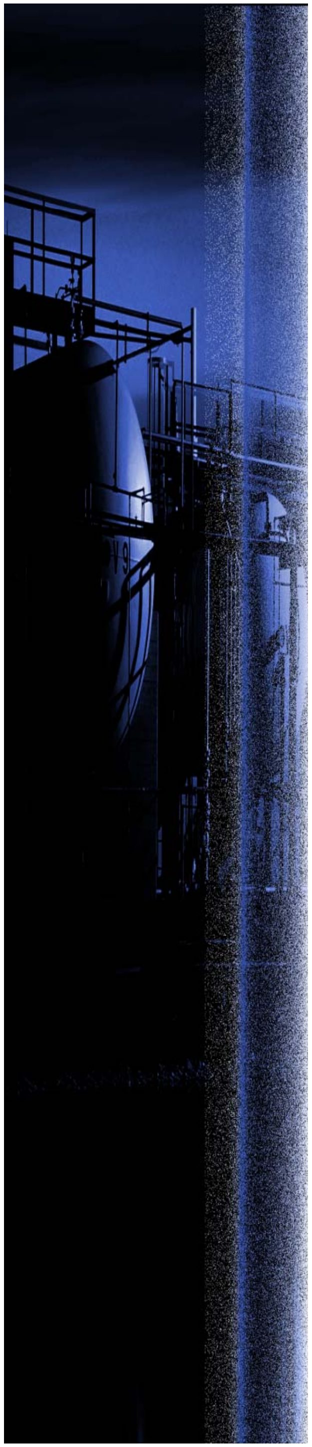
Industrial Security	
	Security Incidents and Trends
	Business Case for industrial Security
	Industrial Security Architectures
	Industrial Security Standards - ISA-99
	Regulatory Issues (CFATS, NERC, etc)
	Emerging Standards and Guidelines (NIST 800-53, 82, etc)
Lab	
	Packet Capture
	Packet Analysis
	Security Vulnerabilities and Exploits
	Scenario Modeling and War Games
	Common Security Tools (Nessus, sniffers, nmap, etc)

Course focuses on emerging attack trends, vulnerabilities in process control systems, and emerging standards and regulatory requirements.

Class Features:

- 12-16 hours Total Training
- In depth analysis of standards and regulatory requirements such as ISA-99, NERC CIP, NIST 800-53, CFATS, etc
- Lab including security vulnerabilities and industrial security network design

KENEXIS



Advanced Industrial Security

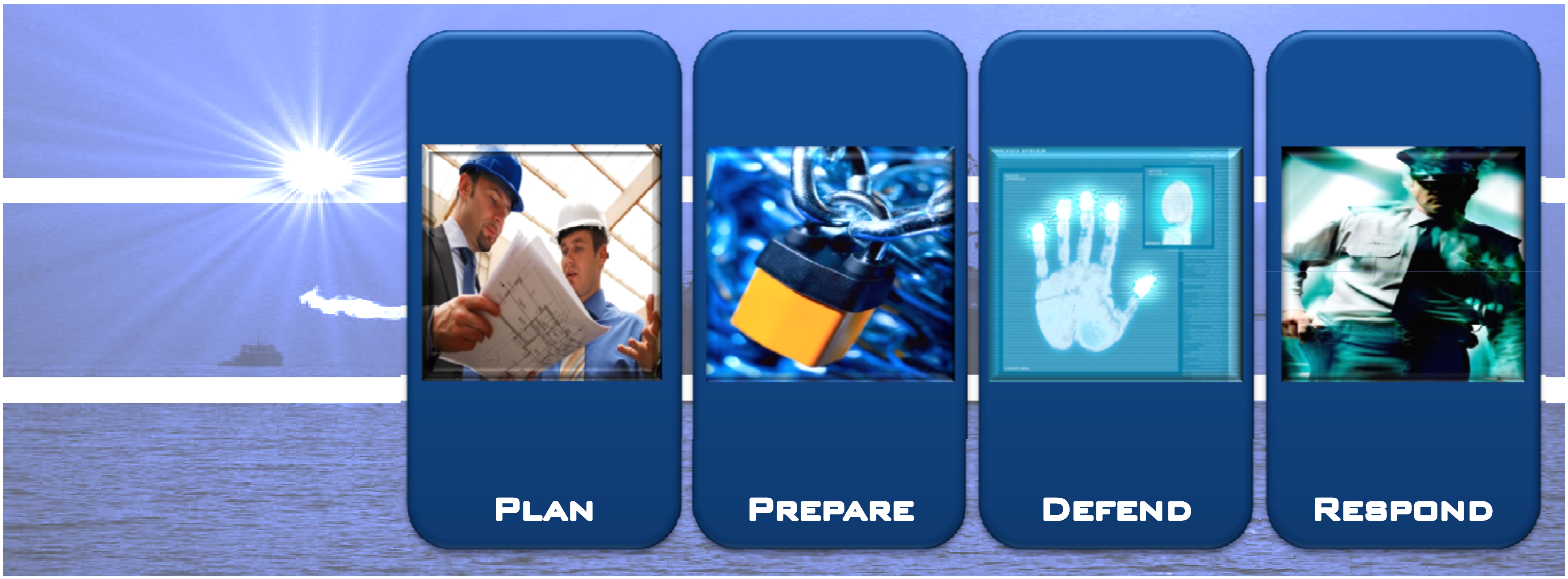
Advanced Industrial Security	
	Process Hazards Analysis for Security
	Security Assurance Levels
	SAL Selection and Verification
	Network Calculations, Projections, and Design
	Leveraging Existing Historians, OEE, MES, Historians, etc
	ROI for Security and Cost of Capital Improvements from Security
Lab	
	SAL Identification, Selection, and Verification
	Determining the Appropriate Course of Action
	Network Traffic Analysis and Data Flow Modeling
	Advanced Security Scenarios (Option for Law Enforcement Only Training as well)
	Incident Response and Forensics Overview

Course offers the latest in industry trends for improving the overall system security for automation and process control. Also takes an "out of the box" view of existing process intelligence applications such as OEE, LIMS, MES, ERP, etc to see how these systems can be leveraged as part of a security program

Class Features:

- 12-16 hours Total Training
- Law Enforcement Only Option for Attack Trends and Forensics
- In depth look at security vulnerabilities, exploits, and process hazard conditions not necessarily covered by existing SIL disciplines

KENEXIS



QUESTIONS?


KENEXIS
Thank You for Attending