



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

Copyright © 2008 Kenexis Security Corporation



PLAN



PREPARE



DEFEND



RESPOND

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

Copyright © 2008 Kenexis Security Corporation

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

Copyright © 2008 Kenexis Security Corporation

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**

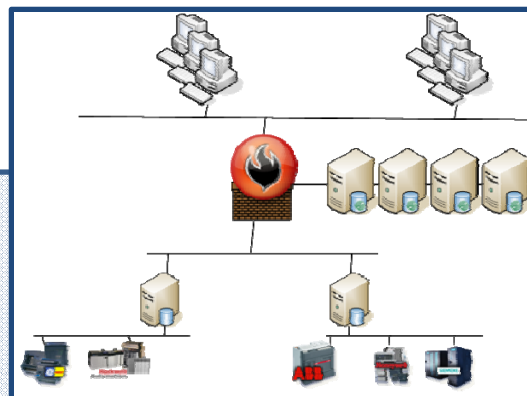
KENEXIS

Copyright © 2008 Kenexis Security Corporation

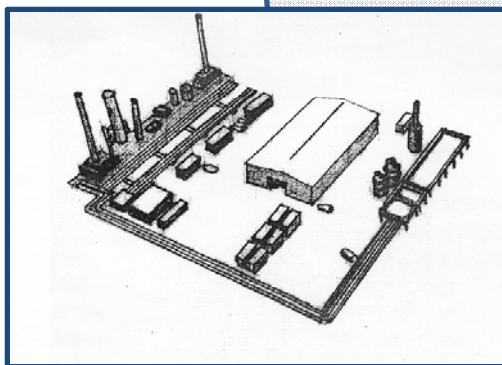
Where Should We Focus?



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

Copyright © 2008 Kenexis Security Corporation



Vulnerability Taxonomies in Process Control

Vulnerability Type	Technical Skill	Process Knowledge	Desired Outcomes
Network and Infrastructure	Moderate	Low	<ul style="list-style-type: none">• Deny, Disrupt, Deter Communications• Shutdowns• Passive Reconnaissance• Active Damage widespread
Devices and Endpoint Vulnerabilities	Mod-High	None-Low	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Catastrophic shutdowns and failures• Permanent System Damage• Retribution

KENEXIS

Copyright © 2008 Kenexis Security Corporation



PLAN



PREPARE



DEFEND



RESPOND

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

Copyright © 2008 Kenexis Security Corporation

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

Copyright © 2008 Kenexis Security Corporation

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

Copyright © 2008 Kenexis Security Corporation

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

Copyright © 2008 Kenexis Security Corporation

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

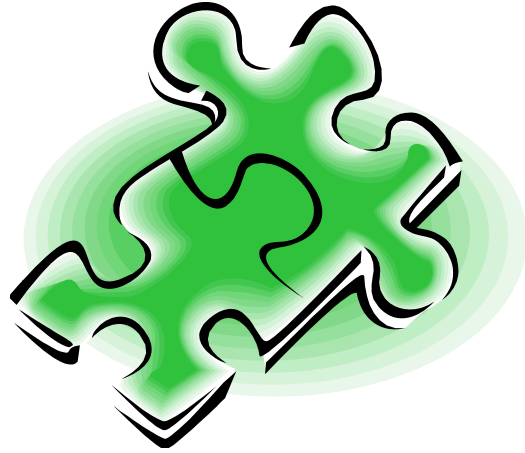
- Extensive redundancy in network and controls, heavy protection in SIS, strong authentication, heavy awareness
- Mass casualty or catastrophic failure scenarios, irrecoverable

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

KENEXIS

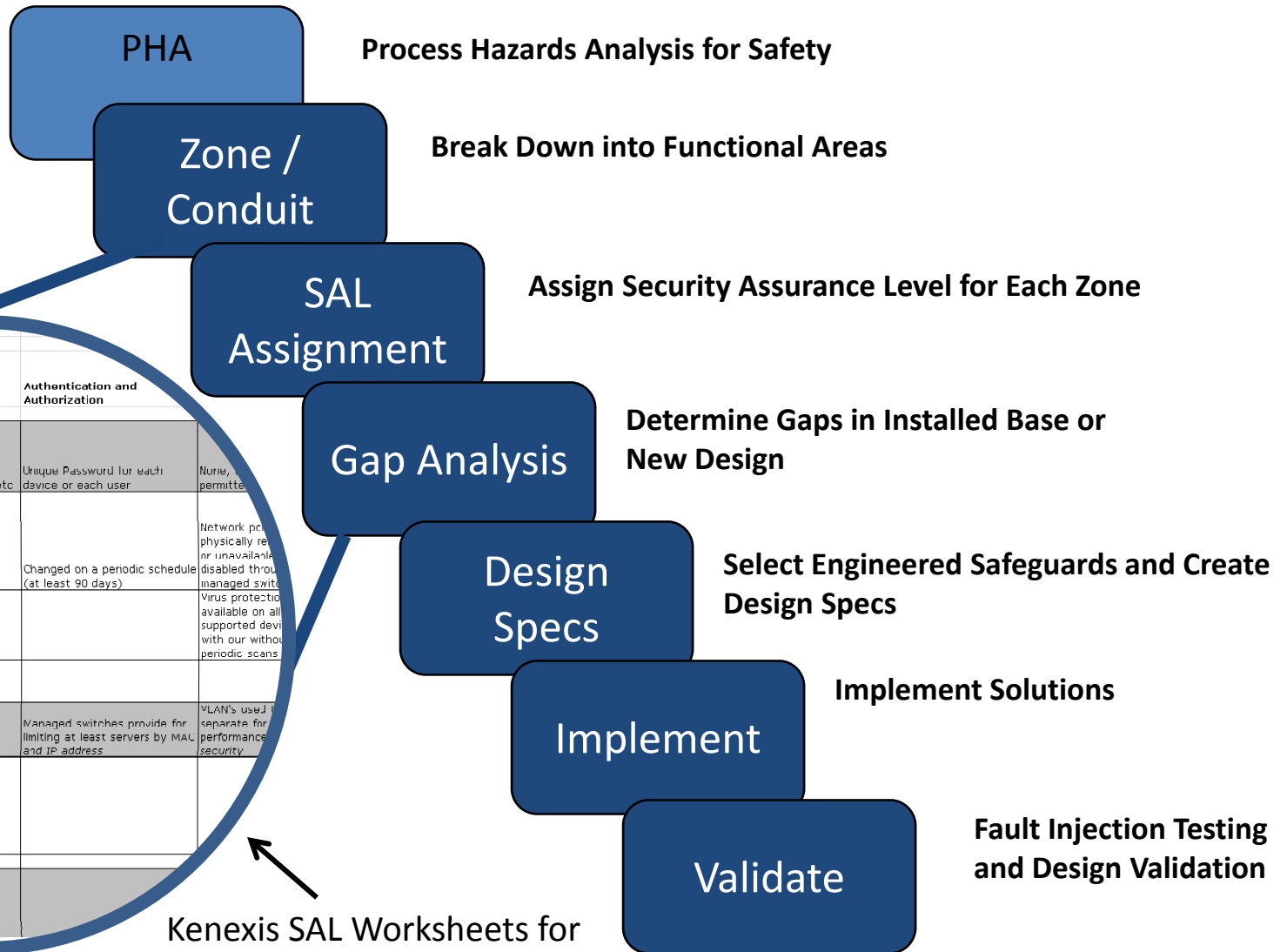
Copyright © 2008 Kenexis Security Corporation

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

Security for Process Control



Category	Basic Features	Authentication and Authorization
Device	Sensors, RTU's, Controllers, HMI's, etc	Unique Password for each device or each user
		Changed on a periodic schedule (at least 90 days)
		Network ports physically removed or unavailable disabled through managed switch
		Virus protection available on all supported devices with our without periodic scans
		Managed switches provide for limiting at least servers by MAC and IP address
Network Segments	Layer 3 - Managed	VLAN's used separate for performance security
	NO hubs Some Layer 2 unmanaged, few devices overall	

Kenexis SAL Worksheets for Consistent Analysis and Recommendations

KENEXIS

Copyright © 2008 Kenexis Security Corporation



PLAN



PREPARE



DEFEND



RESPOND

DESIGN BASIS FOR SECURITY

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

[illegible]

Financial KPIs									
Period	Revenue	Profit	EBITDA	EBIT	EBE	EBT	Net Income	EPS	Dividend
Q1 2023	1000	150	200	180	160	140	120	1.20	0.50
Q2 2023	1100	160	210	190	170	150	130	1.30	0.55
Q3 2023	1200	170	220	200	180	160	140	1.40	0.60
Q4 2023	1300	180	230	210	190	170	150	1.50	0.65
Q1 2024	1400	190	240	220	200	180	160	1.60	0.70
Q2 2024	1500	200	250	230	210	190	170	1.70	0.75
Q3 2024	1600	210	260	240	220	200	180	1.80	0.80
Q4 2024	1700	220	270	250	230	210	190	1.90	0.85
Q1 2025	1800	230	280	260	240	220	200	2.00	0.90
Q2 2025	1900	240	290	270	250	230	210	2.10	0.95
Q3 2025	2000	250	300	280	260	240	220	2.20	1.00
Q4 2025	2100	260	310	290	270	250	230	2.30	1.05
Q1 2026	2200	270	320	300	280	260	240	2.40	1.10
Q2 2026	2300	280	330	310	290	270	250	2.50	1.15
Q3 2026	2400	290	340	320	300	280	260	2.60	1.20
Q4 2026	2500	300	350	330	310	290	270	2.70	1.25
Q1 2027	2600	310	360	340	320	300	280	2.80	1.30
Q2 2027	2700	320	370	350	330	310	290	2.90	1.35
Q3 2027	2800	330	380	360	340	320	300	3.00	1.40
Q4 2027	2900	340	390	370	350	330	310	3.10	1.45
Q1 2028	3000	350	400	380	360	340	320	3.20	1.50
Q2 2028	3100	360	410	390	370	350	330	3.30	1.55
Q3 2028	3200	370	420	400	380	360	340	3.40	1.60
Q4 2028	3300	380	430	410	390	370	350	3.50	1.65
Q1 2029	3400	390	440	420	400	380	360	3.60	1.70
Q2 2029	3500	400	450	430	410	390	370	3.70	1.75
Q3 2029	3600	410	460	440	420	400	380	3.80	1.80
Q4 2029	3700	420	470	450	430	410	390	3.90	1.85
Q1 2030	3800	430	480	460	440	420	400	4.00	1.90
Q2 2030	3900	440	490	470	450	430	410	4.10	1.95
Q3 2030	4000	450	500	480	460	440	420	4.20	2.00
Q4 2030	4100	460	510	490	470	450	430	4.30	2.05
Q1 2031	4200	470	520	500	480	460	440	4.40	2.10
Q2 2031	4300	480	530	510	490	470	450	4.50	2.15
Q3 2031	4400	490	540	520	500	480	460	4.60	2.20
Q4 2031	4500	500	550	530	510	490	470	4.70	2.25
Q1 2032	4600	510	560	540	520	500	480	4.80	2.30
Q2 2032	4700	520	570	550	530	510	490	4.90	2.35
Q3 2032	4800	530	580	560	540	520	500	5.00	2.40
Q4 2032	4900	540	590	570	550	530	510	5.10	2.45
Q1 2033	5000	550	600	580	560	540	520	5.20	2.50
Q2 2033	5100	560	610	590	570	550	530	5.30	2.55
Q3 2033	5200	570	620	600	580	560	540	5.40	2.60
Q4 2033	5300	580	630	610	590	570	550	5.50	2.65
Q1 2034	5400	590	640	620	600	580	560	5.60	2.70
Q2 2034	5500	600	650	630	610	590	570	5.70	2.75
Q3 2034	5600	610	660	640	620	600	580	5.80	2.80
Q4 2034	5700	620	670	650	630	610	590	5.90	2.85
Q1 2035	5800	630	680	660	640	620	600	6.00	2.90
Q2 2035	5900	640	690	670	650	630	610	6.10	2.95
Q3 2035	6000	650	700	680	660	640	620	6.20	3.00
Q4 2035	6100	660	710	690	670	650	630	6.30	3.05
Q1 2036	6200	670	720	700	680	660	640	6.40	3.10
Q2 2036	6300	680	730	710	690	670	650	6.50	3.15
Q3 2036	6400	690	740	720	700	680	660	6.60	3.20
Q4 2036	6500	700	750	730	710	690	670	6.70	3.25
Q1 2037	6600	710	760	740	720	700	680	6.80	3.30
Q2 2037	6700	720	770	750	730	710	690	6.90	3.35
Q3 2037	6800	730	780	760	740	720	700	7.00	3.40
Q4 2037	6900	740	790	770	750	730	710	7.10	3.45
Q1 2038	7000	750	800	780	760	740	720	7.20	3.50
Q2 2038	7100	760	810	790	770	750	730	7.30	3.55
Q3 2038	7200	770	820	800	780	760	740	7.40	3.60
Q4 2038	7300	780	830	810	790	770	750	7.50	3.65
Q1 2039	7400	790	840	820	800	780	760	7.60	3.70
Q2 2039	7500	800	850	830	810	790	770	7.70	3.75
Q3 2039	7600	810	860	840	820	800	780	7.80	3.80
Q4 2039	7700	820	870	850	830	810	790	7.90	3.85
Q1 2040	7800	830	880	860	840	820	800	8.00	3.90
Q2 2040	7900	840	890	870	850	830	810	8.10	3.95
Q3 2040	8000	850	900	880	860	840	820	8.20	4.00
Q4 2040	8100	860	910	890	870	850	830	8.30	4.05
Q1 2041	8200	870	920	900	880	860	840	8.40	4.10
Q2 2041	8300	880	930	910	890	870	850	8.50	4.15
Q3 2041	8400	890	940	920	900	880	860	8.60	4.20
Q4 2041	8500	900	950	930	910	890	870	8.70	4.25
Q1 2042	8600	910	960	940	920	900	880	8.80	4.30
Q2 2042	8700	920	970	950	930	910	890	8.90	4.35
Q3 2042	8800	930	980	960	940	920	900	9.00	4.40
Q4 2042	8900	940	990	970	950	930	910	9.10	4.45
Q1 2043	9000	950	1000	980	960	940	920	9.20	4.50
Q2 2043	9100	960	1010	990	970	950	930	9.30	4.55
Q3 2043	9200	970	1020	1000	980	960	940	9.40	4.60
Q4 2043	9300	980	1030	1010	990	970	950	9.50	4.65
Q1 2044	9400	990	1040	1020	1000	980	960	9.60	4.70
Q2 2044	9500	1000	1050	1030	1010	990	970	9.70	4.75
Q3 2044	9600	1010	1060	1040	1020	1000	980	9.80	4.80
Q4 2044	9700	1020	1070	1050	1030	1010	990	9.90	4.85
Q1 2045	9800	1030	1080	1060	1040	1020	1000	10.00	4.90
Q2 2045	9900	1040	1090	1070	1050	1030	1010	10.10	4.95
Q3 2045	10000	1050	1100	1080	1060	1040	1020	10.20	5.00
Q4 2045	10100	1060	1110	1090	1070	1050	1030	10.30	5.05
Q1 2046	10200	1070	1120	1100	1080	1060	1040	10.40	5.10
Q2 2046	10300	1080	1130	1110	1090	1070	1050	10.50	5.15
Q3 2046	10400	1090	1140	1120	1100	1080	1060	10.60	5.20
Q4 2046	10500	1100	1150	1130	1110	1090	1070	10.70	5.25
Q1 2047	10600	1110	1160	1140	1120	1100	1080	10.80	5.30
Q2 2047	10700	1120	1170	1150	1130	1110	1090	10.90	5.35
Q3 2047	10800	1130	1180	1160	1140	1120	1100	11.00	5.40
Q4 2047	10900	1140	1190	1170	1150	1130	1110	11.10	5.45
Q1 2048	11000	1150	1200	1180	1160	1140	1120	11.20	5.50
Q2 2048	11100	1160	1210	1190	1170	1150	1130	11.30	5.55
Q3 2048	11200	1170	1220	1200	1180	1160	1140	11.40	5.60
Q4 2048	11300	1180	1230	1210	1190	1170	1150	11.50	5.65
Q1 2049	11400	1190	1240	1220	1200	1180	1160	11.60	5.70
Q2 2049	11500	1200	1250	1230	1210	1190	1170	11.70	5.75
Q3 2049	11600	1210	1260	1240	1220	1200	1180	11.80	5.80
Q4 2049	11700	1220	1270	1250	1230	1210	1190	11.90	5.85
Q1 2050	11800	1230	1280	1260	1240	1220	1200	12.00	5.90
Q2 2050	11900	1240	1290	1270	1250	1230	1210	12.10	5.95
Q3 2050	12000	1250	1300	1280	1260	1240	1220	12.20	6.00
Q4 2050	12100	1260	1310	1290	1270	1250	1230	12.30	6.05
Q1 2051	12200	1270	1320	1300	1280	1260	1240	12.40	6.10
Q2 2051	12300	1280	1330	1310	1290	1270	1250	12.50	6.15
Q3 2051	12400	1290	1340	1320	1300	1280	1260	12.60	6.20
Q4 2051	12500	1300	1350	1330	1310	1290	1270	12.70	6.25
Q1 2052	12600	1310	1360	1340	1320	1300	1280	12.80	6.30
Q2 2052	12700	1320	1370	1350	1330	1310	1290	12.90	6.35
Q3 2052	12800	1330	1380	1360	1340	1320	1300	13.00	6.40
Q4 2052	12900	1340	1390	1370	1350	1330	1310	13.10	6.45
Q1 2053	13000	1350	1400	1380	1360	1340	1320	13.20	6.50
Q2 2053	13100	1360	1410	1390	1370	1350	1330	13.30	6.55
Q3 2053	13200	1370	1420	1400	1380	1360	1340	13.40	6.60
Q4 2053	13300	1380	1430	1410	1390	1370	1350	13.50	6.65
Q1 2054	13400	1390	1440	1420	1400	1380	1360	13.60	6.70
Q2 2054	13500	1400	1450	1430	1410	1390	1370	13.70	6.75
Q3 2054	13600	1410	1460	1440	1420	1400	1380	13.80	6.80
Q4 2054	13700	1420	1470	1450	1430	1410	1390	13.90	6.85
Q1 2055	13800	1430	1480	1460	1440	1420	1400	14.00	6.90
Q2 2055	13900	1440	1490	1470	1450	1430	1410	14.10	6.95
Q3 2055	14000	1450	1500	1480	1460	1440	1420	14.20	7.00
Q4 2									

SAL Verification

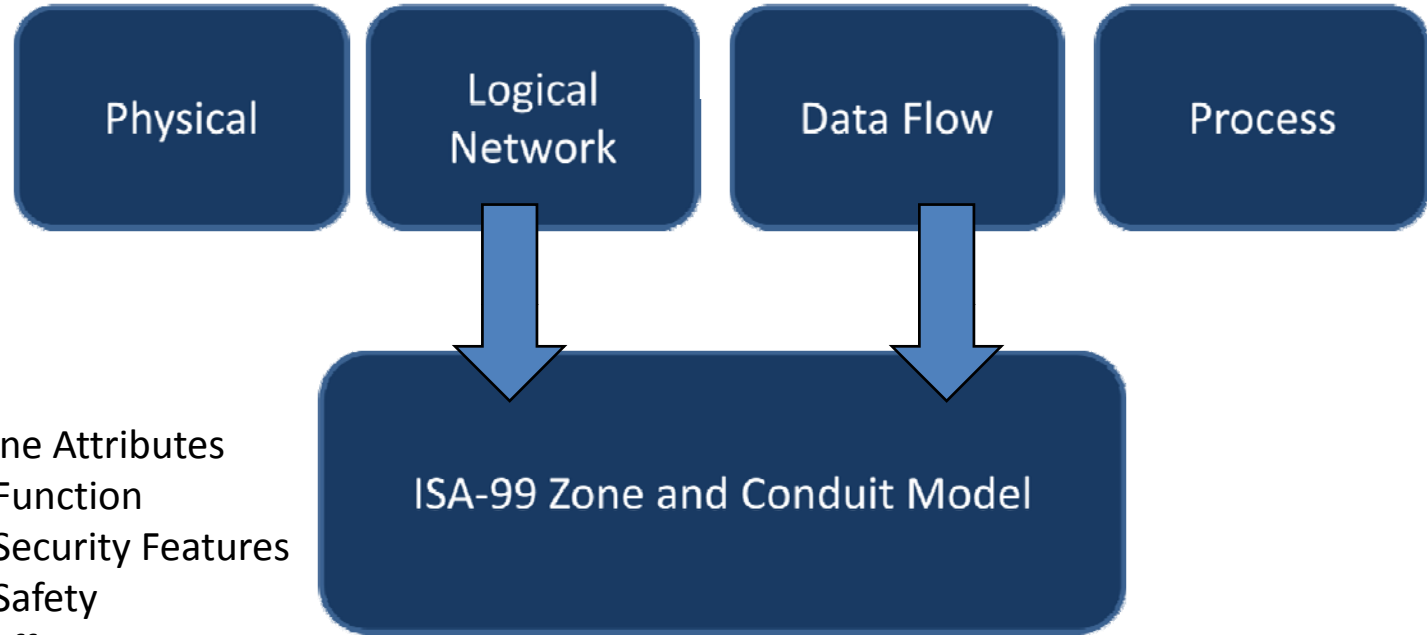
Parent/Zone	Safety/Consequence	Consequence					Target SA _h
		Production Efficiency	Quality	Material Loss	Regulatory Compliance	Public Confidence	
1. A. City	1	1	1	1	1	1	0.0001
2. B. District	2	2	2	2	2	2	0.0002
3. C. Region	3	3	3	3	3	3	0.0003
4. D. Country	4	4	4	4	4	4	0.0004
5. E. Continent	5	5	5	5	5	5	0.0005
6. F. Planet	6	6	6	6	6	6	0.0006
7. G. Galaxy	7	7	7	7	7	7	0.0007
8. H. Universe	8	8	8	8	8	8	0.0008
9. I. Multiverse	9	9	9	9	9	9	0.0009
10. J. Omniverse	10	10	10	10	10	10	0.0010

SAL Selection

KENEXIS

Copyright © 2008 Kenexis Security Corporation

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

Copyright © 2008 Kenexis Security Corporation

Step 2 - SAL Selection

Parent Zone	Consequence					Public Confidence	Target SAL
	Safety Consequence	Production Efficiency	Quality	Material Loss	Regulatory Compliance		
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

Copyright © 2008 Kenexis Security Corporation

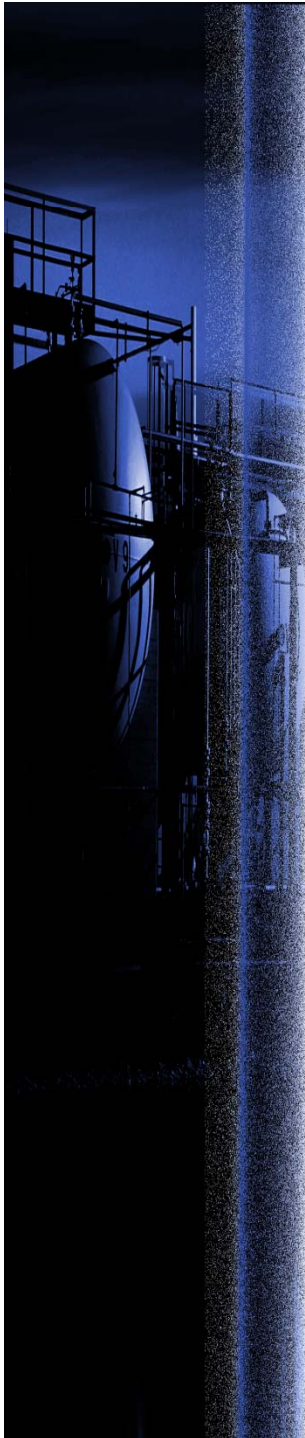
Step 3 - SAL Verification

Parent Zone	Target SAL	BC P	Aut hori zati on	Net wor k	Net Seg me nt	Assessed SAL			Assessed SAL	SAL Gap	Discrepancies	Recommendations
						Saf ety/ 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
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
											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

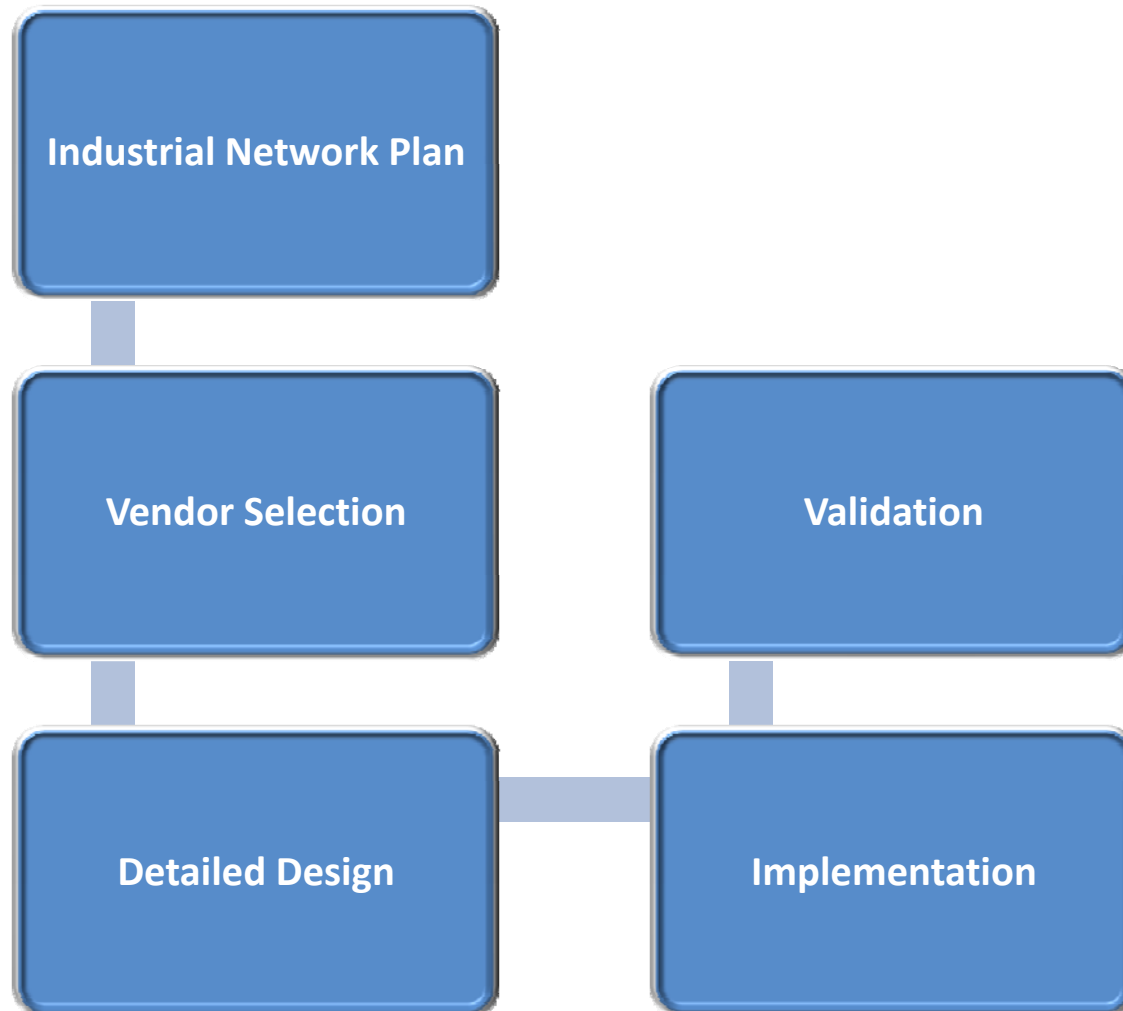
Copyright © 2008 Kenexis Security Corporation



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

Design Basis: Next Steps



KENEXIS



PLAN



PREPARE



DEFEND

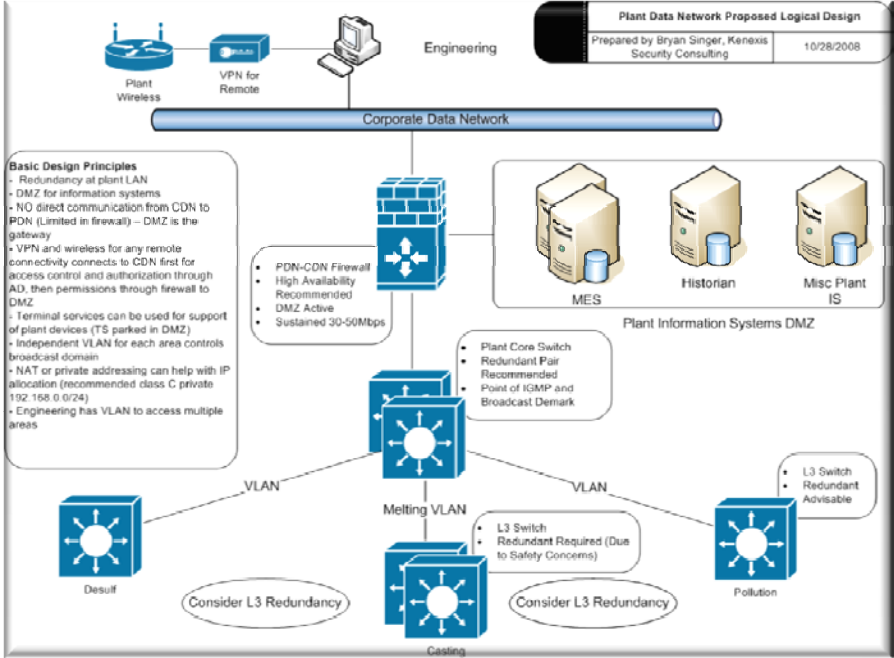


RESPOND

INDUSTRIAL NETWORK DESIGN BASIS

Copyright © 2008 Kenexis Security Corporation

GOAL: Implement an Efficient and Reliable Network Architecture

[illegible]

Industrial Network Assessment and Growth Plan

KENEXIS

Copyright © 2008 Kenexis Security Corporation

Step 1 Consequence Modeling

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

	Sensors/Meters	Valves/Actuators	Driver/Motors	Controllers	HMI	DCS/SCADA	Historians/OM Intelligence	MES	ERP	Corporate Network	Plant Network
Sensors/Meters	X	SECQF	SECQF	ECRQF	ERQF	RQF	RQF	RQF			SECIRQF
Valves/Actuators	SECQF		SECQF	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											

- 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

Copyright © 2008 Kenexis Security Corporation

Step 2 Industrial Network Plan

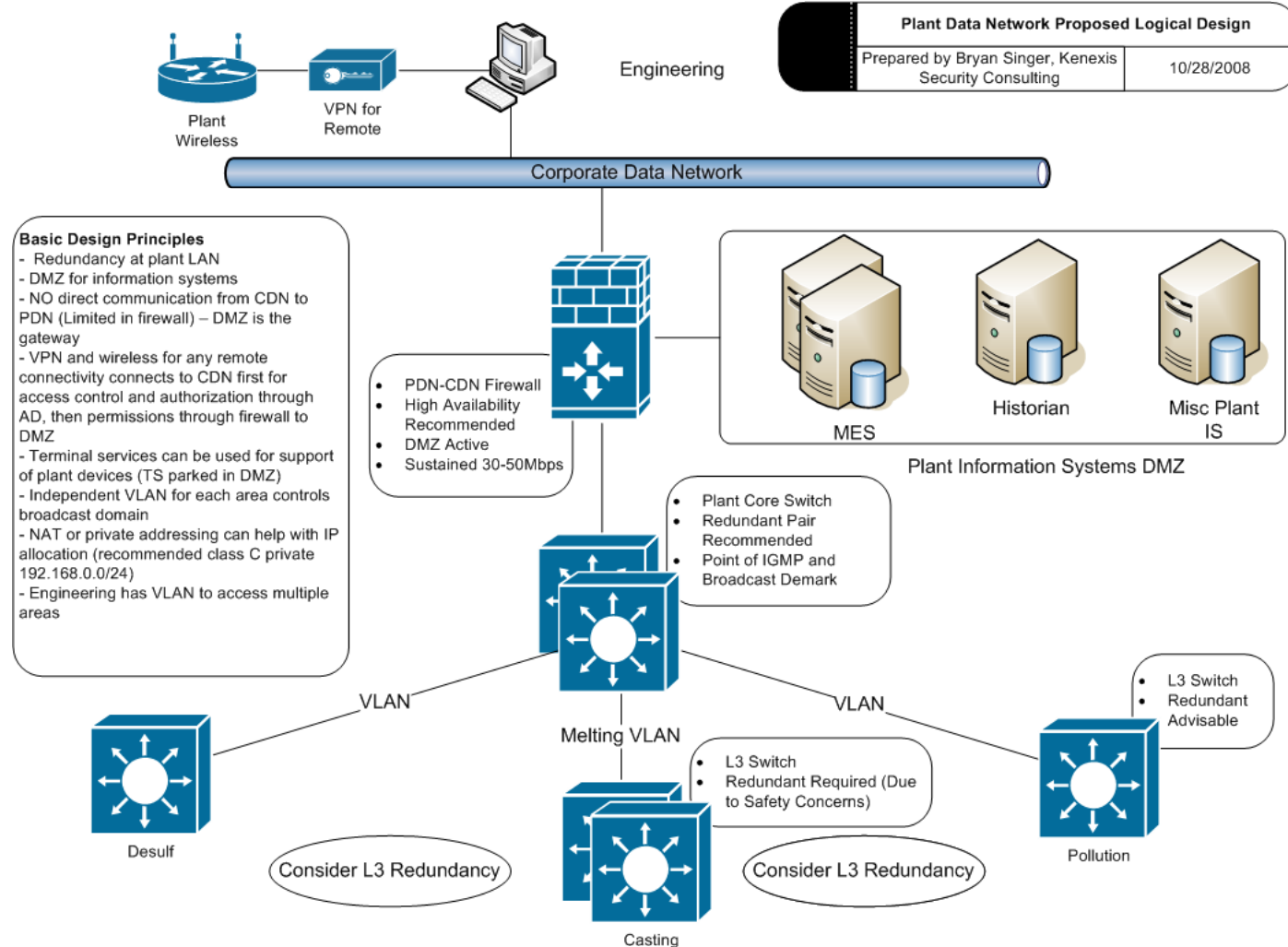
Parent Zone	Network Calculations																
	Servers	Workstation Counts	Processors	I/O Count	IP Cameras	Switches	Power Meters	Peak Capacity	Servers	Workstations	Processors	I/O Count	IP Cameras	Switches	Power Meters	Network Increase	Target Network Load
1. Melting	2	26	8	1606	10	1	13	9Mb/s	0	3	0	0	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

Copyright © 2008 Kenexis Security Corporation

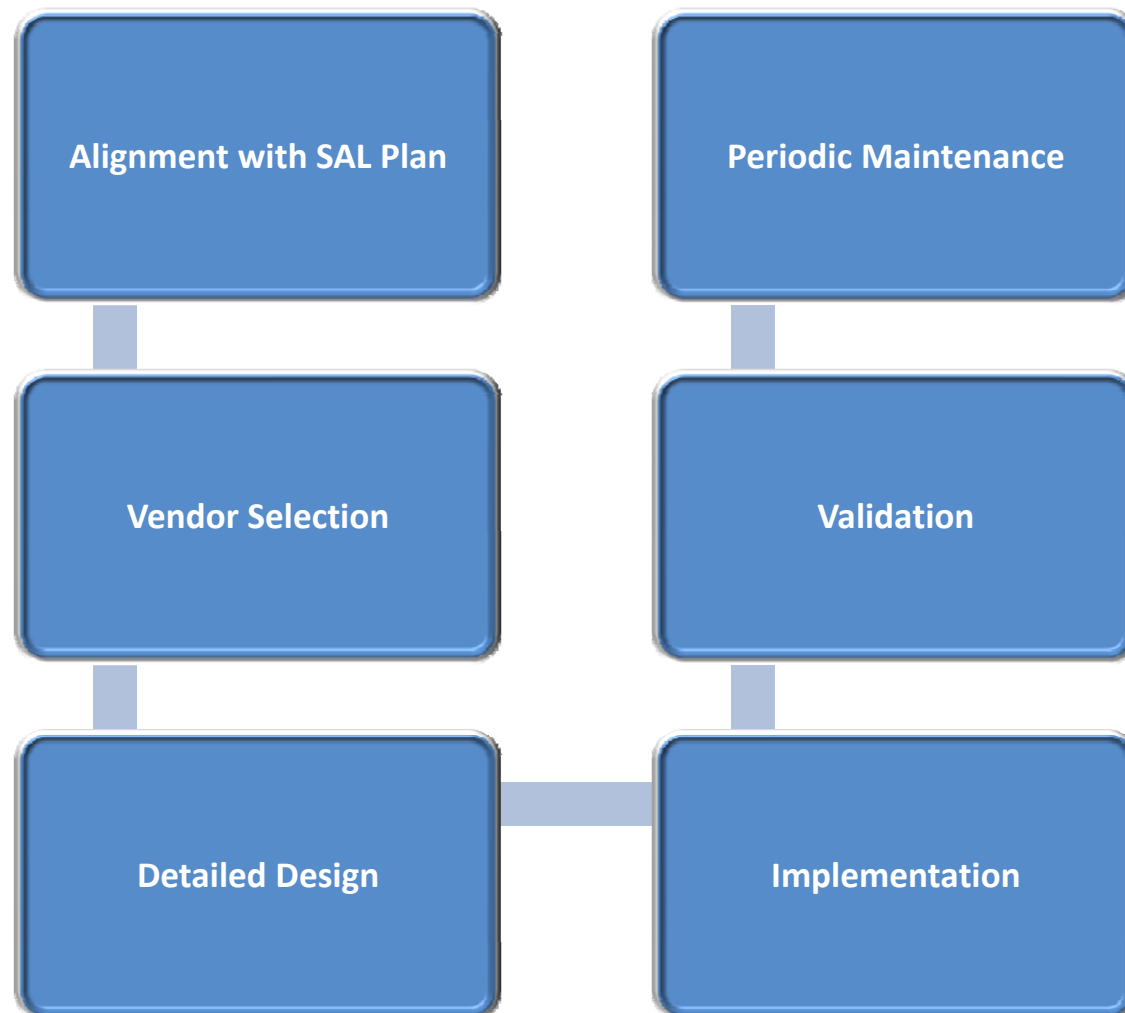
Step 3 – Logical Design



KENEXIS

Copyright © 2008 Kenexis Security Corporation

Industrial Network Design Basis: Next Steps



KENEXIS

Copyright © 2008 Kenexis Security Corporation



PLAN



PREPARE



DEFEND



RESPOND

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

Copyright © 2008 Kenexis Security Corporation



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



KENEXIS

Copyright © 2008 Kenexis Security Corporation

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

KENEXIS

Copyright © 2008 Kenexis Security Corporation

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

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

Copyright © 2008 Kenexis Security Corporation



PLAN



PREPARE



DEFEND



RESPOND

QUESTIONS?

