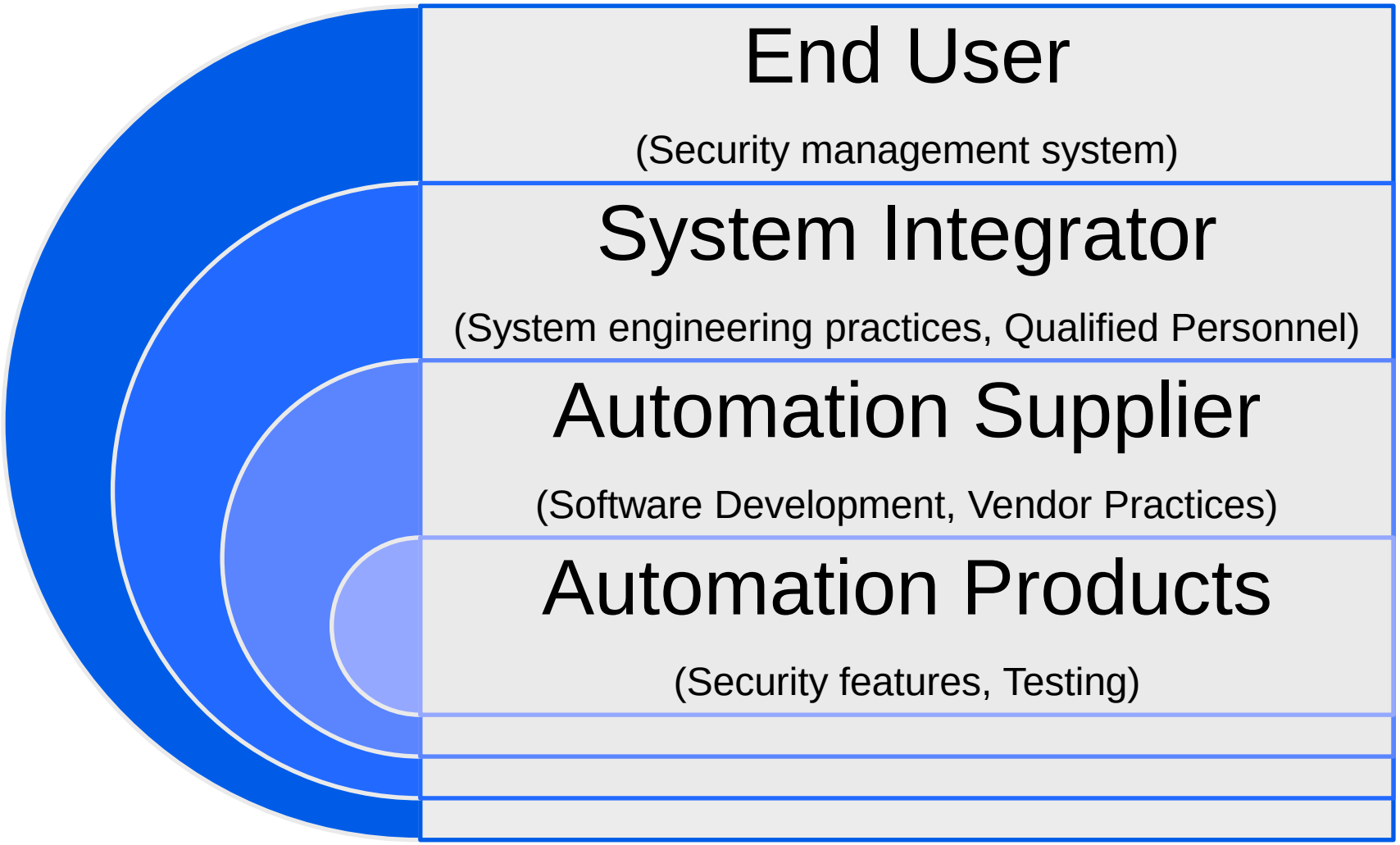
EVALUATING THE SAFETY AND SECURITY OF AUTOMATION PRODUCTS, SUPPLIERS AND SYSTEMS

John Cusimano
exida

Copyright © 2010 - exida

Control System Security
Layers of Responsibility



Copyright © 2010 - exida

ISA99 Work Products

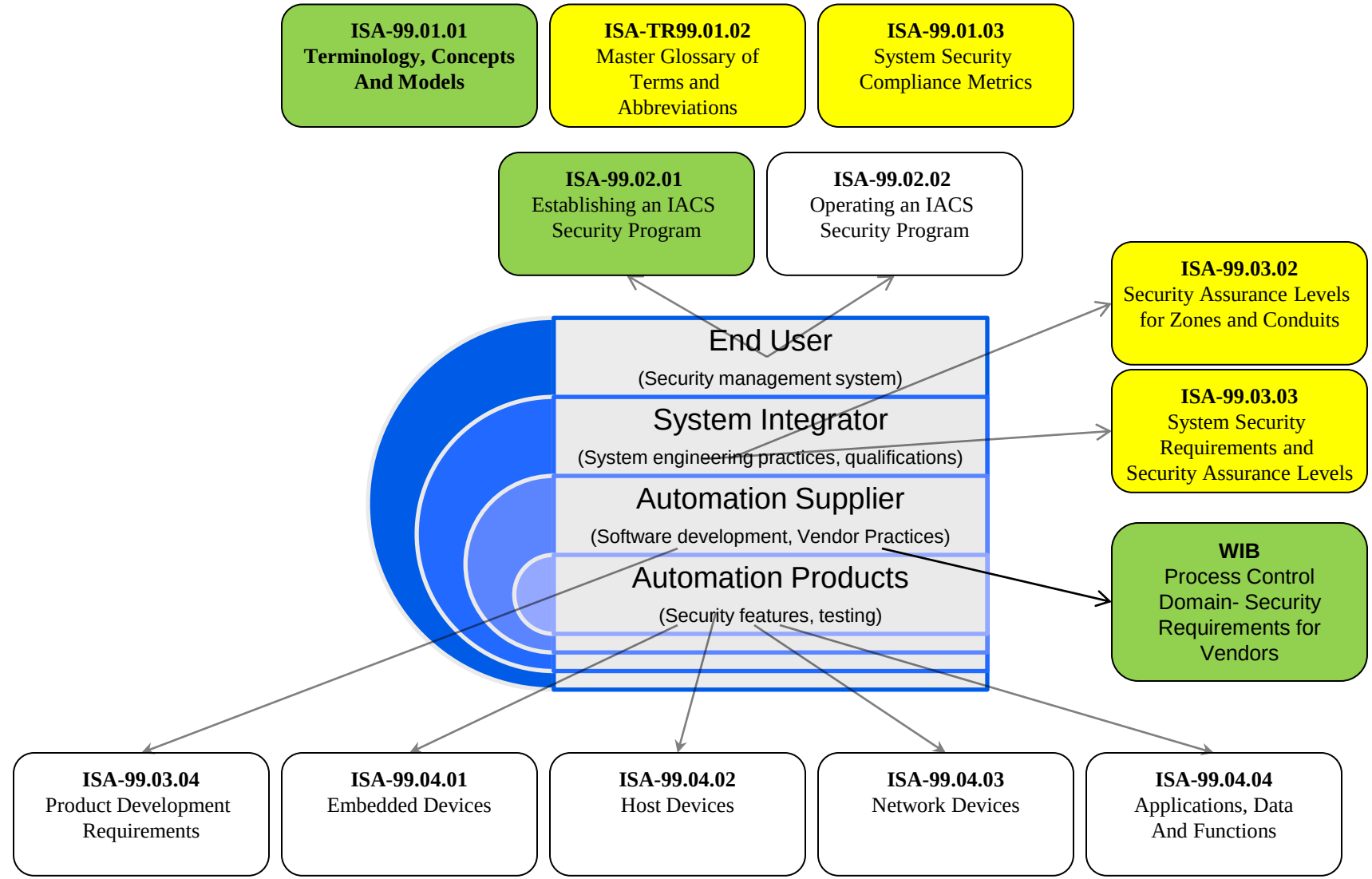
ISA99 Common	**ISA-99.01.01 Terminology, Concepts And Models**	**ISA-TR99.01.02** Master Glossary of Terms and Abbreviations	**ISA-99.01.03** System Security Compliance Metrics	
Security Program	**ISA-99.02.01** Establishing an IACS Security Program	**ISA-99.02.02** Operating an IACS Security Program	**ISA-TR99.02.03** Patch Management in the IACS Environment	
Technical - System	**ISA-TR99.03.01** Security Technologies for Industrial Automation and Control Systems	**ISA-99.03.02** Security Assurance Levels for Zones and Conduits	**ISA-99.03.03** System Security Requirements and Security Assurance Levels	**ISA-99.03.04** Product Development Requirements
Technical - Component	**ISA-99.04.01** Embedded Devices	**ISA-99.04.02** Host Devices	**ISA-99.04.03** Network Devices	**ISA-99.04.04** Applications, Data And Functions

Courtesy of ISA 99 Committee

Complete | In Progress | Planned

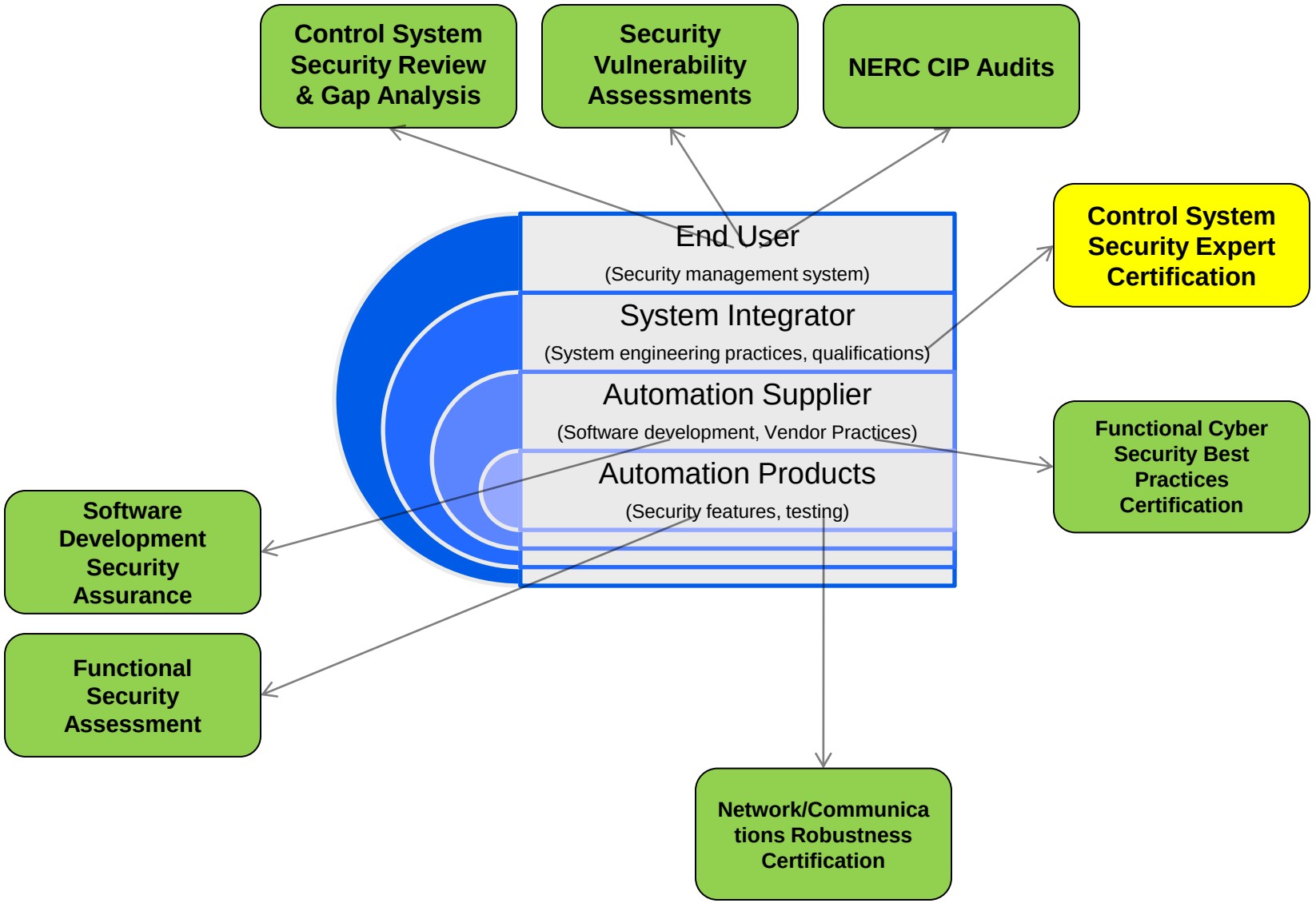
Copyright © 2010 - exida

Control System Security Layers of Responsibility



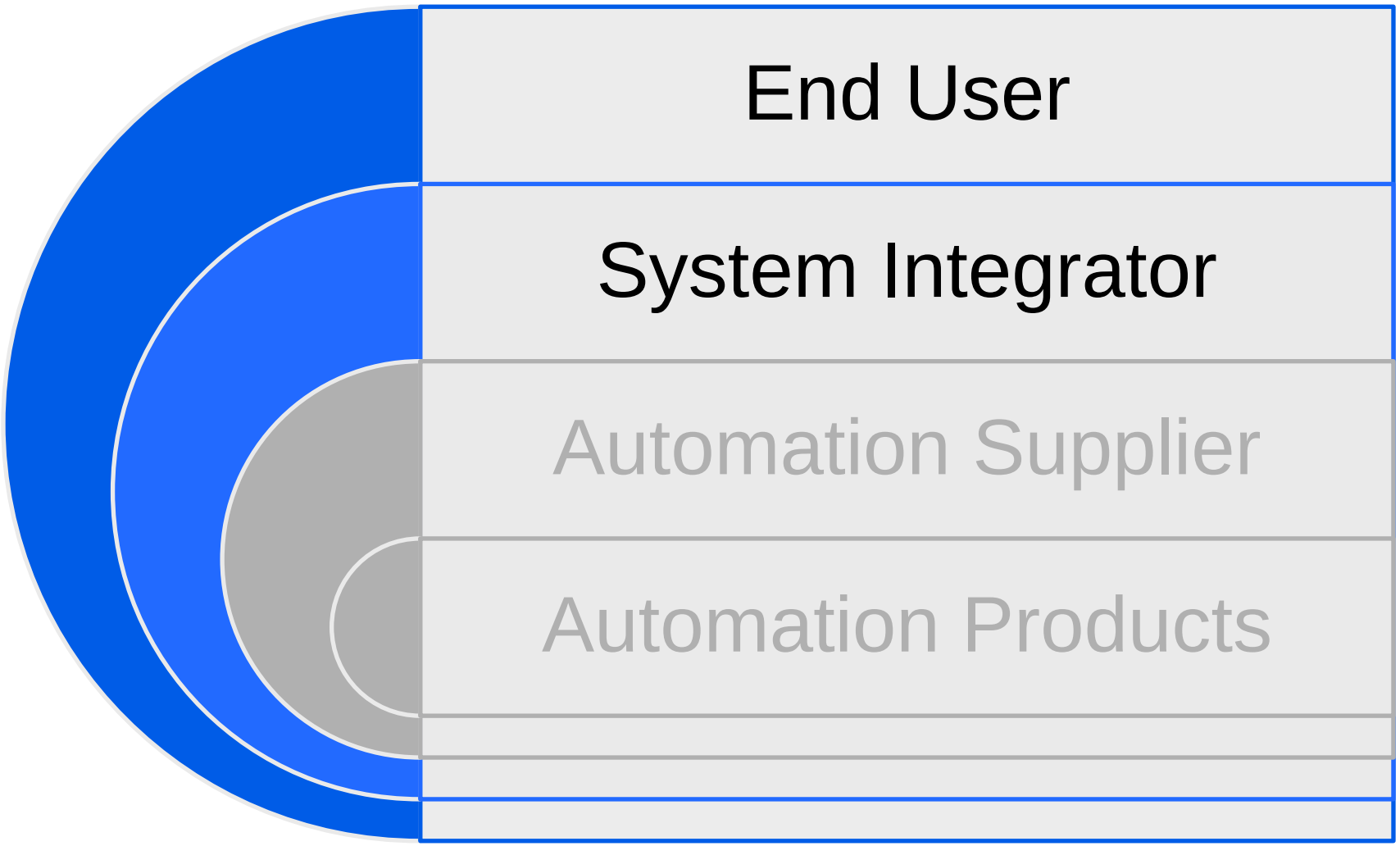
Copyright © 2010 - exida

Measuring Compliance



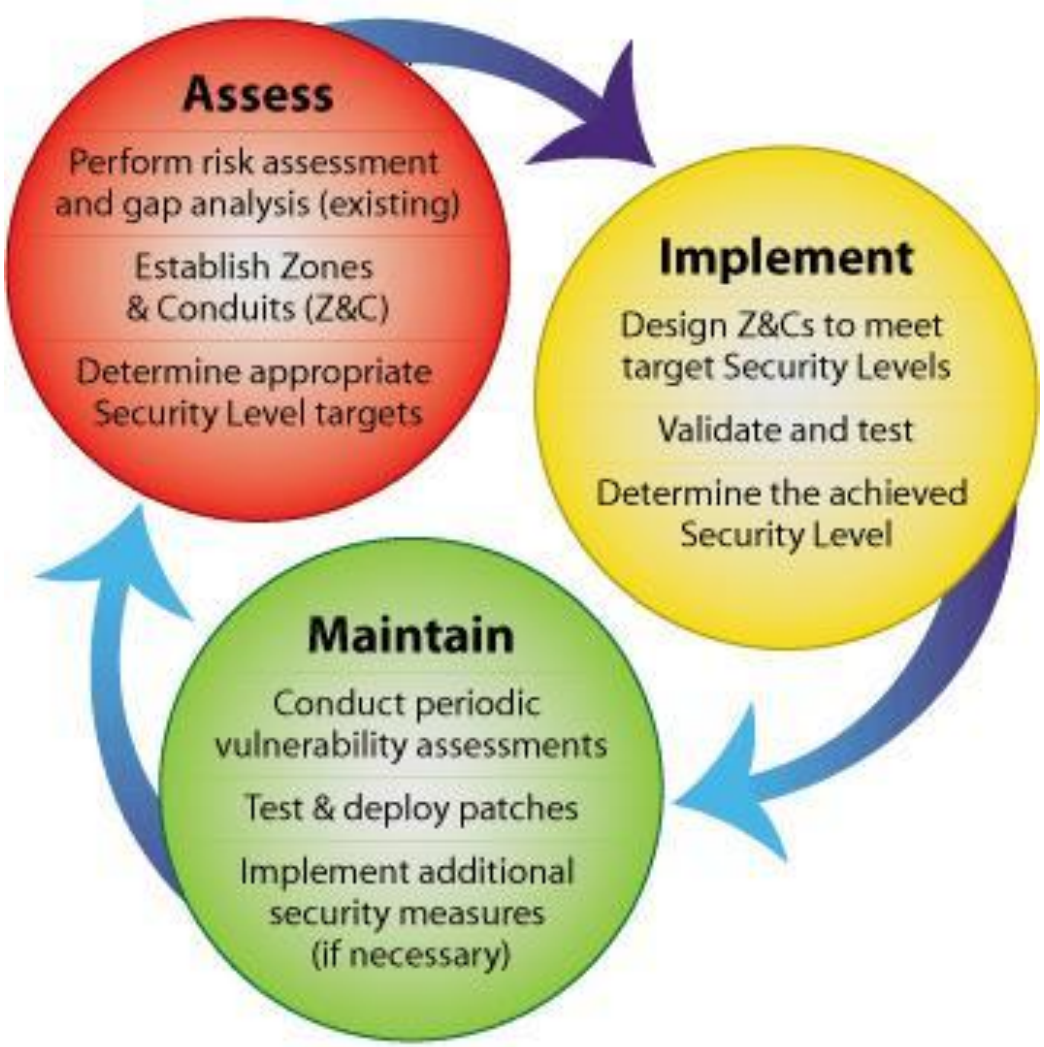
Copyright © 2010 - exida

Layers of Responsibility



Copyright © 2010 - exida

The Security Lifecycle



Copyright © 2010 - exida

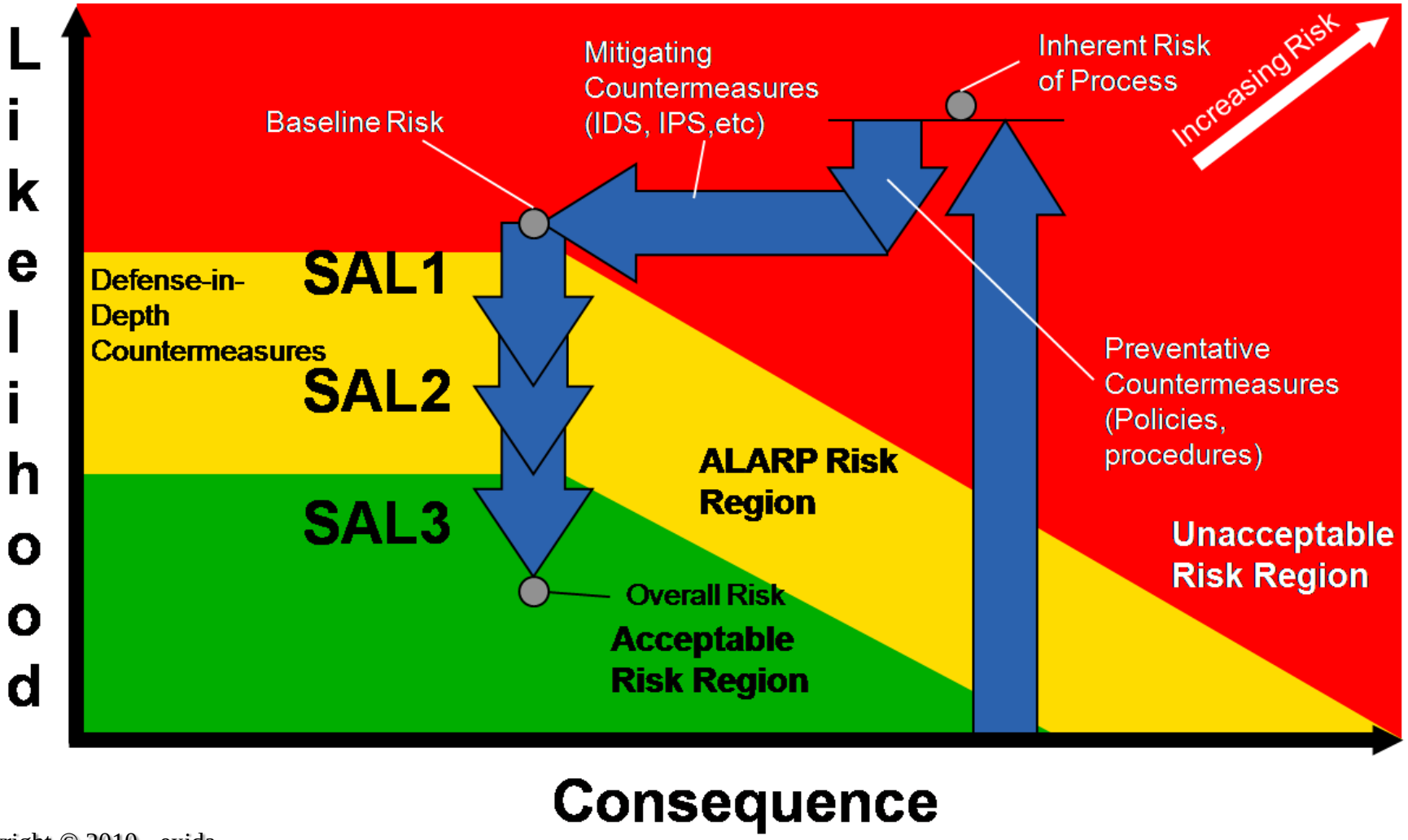
Adapted from ISA S99.01.01

The Assess Phase

- Understanding where you are and where you want to be
- Start with a high-level risk assessment
- Identify major gaps between existing system and relevant regulations, standards and best practices
- Partition the system into areas with common security requirements (e.g. zones, electronic security perimeters)
- Establish security goals or targets for each zone

Copyright © 2010 - exida

Security
Inherent Risk and Risk Reduction



Copyright © 2010 - exida

Quantitative assessment of probability and criticality

Probability	Criticality
A = Very Likely	1 = Severe Impact
B = Likely	2 = Major impact
C = Not Likely	3 = Minor impact
D = Remote Chance	4 = No impact

Network Segment	Threat Probability
Internet, Wireless, Direct Dial-in	A = Very Likely
Internet, Secure Dial-in	B = Likely
Integrated MCN	C = Not Likely
Isolated MCN	D = Remote Chance

Impact Category	1 = Severe	2 = Major	3 = Minor	4 = None
Injury	Loss of life or limb	Requires Hospitaliza -tion	Cuts, bruises requiring first aid	None
Financial loss	Millions	$100,000	$1,000	None
Environmental release	Permanent damage/ off-site damage	Lasting damage	Temporary damage	None
Interruption of Production	Week	Days	Minutes	None
Public Image	Permanent damage	Lasting blemish	Temporary tarnish	None

Source: ANSI/ISA TR99.00.02-2004

Copyright © 2010 - exida

Sample Risk Matrix

Probability	Data Assets	Criticality			
		1 Severe	2 Major	3 Minor	4 None
	A – Very Likely	Mitigation required	Mitigation required	Mitigation required (to Intranet perimeter)	Mitigation required (to Intranet perimeter)
	B – Likely	Mitigation required	Mitigation required		
	C – Not Likely	Mitigation required			
	D – Remote Chance				

Source: ANSI/ISA TR99.00.02-2004

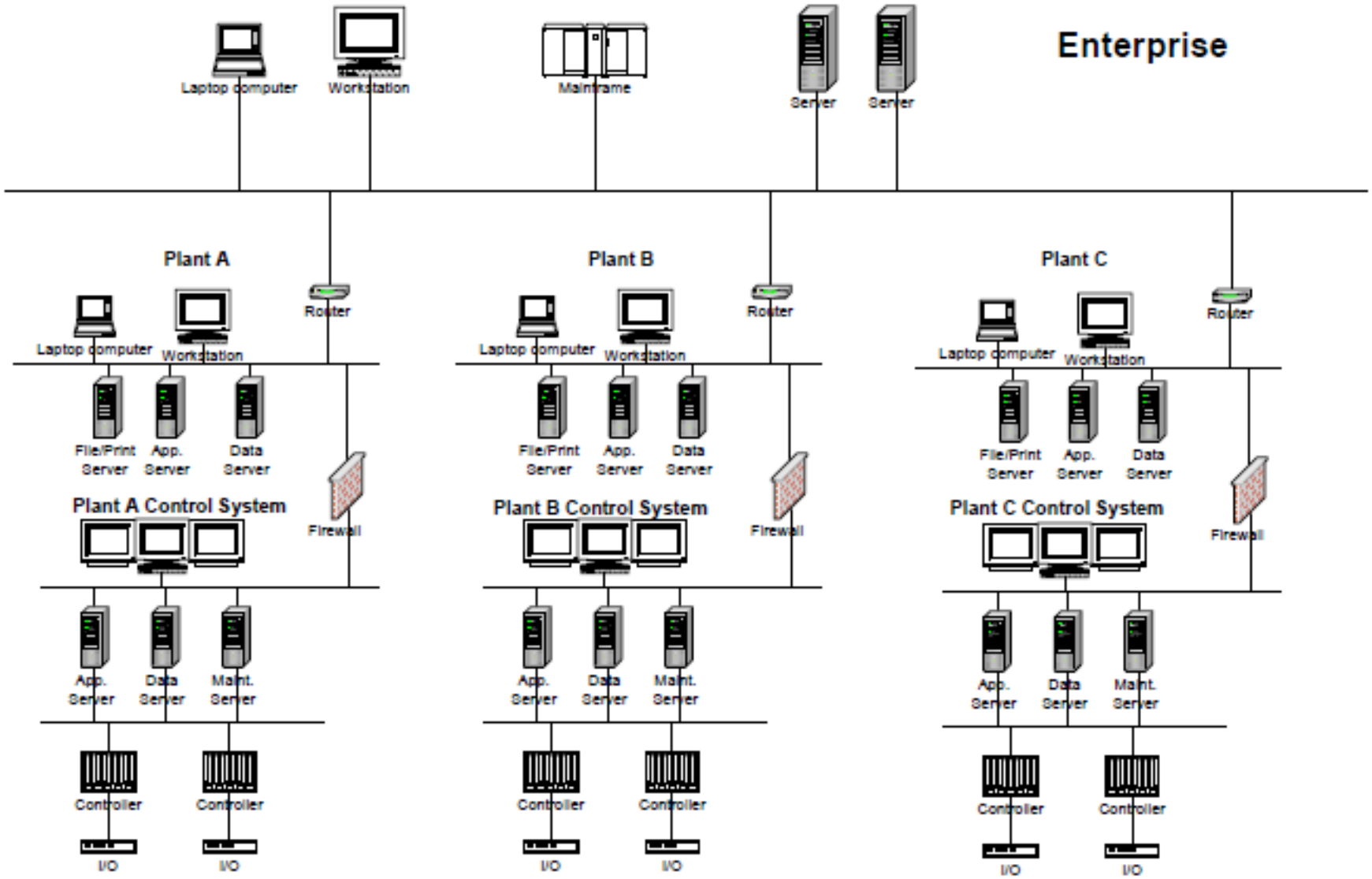
Copyright © 2010 - exida

Security Vulnerability Assessment Example

Threat	Vulnerability	Possible Threat Source	Skill Level	Potential Consequence	Severity	Likelihood	Risk
Release of hazardous product	Manipulate control system	Organized Crime, Activist	Intermediate	Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Terrorist, Organized Crime, Activist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process reactivity incident	Manipulate control system	Domestic or Foreign Terrorist, Disgruntled Employee	Intermediate	Lost Workday or Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Domestic or Foreign Terrorist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process shutdown	Trip emergency shutdown	Malware, Novice Hacker	Low	Shutdown > 6 Hours	Medium	High	High-Risk
	Cause Loss of View of SIS	Malware, Novice Hacker	Low	Shutdown < 6 Hours	Medium	Medium	Medium-Risk
	Manipulate control system	Hacker, Disgruntled Employee	Intermediate	Shutdown > 6 Hours	Medium	Medium	Medium-Risk
	Disable PCN communications	Malware, Novice Hacker	Low	Shutdown < 6 Hours	Low	High	Medium-Risk
	Spoof operators	Hacker, Disgruntled Employee	Intermediate	Shutdown < 6 Hours	Low	Medium	Low-Risk
Environmental spill	Manipulate control system	Activist	Intermediate	Citation by Local Agency	Medium	Low	Low-Risk
	Mislead operators	Activist	Intermediate	Citation by Local Agency	Medium	Low	Low-Risk

Copyright © 2010 - exida

System Architecture



Copyright © 2010 - exida

Partitioning into Zones

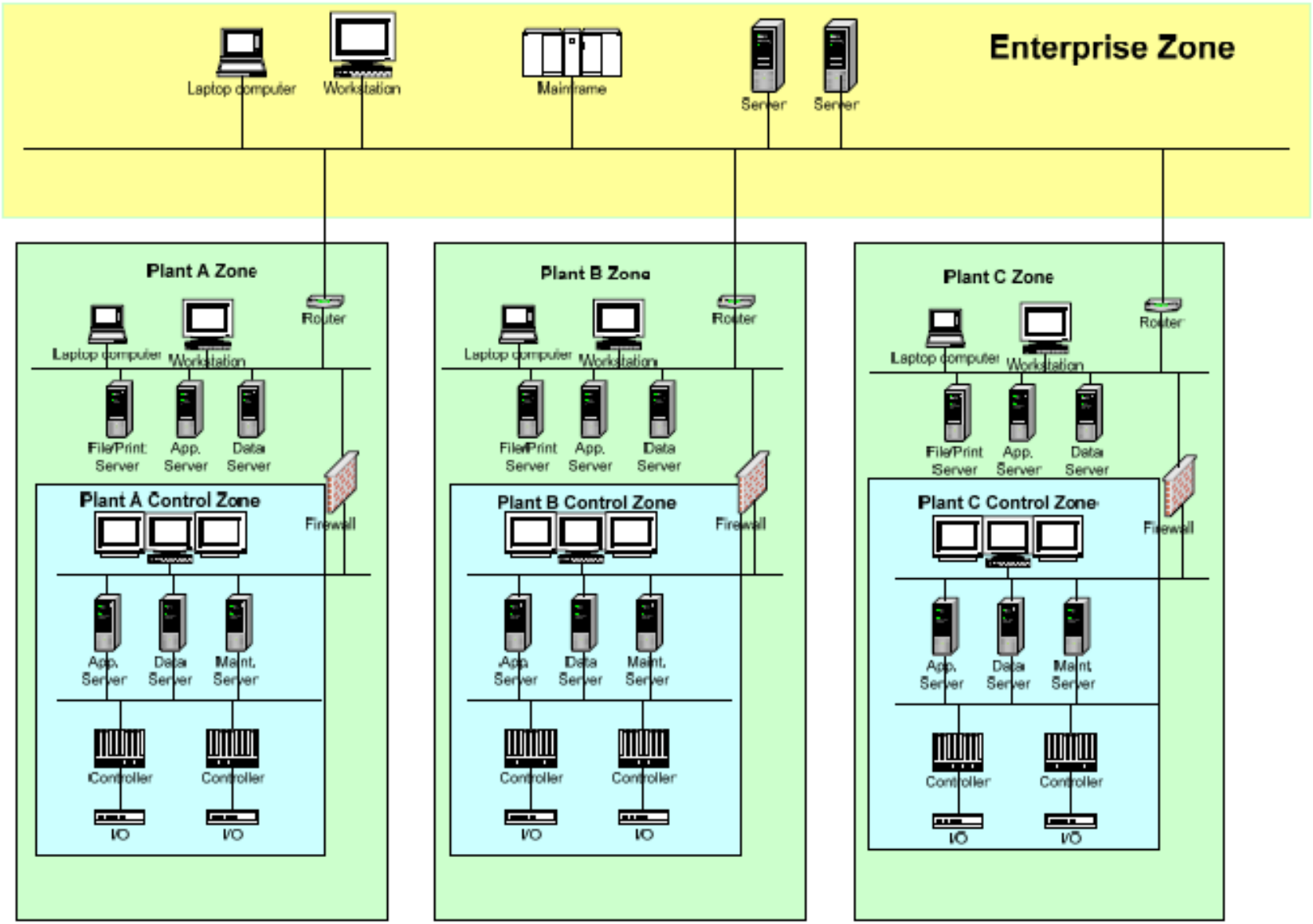


Figure 17 – Multiplant Zone Example

Copyright © 2010 - exida

Zone Definition

- Zone Name
- Description
- Function
- Zone Boundaries
  - Physical
  - Logical
- Asset Inventory
  - Physical
  - Informational
  - Applications
- Conduits
- Risk Assessment

- Security Objectives
  - Availability
  - Integrity
  - Confidentiality
- Security Strategy
  - Physical Boundary Protection
  - Cyber Boundary Protection
- Zone Security Policies
  - Personnel
  - Physical Access
  - Information Network Policies

Copyright © 2010 - exida

The Implement Phase

- Design to close gaps and minimize vulnerabilities
- Redesign network architecture if necessary
- Implement countermeasures
- Validate using Defense-in-Depth Analysis™ or other technique

Copyright © 2010 - exida

Typical Countermeasures

- Network Architecture
- Personnel Security
- Physical Security
- Policies & Procedures
- Access Control

Copyright © 2010 - exida

Multi-Layer Architectures

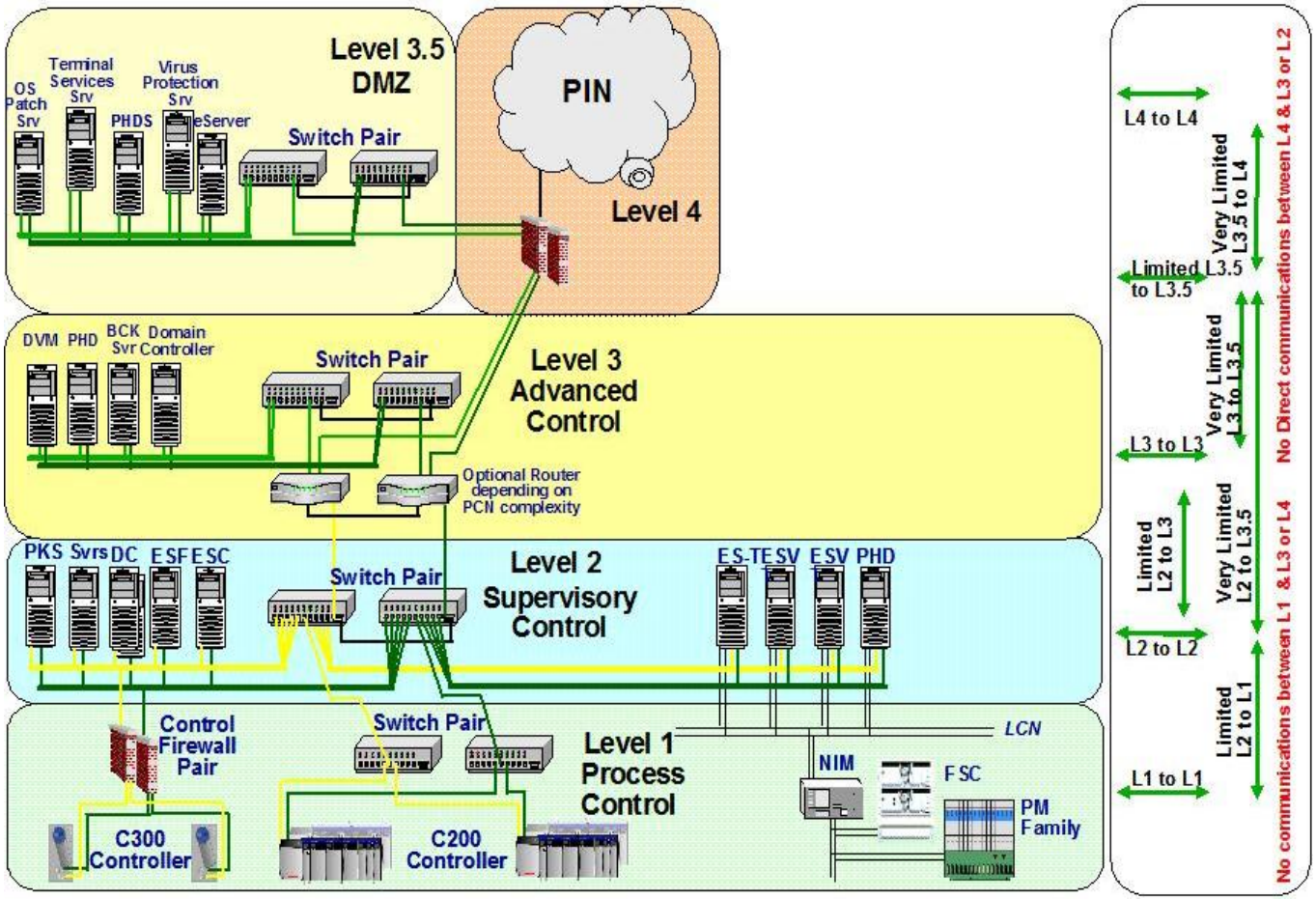


Image Courtesy of Honeywell Process Control

Copyright © 2010 - exida

Defense-in-Depth Analysis

- Semi-quantitative risk assessment method
- Supports decision making
- Parallels Layer of Protection Analysis (LOPA) used in safety
- Assists in identifying and determining the adequacy of existing defense-in-depth

Copyright © 2010 - exida

Using Defense-in-Depth Analysis™ to Quantify Likelihood of Threat Realization

Initiating Event	Defense Layer 1	Defense Layer 2	Defense Layer 3		OUTCOME	
Threat						
Realization					5.00E-05	Unwanted
Frequency			0.05			Event
		0.1				
	0.1					
0.1						No
	0.9	0.9	0.95		7.70E-02	Event

$$F = 0.1\ /yr * 0.1 * 0.1*.05 = 5 \times 10^{-4}/yr$$

Copyright © 2010 - exida

Using Defense-in-Depth Analysis™ to Quantify Likelihood of Threat Realization

INITIATING EVENT	Layer 1	Layer 2	OUTCOME
Virus enters Corporate Network	Firewall fails to prevent spread of virus	Anti-virus Fails	System Infected with Virus
0.1 /yr	0.1	0.25	2.50E-03
			No Event

$$F = 0.1\ /yr * 0.1 * 0.25 = 2.5 \times 10^{-3}/yr$$

Copyright © 2010 - exida

Defense-in-Depth Analysis™ is a trademark of exida Consulting LLC

The Maintain Phase

- Establish and document a patch management procedure
- Establish and document an anti-virus management procedure
- Establish and document a backup and restore procedure
- Establish and document an Incident response plan
- Manage and test changes
- Conduct Periodic audits

Adapted from ISA S99.01.01

Patch Management

- 95% of all network intrusions could have been avoided by keeping systems up to date with appropriate patches.
- Cannot automatically deploy new patches into the controls environment without risking disruption of operations.
- Careful policy is required to balance the need for reliability with the need for security.
- “Patch Management for Control Systems” NERC Security Guidelines for the Electric Sector, May, 2005 provides guidance

Copyright © 2010 - exida

Patch Management (cont'd)

- First all machines are prioritized and categorized into groups that define when and how they are to be patched. Example:
  - "Early Adopters" receive patches as soon as available and act as Test/Quality Assurance machines.
  - "No Touch" machines require manual intervention and/or detailed vendor consultation.
- Next procedure established for keeping track of new patches and level of importance to control operations.

Copyright © 2010 - exida

Anti-Virus Management

- Malware related incidents are the number one cause of cyber-related production losses and upsets in process control systems.
- Viruses are having a major impact on control systems and are likely to do so for the foreseeable future.
- Commonly believed that anti-virus software is incompatible with process control systems and thus should not be used on the plant floor.
- This is NOT TRUE!!! - All major DCS and PLC vendors now support anti-virus software on their Windows-based platforms.

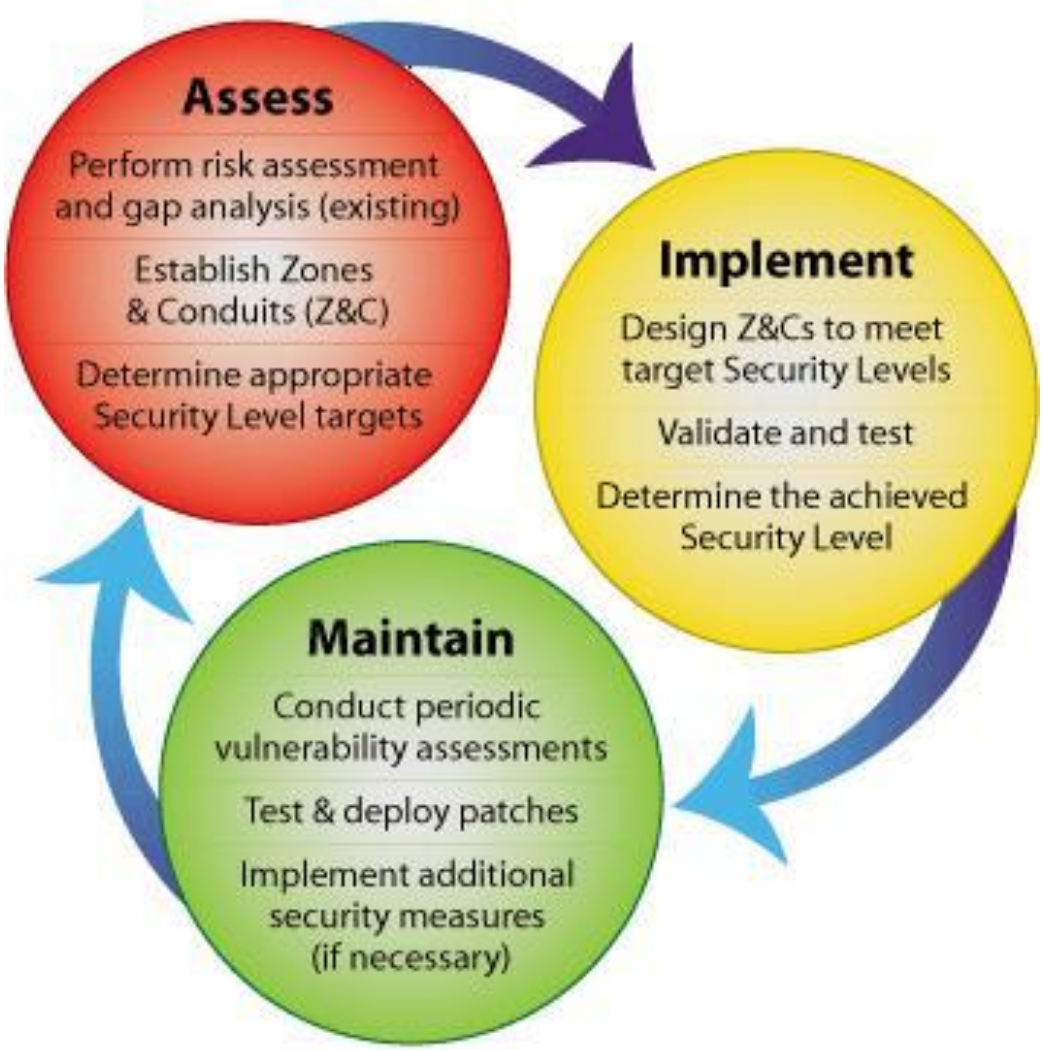
Copyright © 2010 - exida

Anti-Virus Management (cont'd)

- Use a mixed deployment systems:
  - Anti-virus scanning at the control system firewall.
  - Automatic updating for non-critical systems or systems with vendor approved update schemes.
  - Manual scheduled updates for more difficult systems.
- Focus on anti-virus signatures in all computers located in the DMZ.
- A dedicated anti-virus server can located in the DMZ.

Copyright © 2010 - exida

The Security Lifecycle



Adapted from ISA S99.01.01

For more information…

- Exida Security (www.exida.com/security)
- DHS Control System Security (www.us-cert.gov)
- ISA Standards (www.isa.org)
- IEC Standards (www.iec.ch)
- NIST Standards (www.nist.gov)
- CFATS Information (www.dhs.gov)
- ISASecure (http://www.isasecure.org/)
- WIB (http://www.wib.nl/index.html)

Copyright © 2010 - exida