



Setting the Standard for Automation™

Using the ISA/IEC 62443 Standard to Secure Your Control Systems

Course IC32E (Online)
Participant Noteset
Volume I

Copyright © ISA
67 T.W. Alexander Drive
Research Triangle Park, NC 27709 USA

All rights reserved. This book or any portion thereof
may not be reproduced or used in any manner whatsoever
without the express written permission of the publisher.



The unauthorized reproduction or distribution of a copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI and is punishable by fines and federal imprisonment.

ISA Cyber Instruction – IC32E

Online Instructor-Led Course

Using the ISA/IEC 62443 Standard to Secure Your Control Systems

This online/self-study course focuses on the issues involved in developing a cyber security program for industrial automation and control systems including risk assessment, awareness of cyber threats and exploits and the use of ‘countermeasures’ to reduce risk and/or mitigate the consequences of a successful cyber-attack. This course will aid engineering personnel with responsibility for plant/process automation systems in identifying potential vulnerabilities and implementing changes to improve the cyber security of their critical process automation systems.

The course is divided into twelve (12) separate modules, with a recommended one module or two module per week for completion. However, students may work at their own pace, provided they cover the material by the indicated review dates.

Various learning techniques will be provided to cover the weekly course areas including: pre-recorded instructor presentations, additional resources, homework assignments, reading assignments, as well as live Q&A debrief instructor sessions. Refer to your detailed course syllabus, which is provided with your course materials, for further information/instructions.

Course Schedule

Pre-Survey

Students will be asked to take a pre-survey, which includes questions related to the subject matter areas. Answers will be provided for students to assess their knowledge, prior to beginning the course materials.

Module 1: Introduction to Control Systems Security

Module 2: ISA/IEC 62443-1-1 Terminology and Regulations & Standard

Module 3: ISA99 Committee, The 62443 Standards, and Intro to the IACS Cybersecurity Lifecycle

Module 4: Establishing an Industrial Automation and Control Systems Security Program

Module 5: Industrial Networking Basics L1 - L7

Module 6: Demonstration Lab: PCAP Analysis Industrial Protocols

Module 7: Network Security Basics

Module 8: Industrial Protocols

Module 9: ISA/IEC 62443 Models

Module 10: Network Segmentation, Patch Management, and Intrusion Detection

Module 11: Security Risk Assessment and System Design Intro

Module 12: Security Program Requirements for IACS Service Providers

Post-Survey

Students will be asked to take a post-survey, which includes questions related to the subject matter areas. Answers will be provided for students to assess their knowledge, prior to beginning the course materials.

Final Examination

Thank you...

ISA Training Equipment Donors

ISA would like to thank the following companies for donating equipment for use in our hands-on training labs. By donating equipment, these companies have increased their name recognition within the industry while helping ISA continue its efforts to offer superior automation and control training.



ABB Instrumentation, Inc.



SENDING ALL THE RIGHT SIGNALS



Allen-Bradley



INSTRUMENT DIVISION

DRESSER



Process Management

Emerson Process
Management-
Rosemount Measurement

invensys®



www.flne.com

**HART
SCIENTIFIC**

Honeywell



**Prime
Technologies**

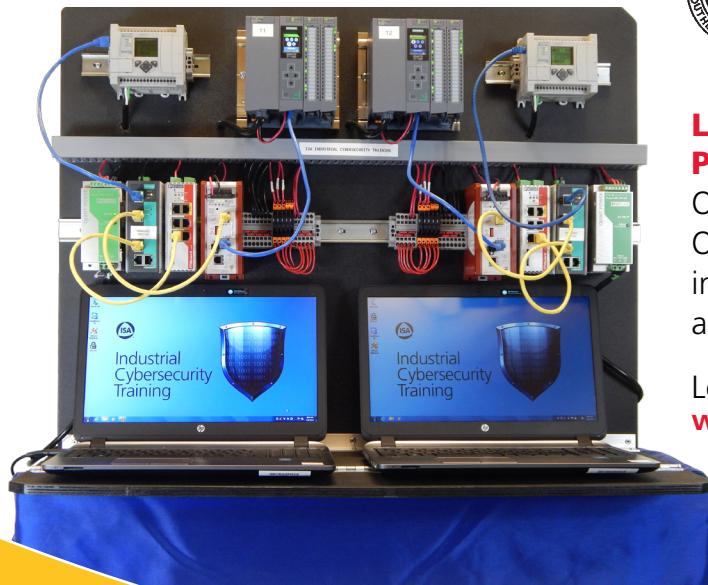
SIEMENS



THE UNDISPUTED LEADER IN PC CONTROL™



**Wade
Associates, Inc.**



Learn more with ISA's hands-on Portable Training Labs!

Our hands-on labs are ready to ship to your facility. Offering state-of-the-art equipment and expert instruction, ISA Onsite Training brings automation training directly to you.

Learn more at
www.isa.org/OnsiteTraining.

Setting the Standard for Automation™



Week 1

Week 1



Setting the Standard for Automation™

Using the ISA/IEC 62443 Standards to Secure Your Control Systems

IC32® Version 4.2

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Disclaimer

- The standard(s) and the instructors(s) cannot anticipate all possible applications or address all possible safety or operational issues associated with use in hazardous conditions
- The use or implementation of the course material information, instructor references, referenced standards, technical reports and third-party tools may adversely affect hazardous materials, operations or equipment
- The user must exercise sound professional judgment concerning use and applicability under the user's particular circumstances
- Any actions and or activities related to the material contained is solely the user's responsibility
- The user must consider the applicability of any governmental regulatory limitations, legal restrictions and ramifications, international laws, code of ethics and health, safety and environmental (HSE) practices

Course Contributors

- Eric Byres, P. Eng.
- Eric Cosman, Co-Chair ISA99 Committee
- John Cusimano, CFSE, CISSP
- Willy Leuvering, BSc, ISA/IEC-62443 Cyberexpert, ISA-88 SME, ISA95 SME
- Wally Magda, CAP, PSP, ISA/IEC-62443 Cybersecurity Expert
- Eric Persson, CACE, CISSP
- Joshua A. Smits, ISA/IEC-62443 Cybersecurity Expert
- Marjorie A Widmeyer, Member, ISA67 Committee
- Tim Shaw, PhD, CISSP
- Robert C. Webb, P.E.
- Leigh Weber, CISSP
- Victor Wegelin, PE



Course Goals

- Describe the need and importance for control system security
- Describe the structure and content of the ISA/IEC 62443 series of documents
- Discuss the principles behind the creating of an effective long-term security program
- Introduce the basics of risk analysis, industrial networking and network security

Course Goals

- Introduce the basic and fundamental concepts that form the basis for the 62443 standards (e.g., defense in depth and zones and conduits)
- Describe how to apply key risk mitigation techniques such as anti-virus, patch management, firewalls and virtual private networks
- Describe how secure software development strategies can make systems inherently more secure
- Describe what is being done to validate or verify the security of systems



Pre-Instructional Survey

- This is a self-assessment of your knowledge
- Answer the questions to the best of your ability
- The results will help you and the instructor(s) to emphasize the appropriate portions of the course



Setting the Standard for Automation™

Introduction to Control Systems Security

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Section Topics

- Defining control system cybersecurity
- Trends in control system cybersecurity
- Potential consequences
- Malware events and trends
- Common Myths Regarding IACS Security
- Regulations and Standards

Defining Control System Cybersecurity

- Electronic Security defined as actions required to protect critical systems or informational assets from unauthorized use, denial of service, modifications, disclosure, loss of revenue, destruction
- Control system defined as hardware and software components of an Industrial Automation and Control System (IACS)
- Cybersecurity defined as measures taken to protect a computer or computer system against unauthorized access or attack

Trends in Control System Cybersecurity

- Businesses have reported more unauthorized attempts and marked increase in malicious code attacks
- Control systems use more commercial off the shelf (COTS) software and hardware
- Common use of Internet Protocols (IP)
- Increased use of remote monitoring and access
- Tools to automate attacks are commonly available



Implications

- Commercial Off The Shelf (COTS) components, increased connectivity and common protocols lead to:
 - Potential adversaries are familiar with the technology
 - Many risks are common with business systems
- Remote access broadens systems “attack surface”
- Isolation or network separation is difficult or impossible

Potential consequences

- Unauthorized access, theft or misuse of data
- Loss of integrity or reliability of the control system
- Loss of control system availability
- Equipment damage
- Personal injury
- Violation of legal and regulatory requirements

Malware Events and Trends

- Malware as a Service (MaaS)
- Hacking as a Service (HaaS)
- Crimeware as a Service (CaaS)
- Fraud as a Service (FaaS)

Malware Events and Trends

- Ransomware detections uptick
- Trojan variations up by over 200 %
- **Norsk Hydro Ransomware cyber attack** (19 March 2019)
 - Global aluminum solutions company
 - Hydro cyber attack in the late hours of 18 March impacting operations
 - Cyber attack financial impact of NOK 400-450 million in the first quarter 2019 (USD 46-52 million)

Operator stated that about 10:45 pm the screen on the system controller turned red and an error message turned up.

Operator contacted emergency telephone!!!

Malware Events and Trends

- Malware knows no borders
- Ransomware gained traction
 - Over 500% increase in attacks against businesses
 - Targets switched from home users to commercial organizations
 - Commercial can afford to pay larger ransoms
 - WannaCry
 - Leaked tool from USA National Security Agency
 - 45,000 hits in 74 countries
- Sea Turtle Domain Name System (DNS) attacks
 - Nation State type attack
 - Began January 2017 and ongoing through 2019
 - 13 countries hit
 - DNS hijacking

Malware Events and Trends

- Oldies but goodies with new variants
- Stuxnet
 - #1 2010 Harm Iran's centrifuges
 - #2 2018 Harm Iran's telecommunications infrastructure
- Shamoon
 - #1 targets Saudi Aramco, wipes 30,000 computers (2012)
 - #2 targets Saudi company, Virtual Desktop Interface affected (2016)
 - #3 targets Italian Oil and Gas Company (2018)
- Malware is Operating System (OS) agnostic
 - Windows OS about 80% of market thus richer target
 - Non-windows OS are vulnerable
 - Non-windows OS can be used to relay malware to Windows OS
 - All can be compromised via password phishing
 - Shellshock (Bashdoor) had Unix | Linux | MacOS X variant

Common Myths Regarding IACS Security

1. We don't connect to the Internet
2. Our control systems are behind a Firewall
3. Hackers don't understand control systems
4. Our facility is not a target
5. Our safety systems will protect us

1. We Don't Connect to the Internet

- Industrial protocols found on Shodan ICS Radar
 - Sample of typical applications
 - **BACnet**—Building Automation
 - **DNP3**—Electric/Water
 - EtherNet/IP—Common Industrial Protocol
 - Modbus—Open-source SCADA
 - **Niagara Fox**—Building automation
 - Niagara Fox with SSL—Building automation
 - Siemens S7—Ethernet S7 PLC

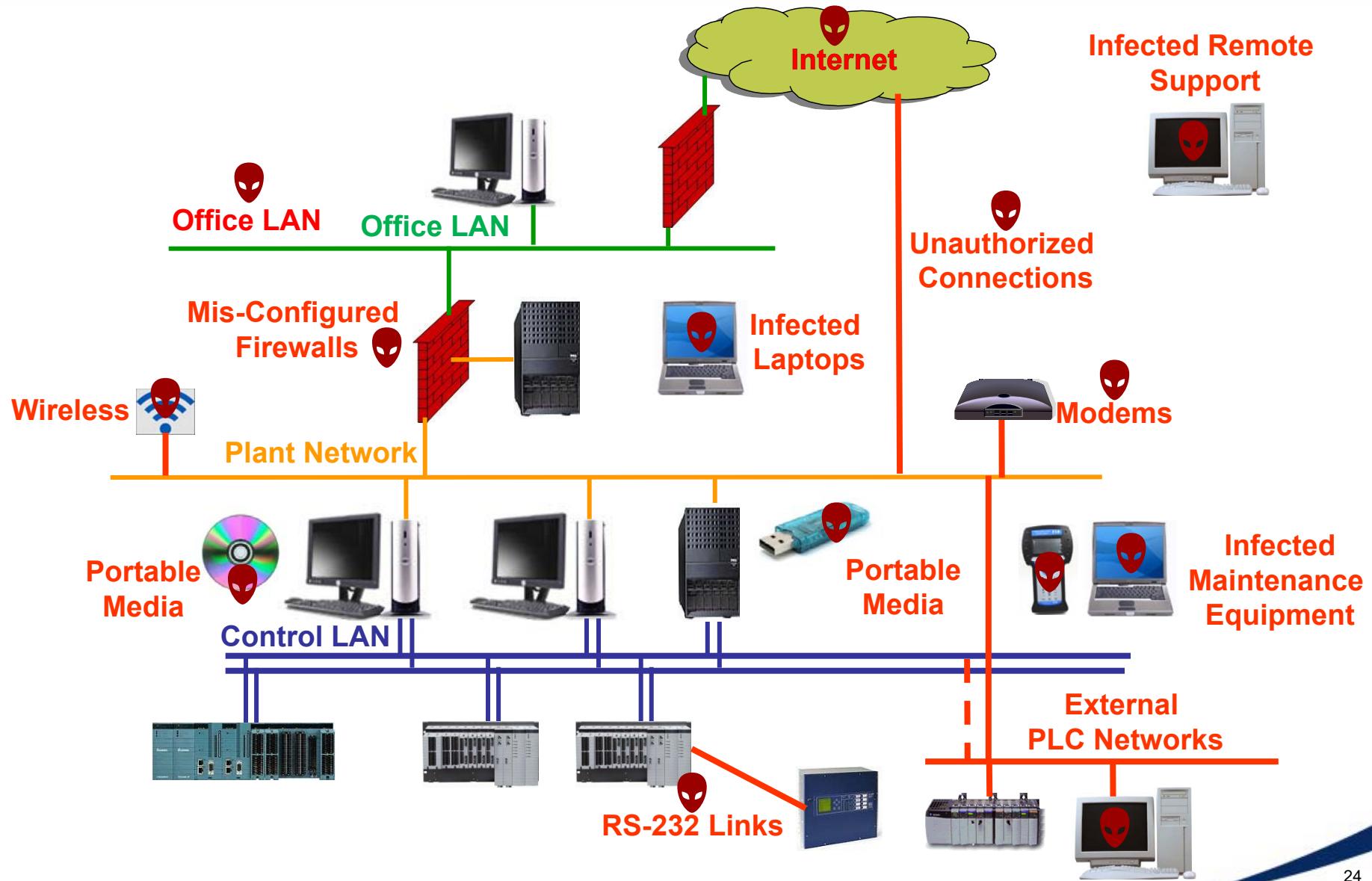
Systems are connected to the Internet!

(SHODAN / Project SHINE)

<https://www.shodan.io/>

<https://ics-radar.shodan.io/>

1. We Don't Connect to the Internet



2. Our Control Systems Are Behind a Firewall

- 2004 study of 37 firewalls from financial, energy, telecommunications, media, automotive, and security firms...
“Almost 80 percent of firewalls allow both the “Any” service on inbound rules and insecure access to the firewalls. These are gross mistakes by any account.”
- 2010 study revisits 2004 findings
 - 84 firewalls evaluated
 - Firewalls are still badly misconfigured
 - Modern configuration software doesn’t help admins make fewer mistakes
- 2014 and 2015 study finds top control system cyber weakness was insufficient network boundary protection
- Even if configured correctly there are published vulnerabilities



3. Hackers Don't Understand Control Systems



- This is no longer true
- Hacking is no longer just for fun – hackers now sell zero-day exploits to organized crime
- Hacking as a Service has hit the mainstream
 - No longer only on underground dark web
 - Jobs put out to bid
- SCADA and process control systems are now common topics at “DEFCON” and “Blackhat” conferences

3. Hackers Don't Understand Control Systems

- Double edged sword providing timely information about current security issues, vulnerabilities, and exploits

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.

ICSMA-21-084-01 : Philips Gemini PET/CT Family

ICSA-21-082-02 : GE MU320E

ICSA-21-033-01 : Rockwell Automation MicroLogix 1400

ICSA-21-075-03 : Hitachi ABB Power Grids AFS Series

ICS-CERT Alerts

ICS-ALERT-20-217-01 : Robot Motion Servers

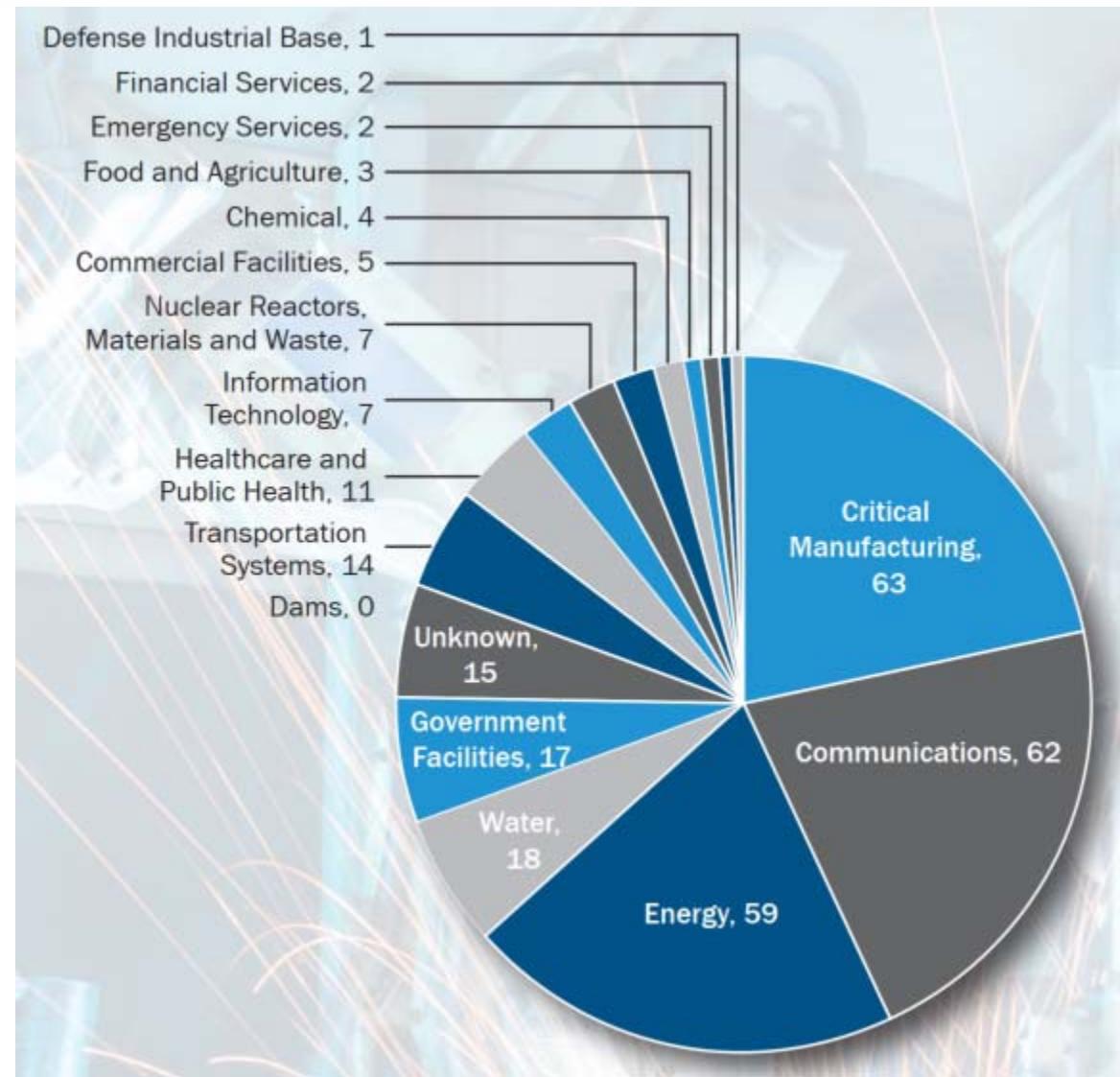
ICS-ALERT-20-063-01 : SweynTooth Vulnerabilities

ICS-ALERT-19-225-01 : Mitsubishi Electric Europe B.V. smartRTU |

ICS-ALERT-19-211-01 : CAN Bus Network Implementation in Avionics

4. Our Facility is Not a Target

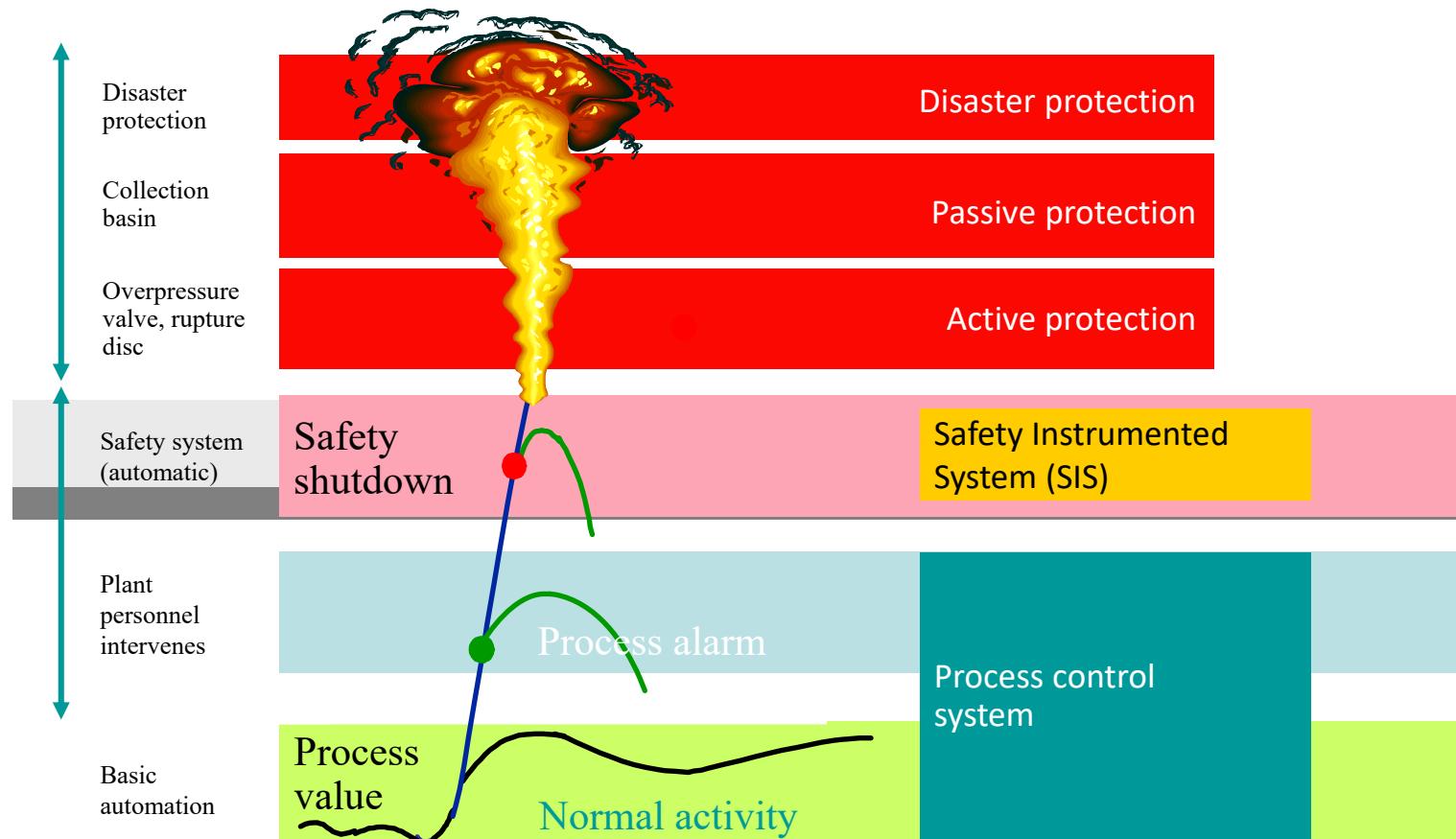
Incidents by sector
290 in 2016



5. Our Safety Systems Will Protect Us

- Modern safety systems are micro-processor based, programmable systems configured with a Windows PC
- Now commonplace to integrate control and safety systems using Ethernet communications with open and insecure protocols (Modbus TCP, OPC, etc.)
- Many safety system communication interface modules run embedded operating systems and Ethernet stacks that have known vulnerabilities
- “Triton” or “Trisis,” malware disrupts an emergency shutdown capability in Triconex safety instrumented system (SIS), shut down operations

5. Our Safety Systems Will Protect Us



- Even the most sophisticated SIS/SIL can be defeated by an attacker



Setting the Standard for Automation™

Regulations and Standards

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits



Regulations

ISA
NIST
NEI ISO
ICPA-Japan FISMA
CFATS AGA FCC
NISS-D7-Saudi-Arabia
NESAA-UAE Local/State
FERC SEC DHS
DOE OSHA
NERC-CIP
NIS-Directive Regulation EU

Some are Mandatory

- Department of Homeland Security
 - 6 CFR part 27: Chemical Facility Anti-Terrorism Standards (CFATS)
- Department of Energy
 - Federal Energy Regulatory Commission (FERC)
 - 18 CFR Part 40, Order 822 (mandates NERC CIPs 002-014)
- Nuclear Regulatory Commission
 - 10 CFR 73.54 Cyber Security Rule (2014)
 - RG 5.71
- Above are North American focused
 - Do you know of any in your region?

Limitations

- Limited number enforced cyber and physical security regulations—no teeth
- National cyber security strategies may or may not be in place
- Public-private partnerships lacking
- Sector-specific cybersecurity plans may or may not exist
- Regulation compliance is mandatory while standards compliance is voluntary
- General agreement that no country or government can address cybersecurity risk in isolation

Standards

- Compliance and conformance is voluntary
 - Consensus driven
 - Collaborative approach preferred
- There is no requirement on anyone to use them unless....
 - If agreed to in a contract or referred to in regulation
 - Penalty, either civil or criminal, for not complying with them
- Courts may decide in the absence of relevant regulation
 - Non-compliance with a standard
 - Using a “what would a reasonable man on the street do” test
 - Sufficient grounds to determine liability
 - EUROPEAN COMMISSION Standards and Standardization Handbook



Standards Content

- Standards contain both normative and informative elements
- Normative elements are those parts that shall be complied with in order to demonstrate compliance with the standard
- Normative elements are indicated by the use of the words “shall” or “must”
- Informative elements provide clarification or additional information
- Informative elements may not contain requirements
 - The words “shall” and “must” are not used

Recap

- ✓ Defining control system cybersecurity
- ✓ Trends in control system cybersecurity
- ✓ Potential consequences
- ✓ Malware events and trends
- ✓ Common Myths Regarding IACS Security
- ✓ Regulations and Standards



Setting the Standard for Automation™

Concepts and Models

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Concepts

- Differences between IT and IACS
- Defense-in-Depth
- Security Zones & Conduits

Differences between IT and IACS

- There are important differences between IT systems and IACS
- Problems occur because assumptions that are valid in an IT environment may not be valid on the plant floor and vice versa
- IACS cyber security must address issues of safety, which is not usually an issue with conventional IT cybersecurity
- Understanding the different needs of IACS and IT system security leads to cooperation and collaboration between historically disconnected camps

Different Security Priorities

Industrial Automation &
Control Systems

Availability

Integrity

Confidentiality

Priority

General Purpose
Information Technology
Systems

Confidentiality

Integrity

Availability

- ANSI/ISA-62443-1-1, sub-clause 5.2 Security Objectives, page 36

Different Performance Requirements

IT	IACS
Response must be reliable	Response is time critical
High throughput	Modest throughput
High delay and jitter tolerated	High delay a serious concern
Less critical emergency interaction	Response to emergencies is critical
IT protocols	IT and industrial protocols

Different Availability Requirements

IT	IACS
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Rebooting tolerated	Rebooting may not be acceptable
Beta testing in the field acceptable	Thorough QA testing expected in non-production environment
Modifications possible with little paperwork	Formal certification may be required after any change

- Need to understand the reliability impacts of information security technologies before deploying.
- Example: Installing a service pack in the pharmaceutical industry requires an expensive recertification of the system.

Different Operating Environments

IT	IACS
Typical “Office” Applications	Special Applications
Standard OS's	Standard and embedded OS's
Upgrades are straightforward	Upgrades are challenging and may impact hardware, logics and graphics
Technology is refreshed often Commercial Off The Shelf (COTS) (3 to 5 years)	Legacy systems (15-20 years)
Abundant resources (memory, bandwidth)	Resource constrained
Data center, server room or office environment	Industrial environment

Different Risk Management Goals

IT	IACS
Data confidentiality and integrity paramount	HSE and production are paramount (integrity & availability)
Risk impact is loss of data, delay of business operations	Risk Impact is loss of life, equipment or product
Recover by reboot	Fault tolerance essential

- Example: **Password lockout procedures:**
 - IT: Lockout ALL access for the 10 minutes after 3 failed login attempts.
 - IACS: Make operator access easy and foolproof.
- Operator panics during chlorine leak and miss-spells his password three times. HMI lockouts ALL access for 10 minutes.
 - The outcome can be disastrous

Addressing the Differences

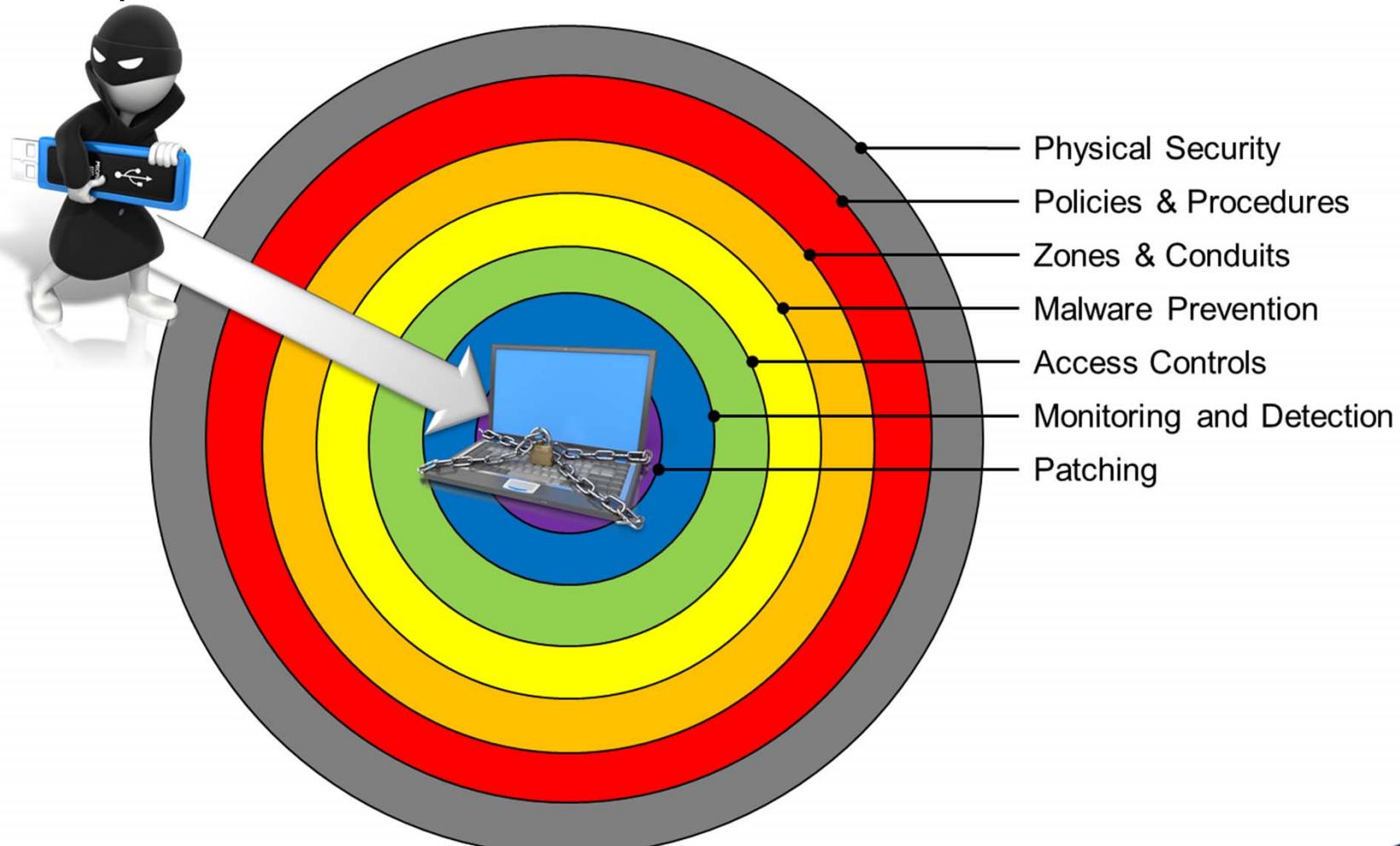
- DON'T throw out all IT security technologies and practices and start from scratch
- DO borrow IT security technologies and practices but modify them and learn how to use them properly in IACS
 - IACS uses IT technologies like Windows, TCP/IP and Ethernet
 - Much of IT policy and technology will work for control systems
 - IT environment doesn't deal in safety, only security
- DO develop clear understanding how IACS assumptions and needs differ from that of the IT environment
 - Identify and address the 10% that differs early on
 - AIC versus CIA security orientation

Defense-in-Depth

- A Perimeter Defense is Not Enough
- The bad guys will eventually get in.
- Can't just install a firewall and forget about security
- Must harden the control systems network
- You need
 - Defense in Depth
 - Detection in Depth
 - Accountable and timely incident response

Defense-in-Depth

“Defense in Depth” – applying multiple countermeasures in a layered or stepwise manner.



Detection in Depth

- There should be alarms, logs, and detection methods to identify:
 - Unusual data transfer patterns
 - Unexpected protocols being used
 - Out-of-time data traffic
 - Communication to unknown or unexpected MAC/IP Addresses
 - Logs turned-on to monitor activity
 - Send SYSLOG compatible logs to a central logging server
 - IDS sensors deployed across multiple zones in the production environment tuned to detect anomalous traffic
 - Patch Management & Anti-virus report devices out-of-date
 - Detection of unknown devices
 - Detection of missing devices

Cyber Risk

- Risk = Threat x Vulnerability x Consequence
- Risk Response
 - Design the risk out
 - Reduce the risk
 - Accept the risk
 - Transfer or share the risk
 - Eliminate/redesign redundant or ineffective controls
- Risk Tolerance
 - It is management's responsibility to determine the level of risk the organization is willing to tolerate

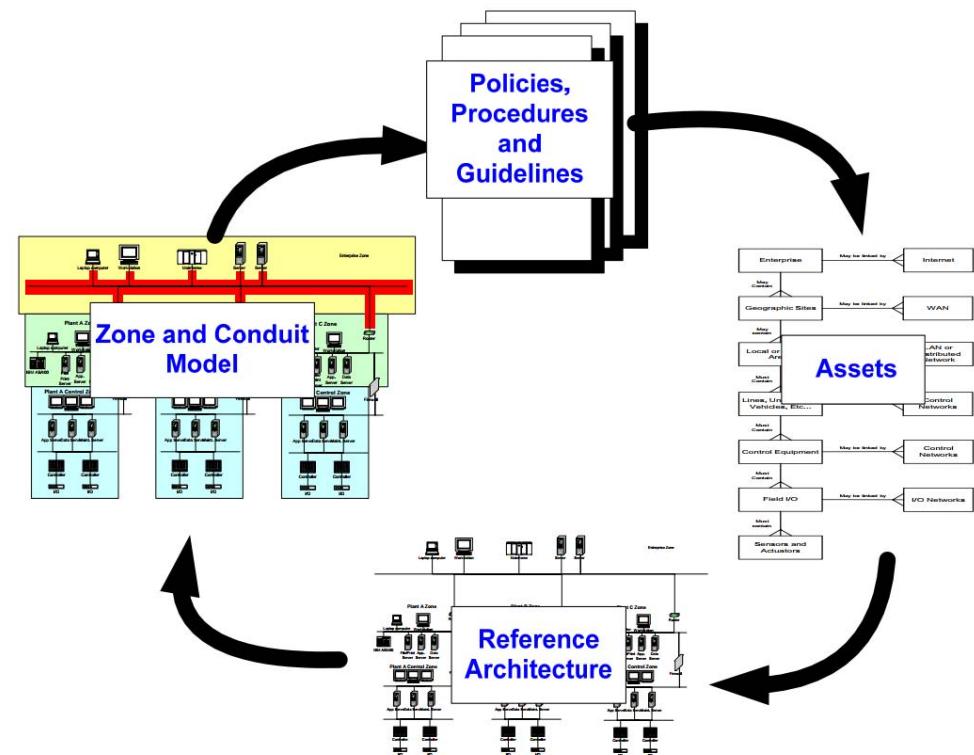


Models

- Reference models provide the overall conceptual basis
- Asset model describes relationships between assets within an industrial automation and control system
- Reference architecture describes the configuration of assets
- Zone model groups reference architecture elements according to defined characteristics (zone and conduits)
- This provides a context for the definition of policies, procedures, and guidelines, applied to the assets
 - ANSI/ISA-62443-1-1, clause 6, page 69

ISA99 Model Relationships

- Policies, Procedures and Guidelines
- Assets
- Reference Architecture
- Zone and Conduit Model
- Related to one another
- Make up a security program



Reference Model Levels

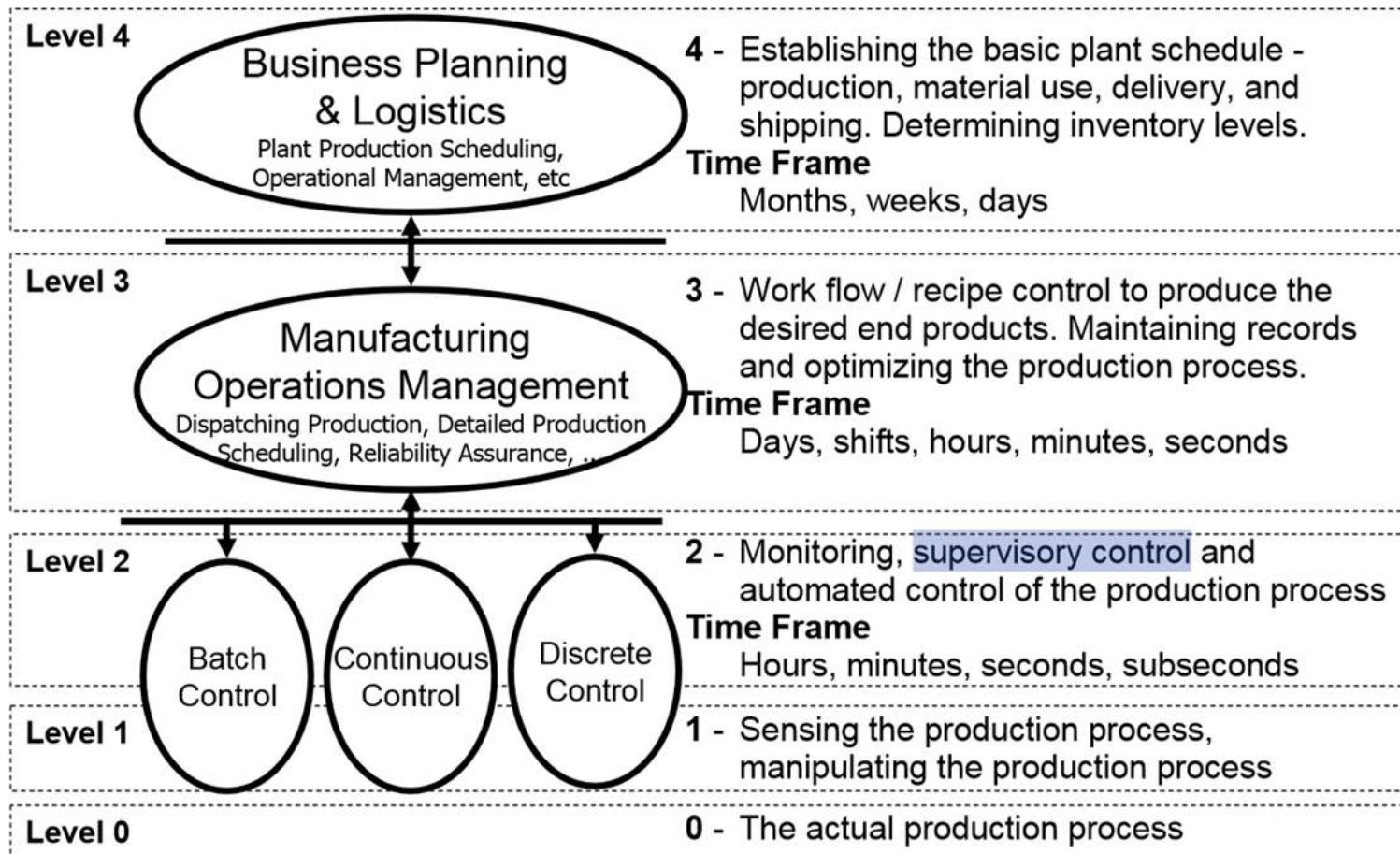
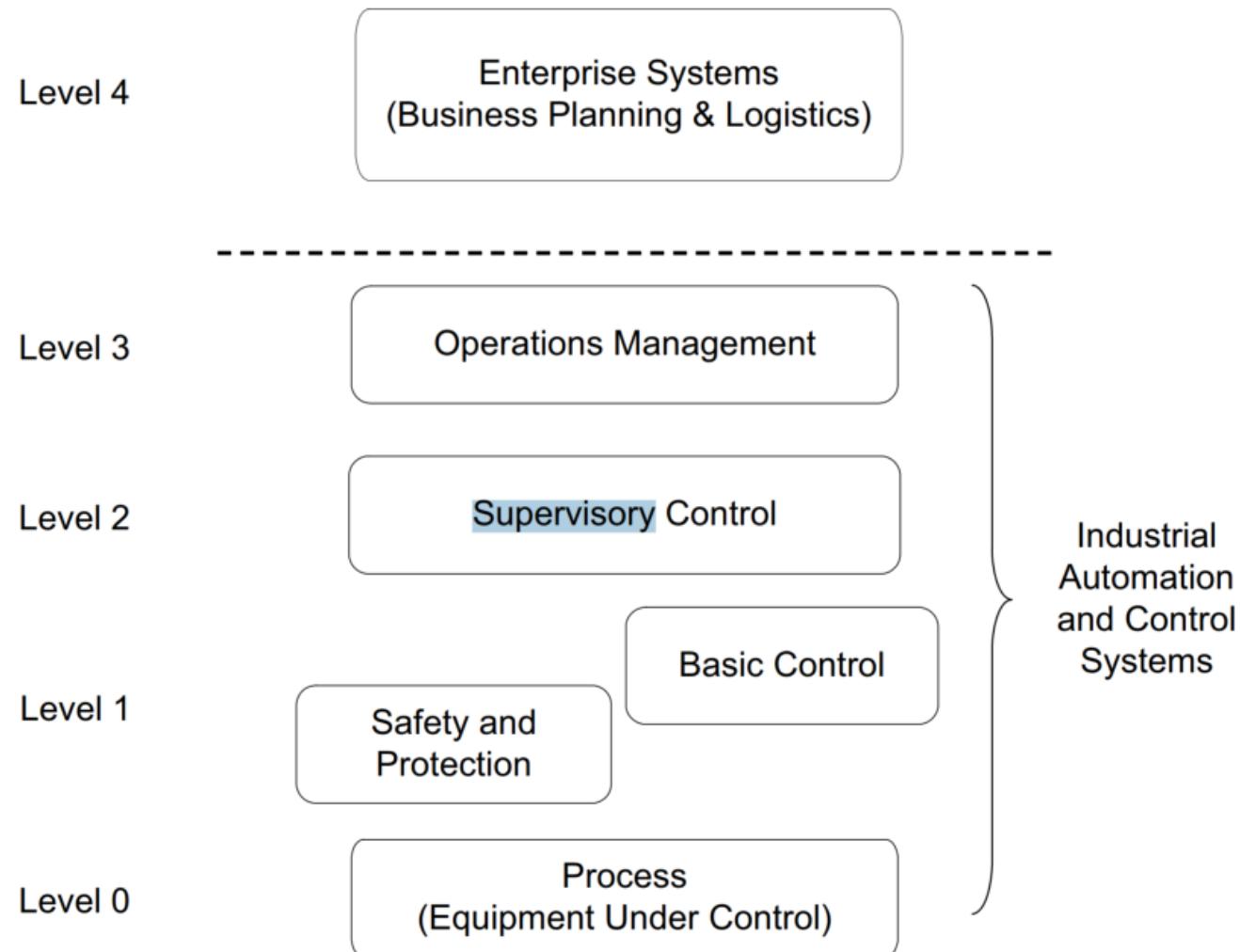


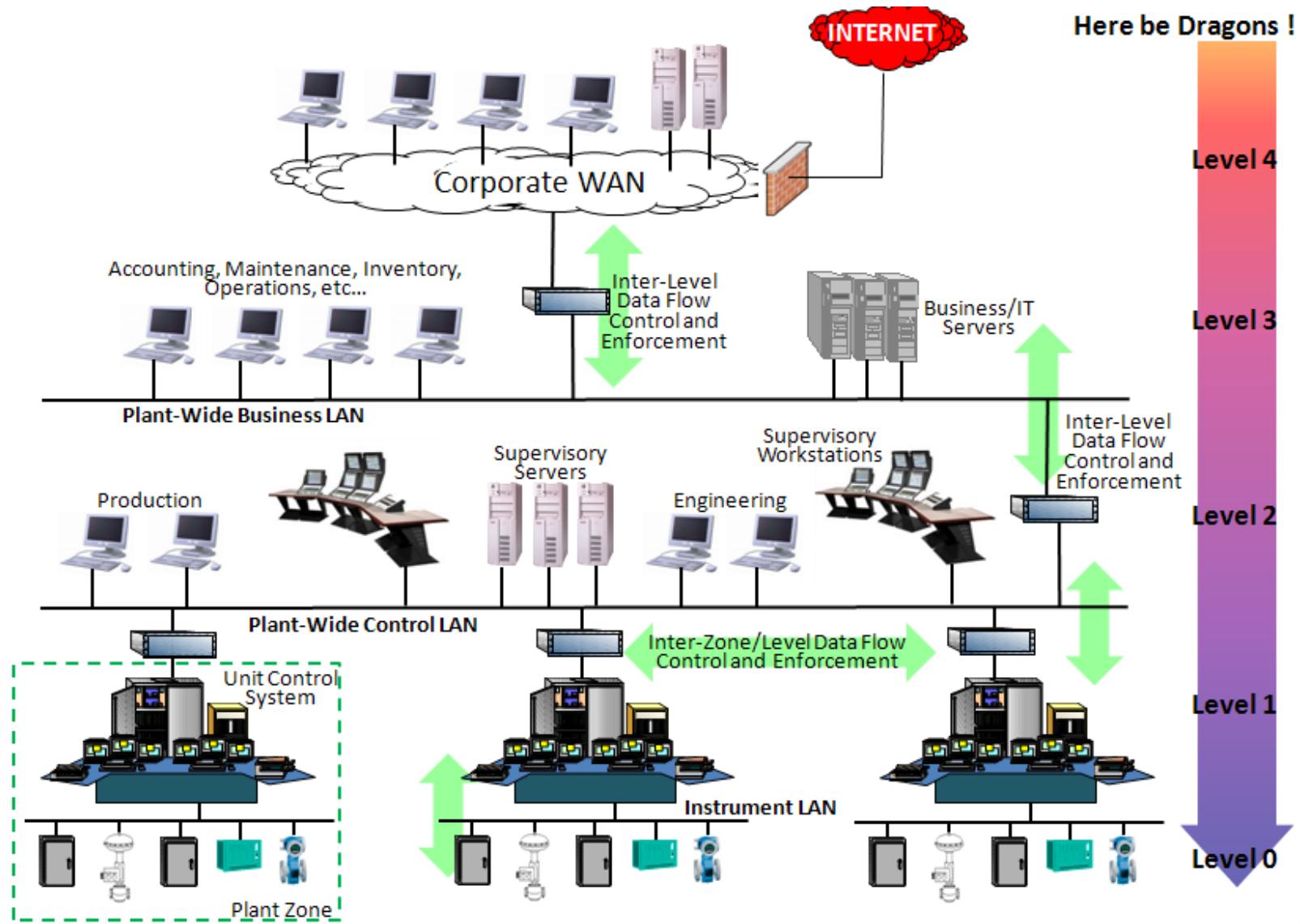
Figure 3 – Functional hierarchy

ANSI/ISA-95

Reference Model for ISA99 Standards



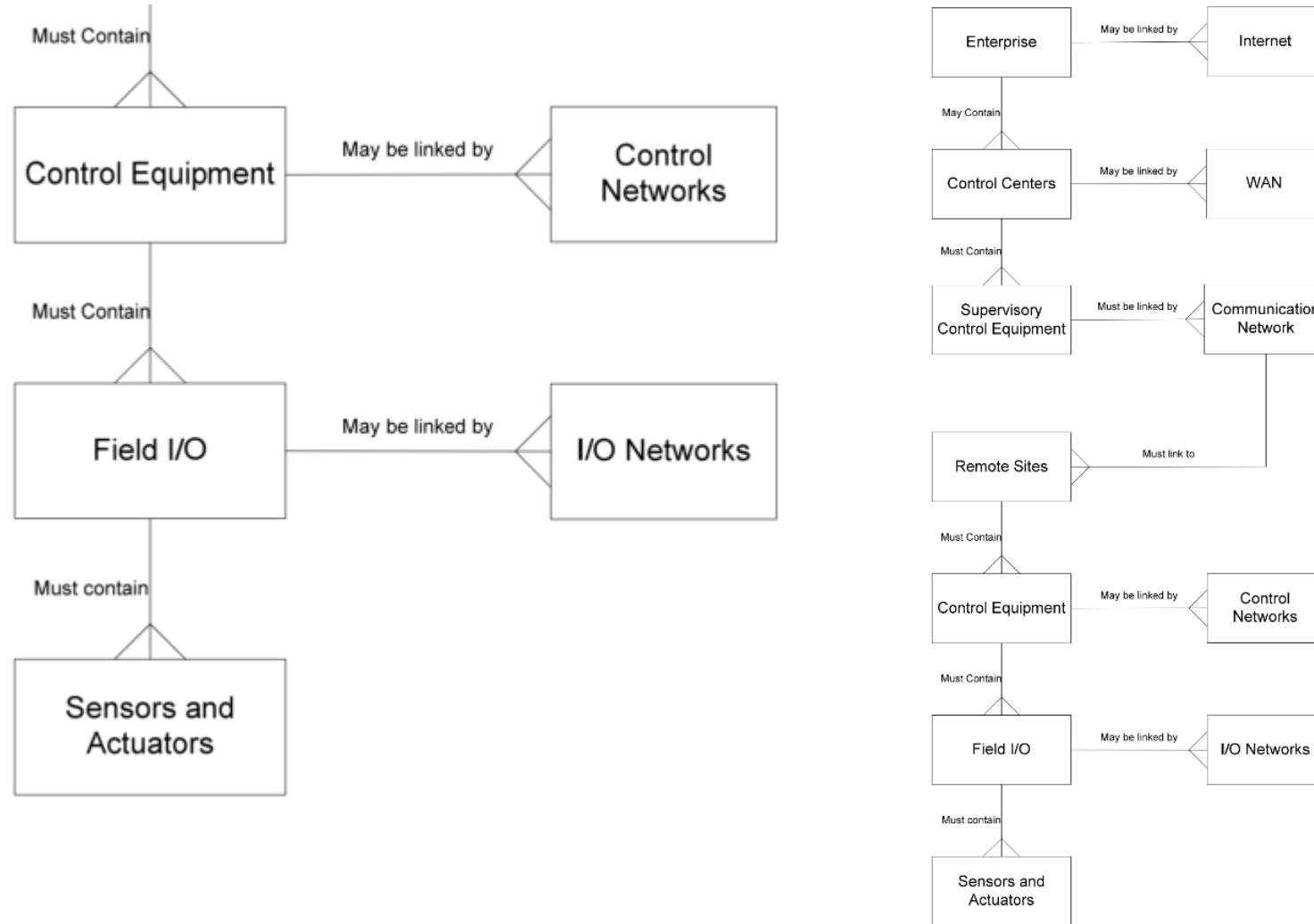
Generic Reference Model



Asset Models

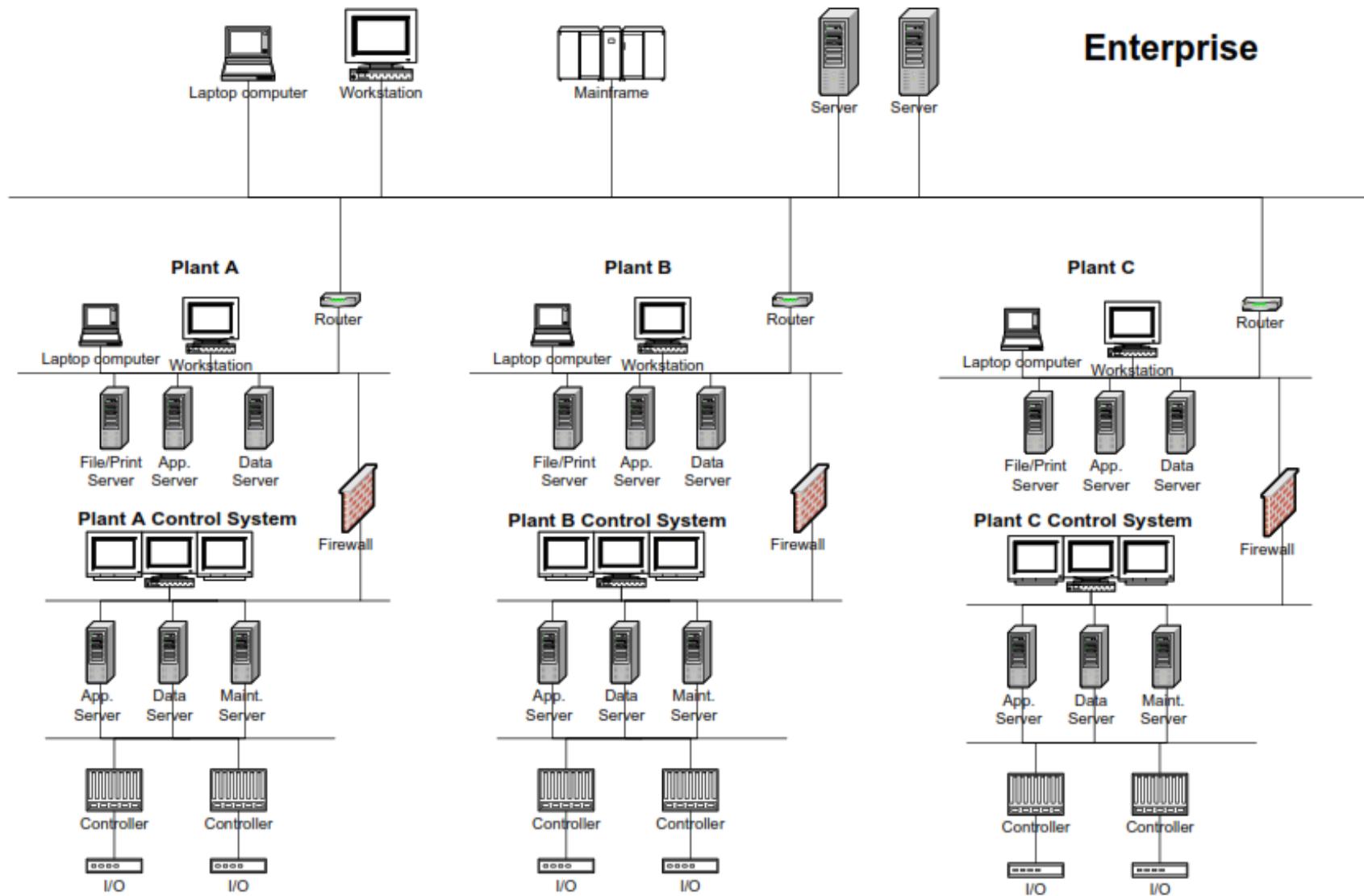
- Asset model starts at a high level
- Includes all ANSI/ISA-95 Level 0, 1, 2, 3, 4 equipment and information systems
- Explicitly includes networks and ancillary equipment
- Generic enough to fit the many situations where control systems are deployed

Asset Model SCADA system example



Refer to ANSI/ISA-62443-1-1, Figure 15, page 75

Reference Architecture Example



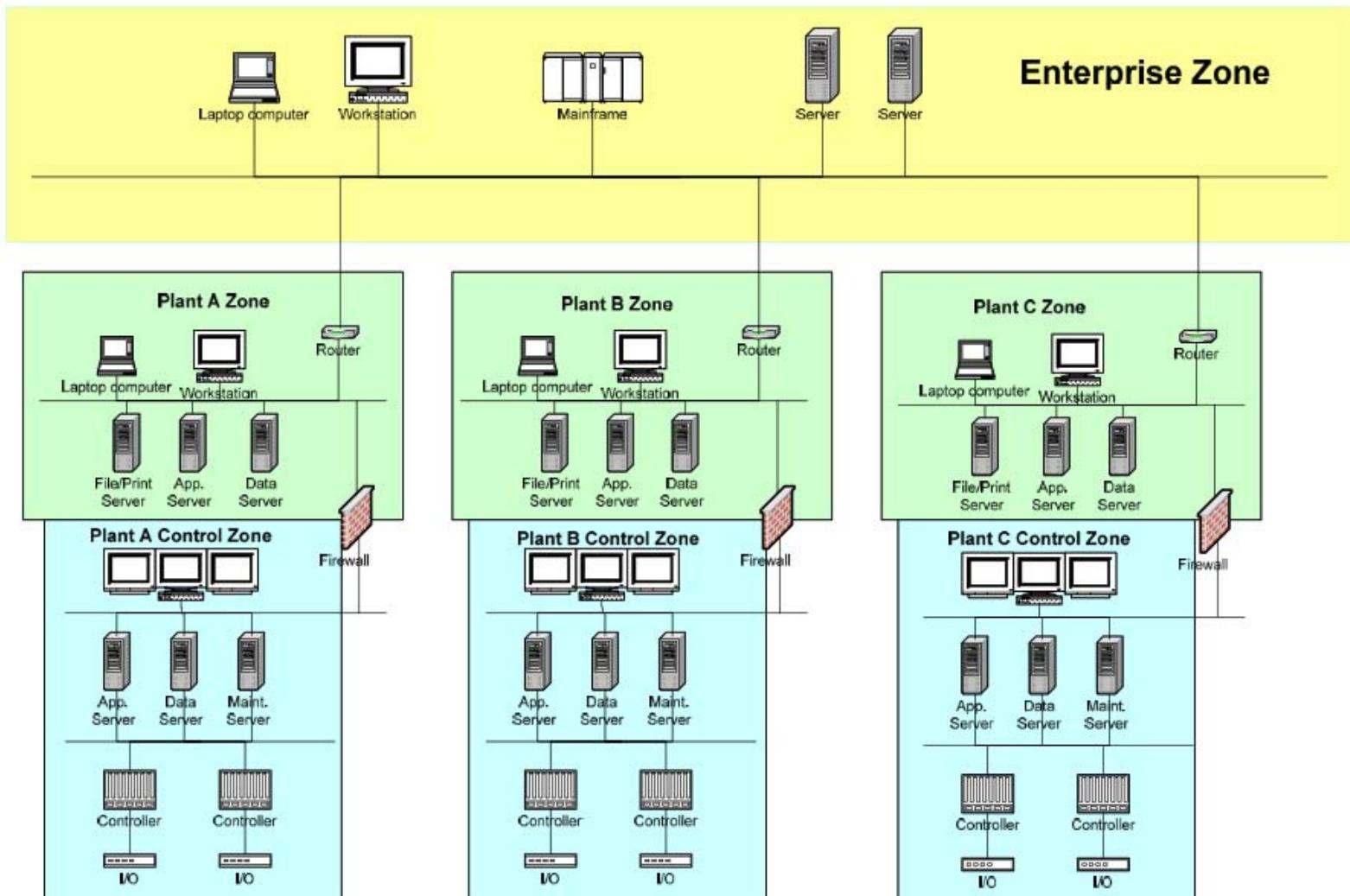
Security Zones

- Security zone is a logical grouping of physical, informational, and application assets sharing common security requirements
- There can be zones within zones, or subzones, that provide layered security, giving defense in depth and addressing multiple levels of security requirements
- A security zone has a border, which is the boundary between included and excluded elements
- Security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone

Security Zones

- Trusted definition
 - Confidence that an operation or data transaction source, network or software process can be relied upon to behave as expected
 - Attribute of an entity that is relied upon to a specified extent to exhibit an expected behavior
- Untrusted definition
 - Not meeting predefined requirements to be trusted
 - Entity that has not met predefined requirements to be trusted
 - Entity may simply be declared as untrusted.
- Zones can be defined
 - Physically (physical zone)
 - Logically (virtual zone)

Security Zone Model



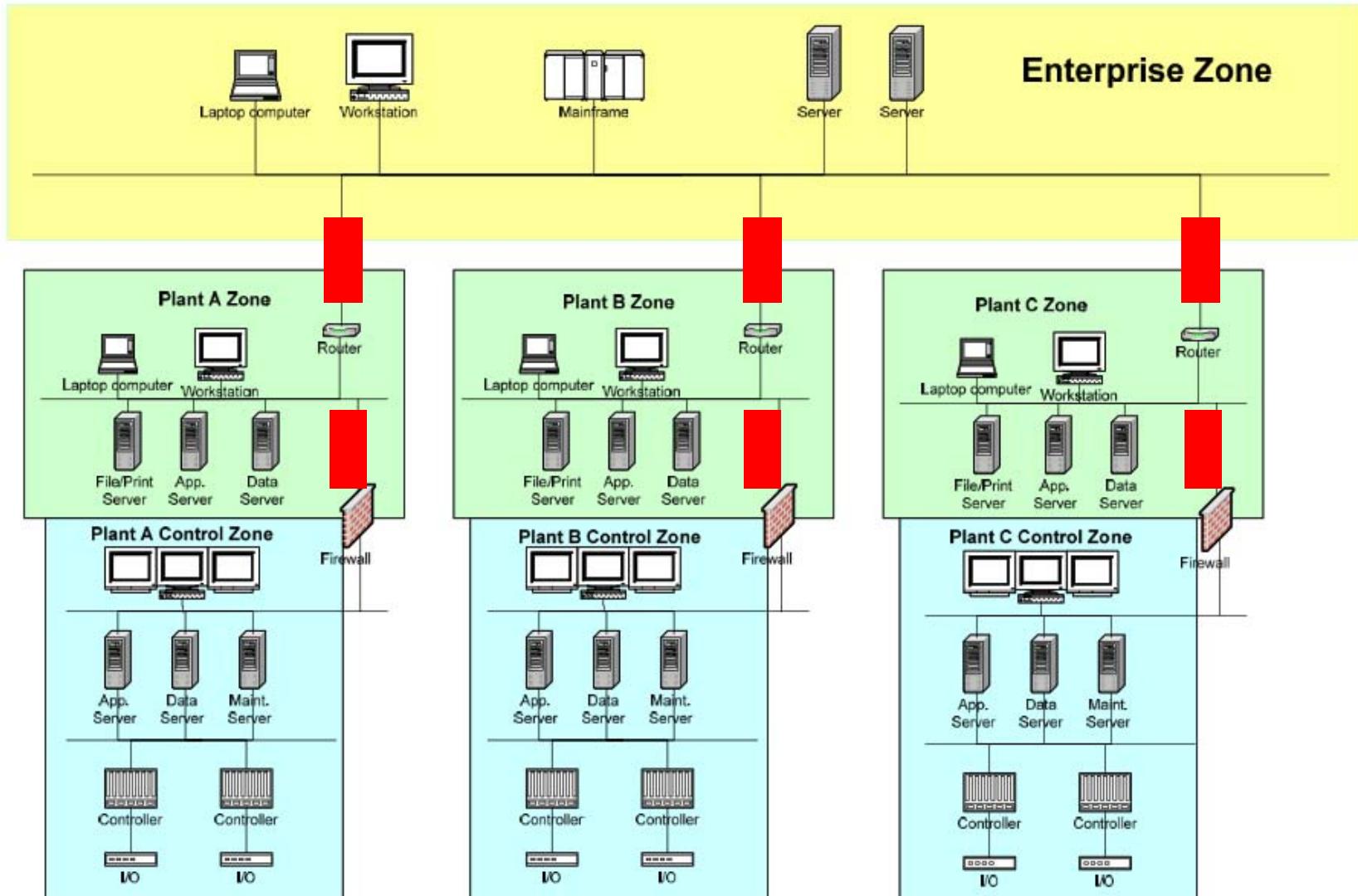
Conduits

- Conduit is a logical grouping of communication assets that protects the security of the channels it contains
 - Similar to how physical conduit protects cables from physical damage
- Stated another way
 - logical grouping of communication channels, connecting two or more zones, that share common security requirements
- Trusted conduits crossing zone boundaries must use an end-to-end secure process
- Physical devices and applications that use the channels contained in a conduit define the conduit end points
- Can be defined physically or logically

Conduits

- Physically a conduit can be cable or wireless that connects zones for communication purposes
- A conduit is a type of zone that cannot have subzones
 - Conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone
 - Can be trusted or untrusted
- Conduits are defined by the list of all zones that share the given communication channels
- It can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carrier
- Conduit is the wiring, patch panels, black boxes, hubs, media converters, routers, switches, and network management devices that make up the communications path under study

Conduit Model



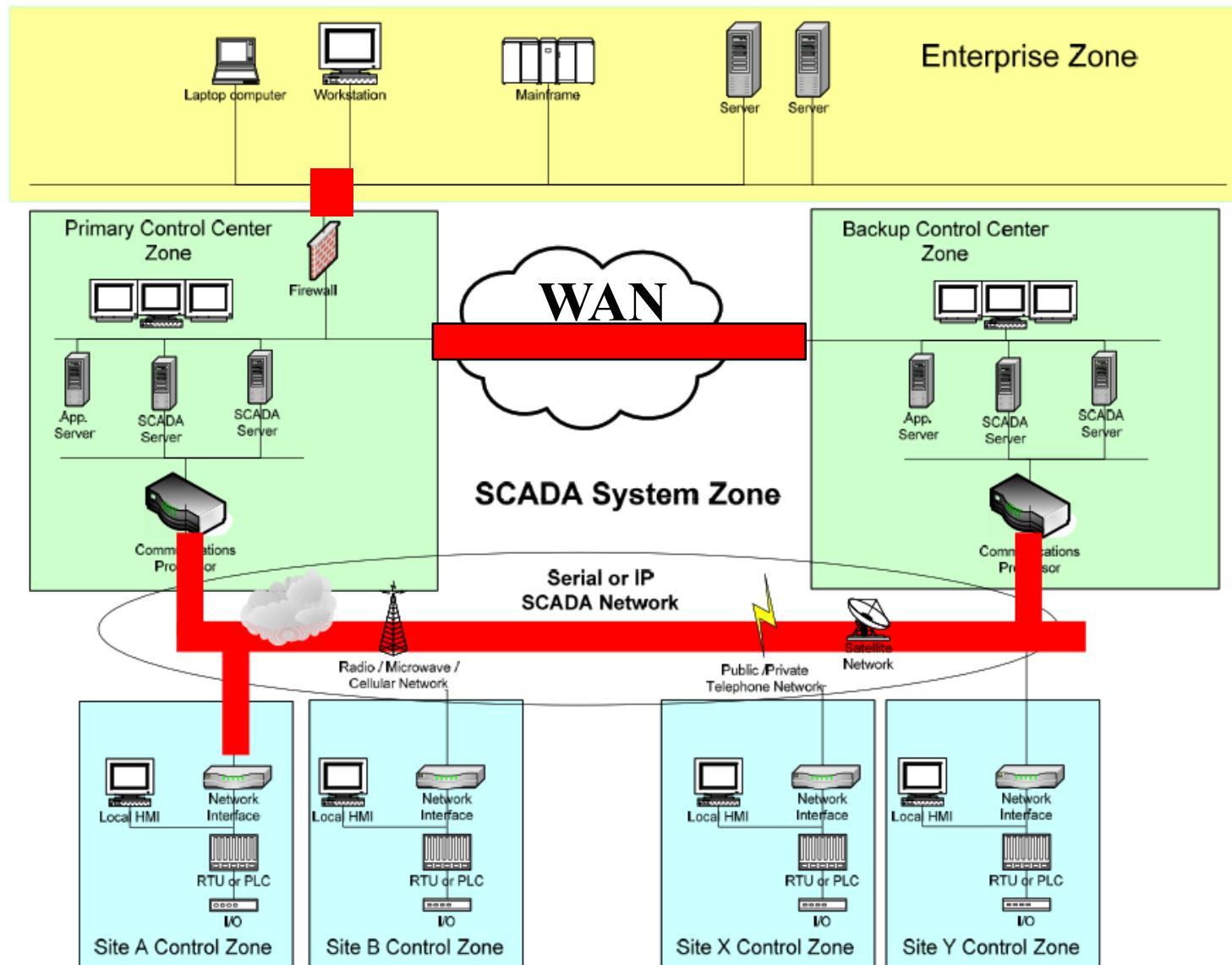
Zone & Conduit Characteristics

- Name and/or Unique Identifier
- Accountable organization(s)
- Definition of logical boundary
- Definition of physical boundary
- Safety designation
- Connected zones or conduits
- SL-T

Zone & Conduit Characteristics – cont'd

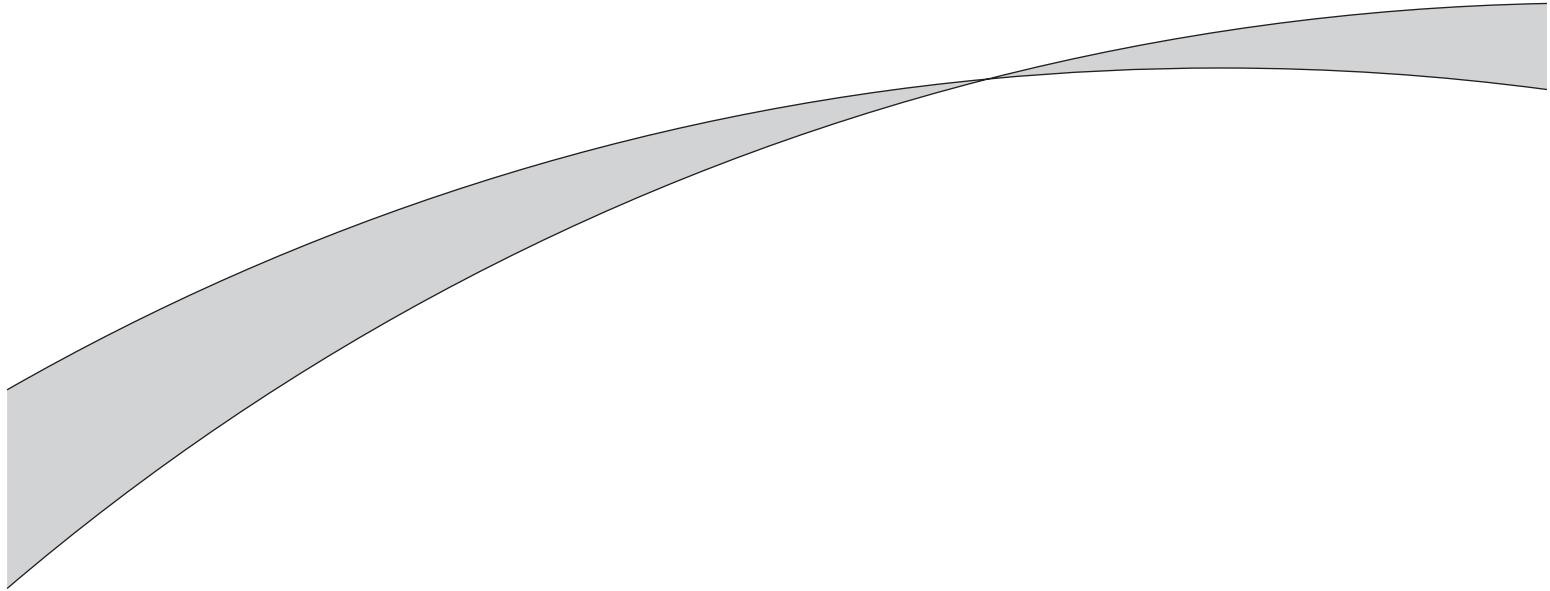
- Applicable security requirements
- Applicable security policies
- Assumptions and external dependencies
- List of logical access points
- List of physical access points
- List of data flows
- List of assets

Zone & Conduit Models



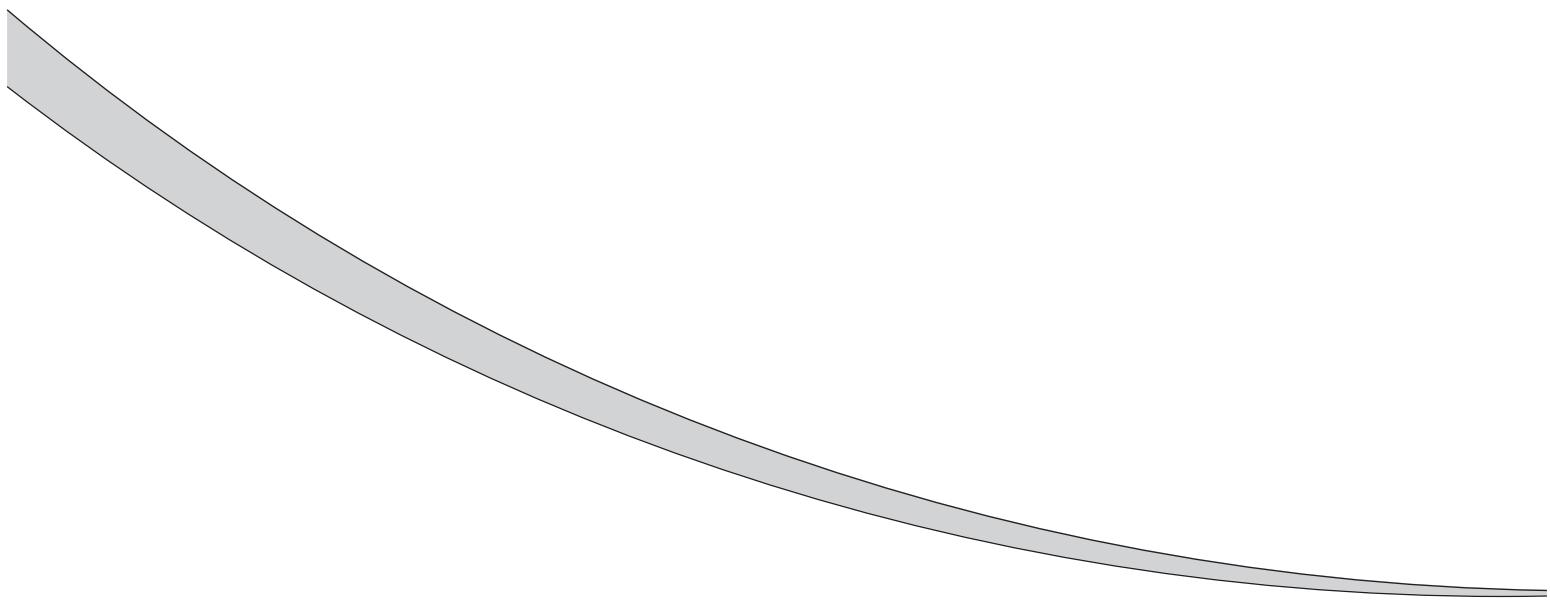
Recap

- Differences between IT and IACS
- Defense-in-Depth
- Security Zones & Conduits



Week 2

Week 2





Setting the Standard for Automation™

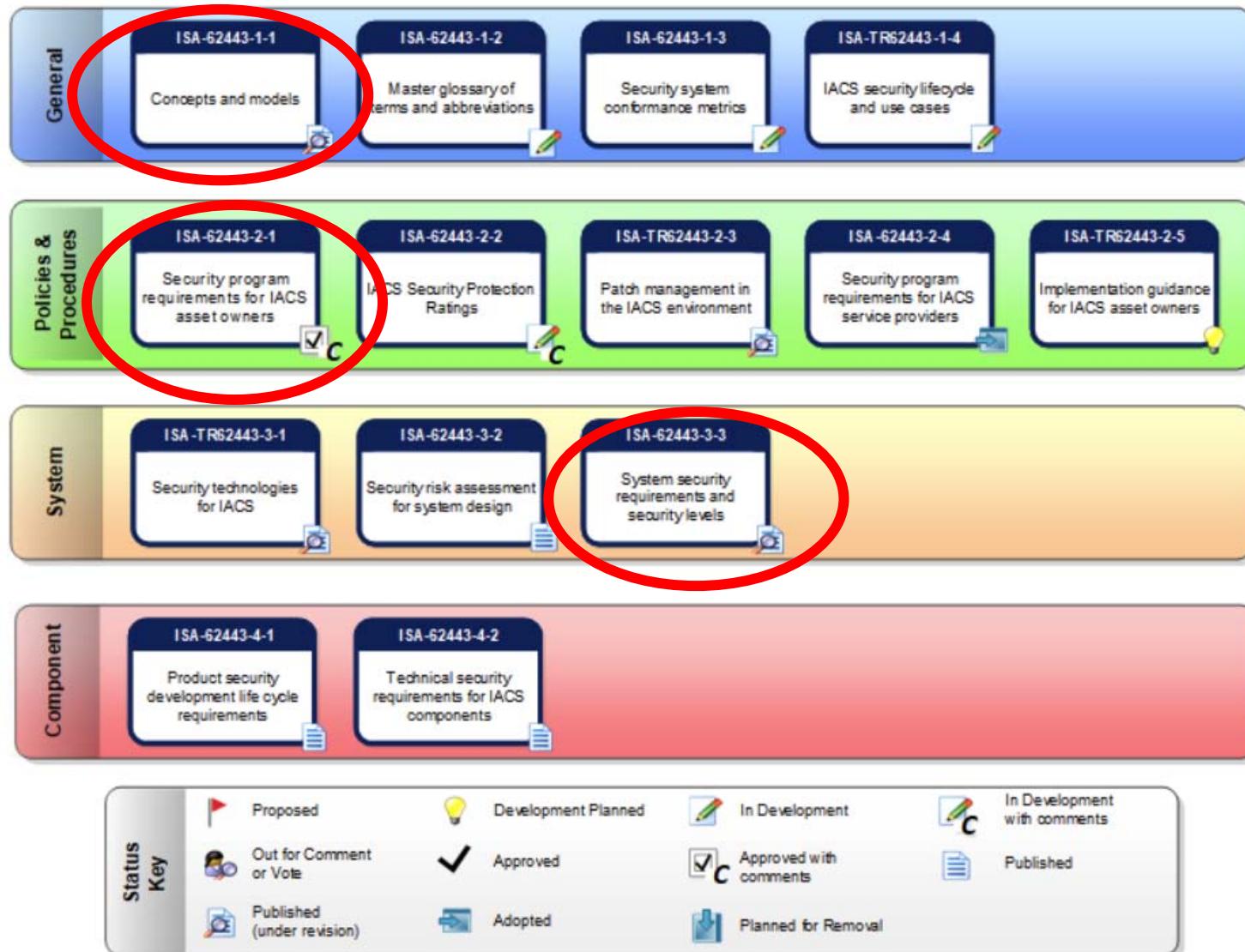
ISA/IEC 62443 Terminology

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Topics

- ISA/IEC 62443 Series Overview
- Course Primary Sources
- ICS versus IACS
- Terminology and Concepts

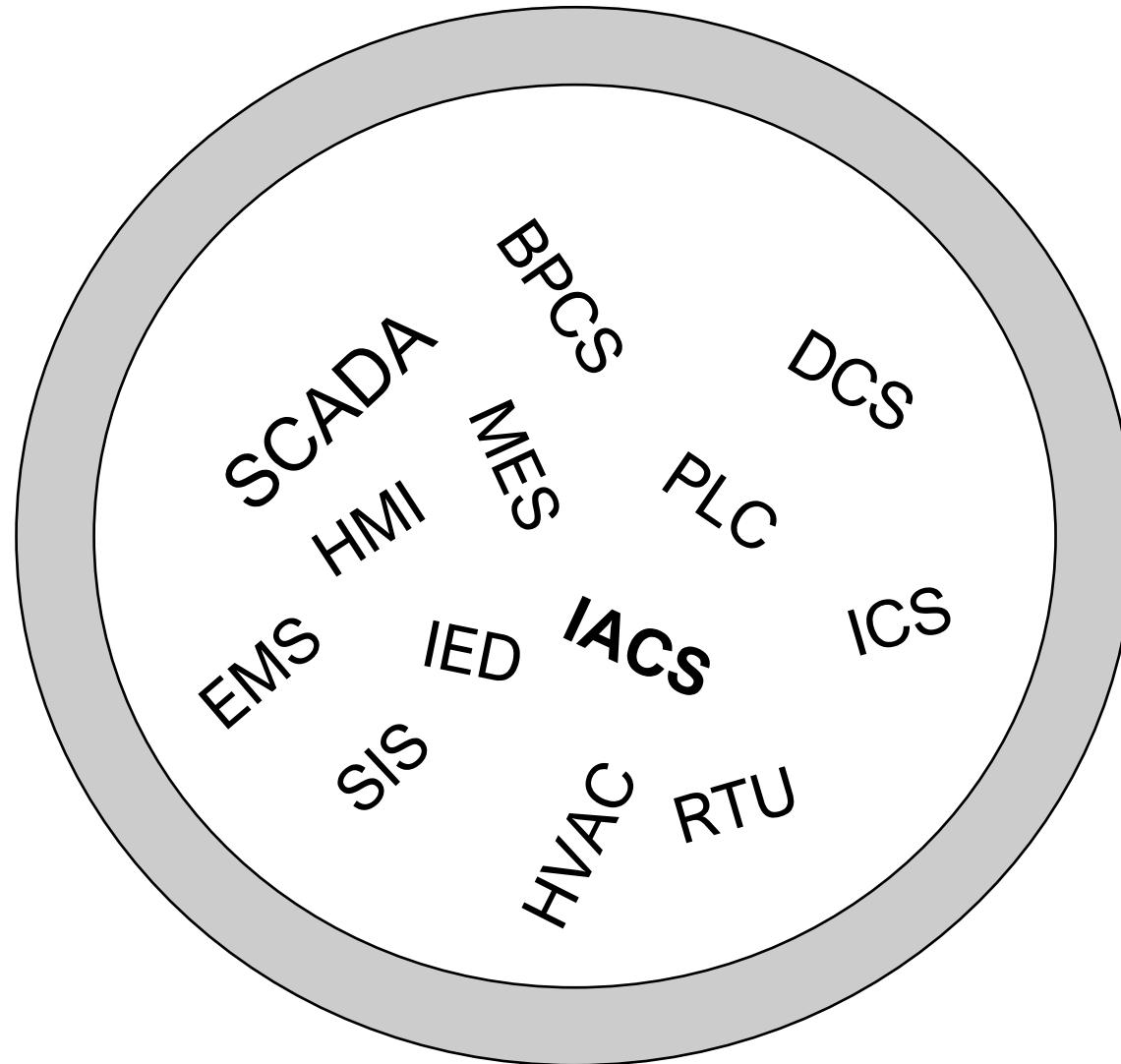
Series Overview



Course Primary Sources

- Primary Sources for Course
 - **ANSI/ISA-62443-1-1** Security for Industrial Automation and Control Systems: Part 1: Terminology, Concepts, and Models (Approved 29 October 2007)
 - **ANSI/ISA-62443-2-1** Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control System Security Program (Approved 13 January 2009)
 - **ANSI/ISA-62443-3-3** Security for industrial automation and control systems Part 3-3: System security requirements and security levels (Approved 12 August 2013)

Alphabet Soup of Control System Acronyms



ICS or IACS?

- ICS = Industrial Control System(s)
 - General term for types of control systems acting together to achieve an industrial objective
- IACS = Industrial Automation and Control System(s)
 - collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation
- IACS used in ISA 62443 publications

Terminology

- 62443 series is a large collection of related standards and reports
 - Clause 3 of each publication is go-to source:
 - 3 Terms, definitions, abbreviated terms, acronyms, and conventions
 - 3.1 Terms and definitions
 - 3.2 Abbreviated terms and acronyms
 - 3.3 Conventions
- Master Glossary in development ISA-TR62443-1-2
 - Important that there be terminology consistency across the various documents

Recap

- ISA/IEC 62443 Series Overview
- Course Primary Sources
- ICS versus IACS
- Terminology and Concepts



Setting the Standard for Automation™

Section: Standards

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits



Setting the Standard for Automation™

Regulations and Standards

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits



Regulations

ISA
NIST
NEI ISO
ICPA-Japan FISMA
CFATS AGA FCC
NISS-D7-Saudi-Arabia
NESAA-UAE Local/State
FERC SEC DHS
DOE OSHA
NERC-CIP
NIS-Directive Regulation EU

Some are Mandatory

- Department of Homeland Security
 - 6 CFR part 27: Chemical Facility Anti-Terrorism Standards (CFATS)
- Department of Energy
 - Federal Energy Regulatory Commission (FERC)
 - 18 CFR Part 40, Order 822 (mandates NERC CIPs 002-014)
- Nuclear Regulatory Commission
 - 10 CFR 73.54 Cyber Security Rule (2014)
 - RG 5.71
- Above are North American focused
 - Do you know of any in your region?

Limitations

- Limited number enforced cyber and physical security regulations—no teeth
- National cyber security strategies may or may not be in place
- Public-private partnerships lacking
- Sector-specific cybersecurity plans may or may not exist
- Regulation compliance is mandatory while standards compliance is voluntary
- General agreement that no country or government can address cybersecurity risk in isolation

Standards

- Compliance and conformance is voluntary
 - Consensus driven
 - Collaborative approach preferred
- There is no requirement on anyone to use them unless....
 - If agreed to in a contract or referred to in regulation
 - Penalty, either civil or criminal, for not complying with them
- Courts may decide in the absence of relevant regulation
 - Non-compliance with a standard
 - Using a “what would a reasonable man on the street do” test
 - Sufficient grounds to determine liability
 - EUROPEAN COMMISSION Standards and Standardization Handbook



Standards Content

- Standards contain both normative and informative elements
- Normative elements are those parts that shall be complied with in order to demonstrate compliance with the standard
- Normative elements are indicated by the use of the words “shall” or “must”
- Informative elements provide clarification or additional information
- Informative elements may not contain requirements
 - The words “shall” and “must” are not used



Setting the Standard for Automation™

Evolving Security Standards and Practices

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Public-Private Collaboration
- Graphical Representation of NIST CSF Framework
- Monitor and Evaluate Applicable Legislation
- Global Frameworks
- Standards Development Organizations (SDO's)

Public-Private Collaboration

- USA Presidential Executive Order 13636 issued in 2013 to enhance the security and resilience of the Nation's critical infrastructure
- NIST Cybersecurity Framework Version 1.0 (CSF) published 2014
 - Version 1.1 published April 2018
- Public-private collaboration
- Framework is a guidance
- Basic, flexible, adaptable tool for managing and reducing cybersecurity risks



Public-Private Collaboration

- Framework Core
 - Set of desired cybersecurity activities and outcomes using common language that is easy to understand
 - Guides organizations in managing and reducing their cybersecurity risks
 - Complements an organization's existing cybersecurity and risk management processes
- Framework Implementation Tiers
 - Provide context on how an organization views cybersecurity risk management
 - Guide to consider the appropriate level of rigor for cybersecurity program
 - Used as a communication tool to discuss risk appetite, mission priority, and budget
- Framework Profile
 - Unique alignment of organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core
 - Primarily used to identify and prioritize opportunities for improving cybersecurity at an organization

Graphical Representation of NIST CSF Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Monitor and Evaluate Applicable Legislation

- Okay! So, what does this “framework” have to do with using the ISA/IEC 62443 Standards to Secure Your Control Systems?



Global Frameworks

- **Multi-lingual Framework**

إطار عمل لتحسين الأمان السيبراني للبنية
التحتية الحساسة

النسخة 1.1
المعهد الوطني للمعايير والتكنولوجيا (NIST)
16 أبريل، 2018

Arabic

Рамка за подобряване на киберсигурността
на критичната инфраструктура

Версия 1.1
Национален институт по стандарти и
технологии
16 април 2018 г.

Bulgarian

重要インフラのサイバーセキュリティを
改善するためのフレームワーク

Version 1.11.1 版
April 16, 2018 2018 年 4 月 16 日

Japanese

Ramy Usprawniania Cyberbezpieczeństwa
Krytycznej Infrastruktury

Wersja 1.0
Narodowy Instytut ds. Norm i Technologii
12 Lutego, 2014

Polish

GUIA DE APERFEIÇOAMENTO
DA SEGURANÇA CIBERNÉTICA
PARA INFRAESTRUTURA CRÍTICA
Versão 1.1

Portuguese

Marco para la mejora de la seguridad
cibernética en infraestructuras críticas

Versión 1.1
Instituto Nacional de Estándares y Tecnología
16 de abril de 2018

Spanish

Monitor and Evaluate Applicable Legislation

- Review, improve and maintain the CSMS
 - **Should** monitor and evaluate industry CSMS strategies
 - **Shall** monitor and evaluate applicable legislation relevant to cybersecurity
- NIST CSF Informative References consists of globally recognized standards for cybersecurity
- One of those standards are the ISA/IEC 62443's
- Framework can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity

Monitor and Evaluate Applicable Legislation

PROTECT (PR) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	<p>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes</p> <ul style="list-style-type: none"> · CIS CSC 1, 5, 15, 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
	<p>PR.AC-2: Physical access to assets is managed and protected</p> <ul style="list-style-type: none"> · COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
	<p>PR.AC-3: Remote access is managed</p> <ul style="list-style-type: none"> · CIS CSC 12 · COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
	<p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</p> <ul style="list-style-type: none"> · CIS CSC 3, 5, 12, 14, 15, 16, 18 · COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
	<p>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)</p> <ul style="list-style-type: none"> · CIS CSC 9, 14, 15, 18 · COBIT 5 DSS01.05, DSS05.02 · ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7

Source:

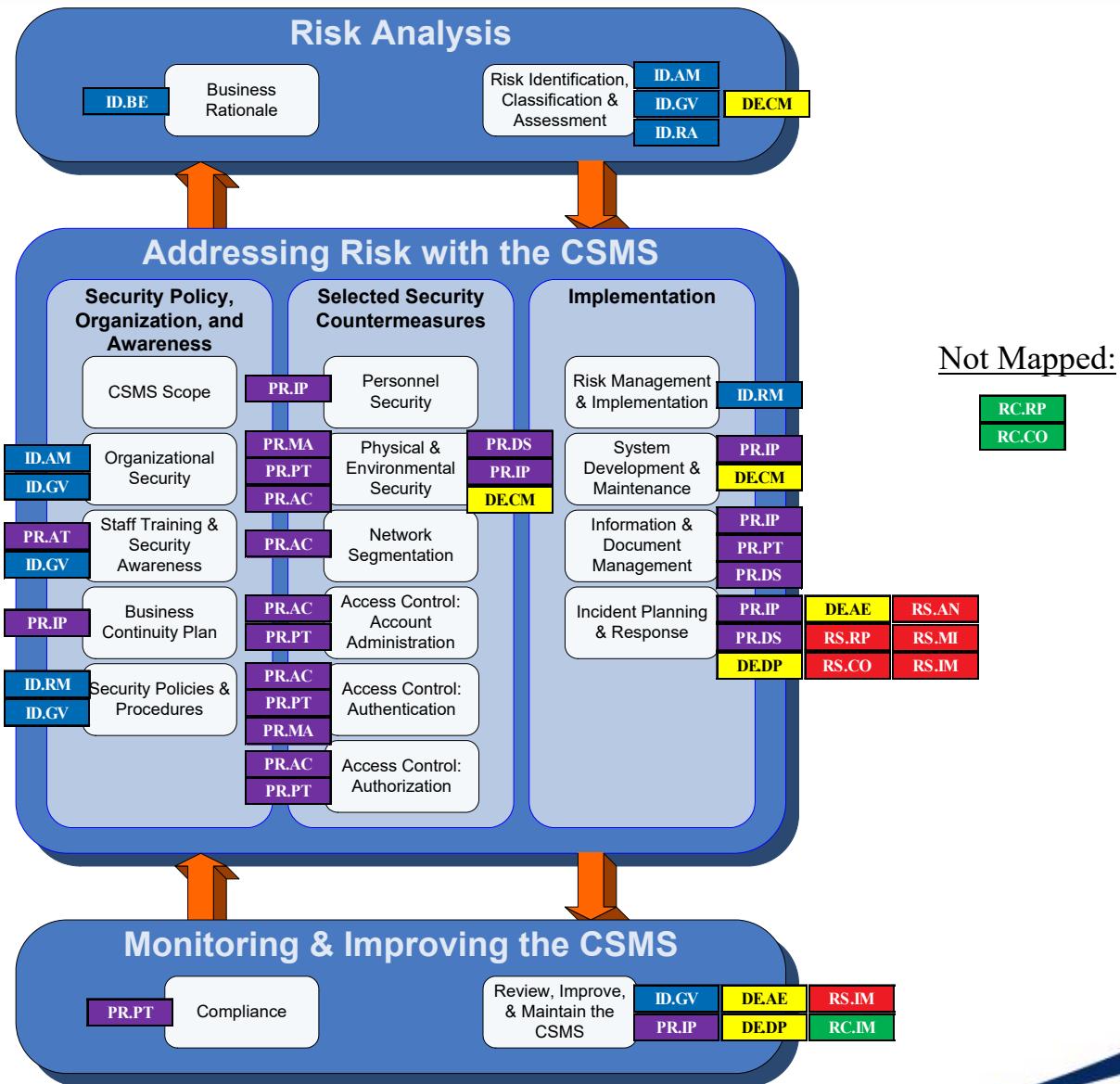
National Institute of Standards and Technology (NIST)

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1 National Institute of Standards and Technology, April 16, 2018

Mapping the NIST Framework Categories

ID.AM	Asset Management
ID.BE	Business Environment
ID.GV	Governance
ID.RA	Risk Assessment
ID.RM	Risk Management Strategy
ID.SC	Supply Chain Risk Management
PR.AC	Identity Management and Access Control
PR.AT	Awareness and Training
PR.DS	Data Security
PR.IP	Information Protection Processes and Procedures
PR.MA	Maintenance
PR.PT	Protective Technology
DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
RS.RP	Response Planning
RS.CO	Communications
RS.AN	Analysis
RS.MI	Mitigation
RS.IM	Improvements
RD.RP	Recovery Planning
RC.IM	Improvements
RC.CO	Communications



Global Frameworks

- Frameworks provide a common taxonomy and mechanism
 - Describe current cybersecurity posture
 - Describe target state for cybersecurity
 - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
 - Assess progress toward the target state
 - Communicate among internal and external stakeholders about cybersecurity risk

Global Frameworks

- ISO 27001:2013
 - Information technology -- Security techniques -- Information security management systems -- Requirements
- ISA 62443-2-1:2009
 - Requirements for an IACS security management system
- ISA 62443-3-3-2013
 - System security requirements and security levels
- COBIT 5
 - Control Objectives for Information and Related Technology (ISACA)
- CCS CSC
 - Council on Cyber Security Critical Security Controls
- NIST Special Publication 800-82 Revision 2
 - Guide to Industrial Control Systems (ICS) Security

Global Frameworks

- Standard ending with 2008 does not necessarily mean the standard is out of date.
 - ISO/IEC reviews and confirms the standards and posts the last review and confirmation on their site
- ISO/IEC 15408:2009
 - Information Technology -- Security Techniques -- Evaluation Criteria for IT Security (Common Criteria)
 - Last reviewed and confirmed in 2015 and is still current
- ISO/IEC 21827:2008
 - Information Technology -- Security Techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)
 - Last reviewed and confirmed in 2020 and is still current

Standards Development Organizations (SDO's)



- International Electrotechnical Commission (IEC)
 - IEC 62443 series of standards (equivalent to ISA 99)
- International Society of Automation (ISA)
 - ISA99, Industrial Automation and Control System (IACS) Security
- National Institute of Standards and Technology (NIST)
 - SP800-82 Guide to Industrial Control Systems (ICS) Security
- EU Cybersecurity Dashboard
 - EU Cybersecurity Maturity Dashboard 2015
- UAE National Electronic Security Authority
 - UAE Information Assurance Standards (UAE IAS)



NESA UAE

Standards Development Organizations (SDO's)



- Petroleum Sector
 - American Petroleum Institute



- Chemical Sector
 - American Chemistry Council



- Water & Wastewater Sector
 - American Water Works Association (AWWA)



- Electric Sector
 - North American Electric Reliability Council (NERC)
 - NERC CIP



Recap

- Public-Private Collaboration
- Graphical Representation of NIST CSF Framework
- Monitor and Evaluate Applicable Legislation
- Global Frameworks
- Standards Development Organizations (SDO's)



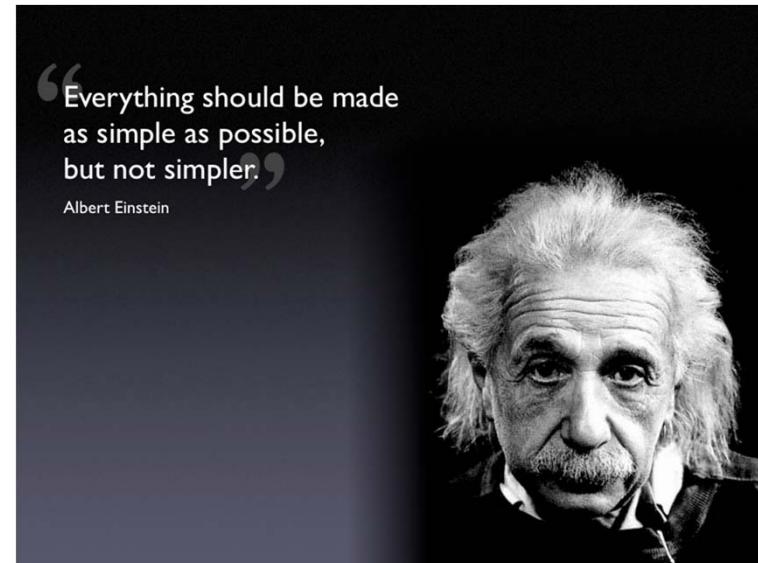
Setting the Standard for Automation™

ISA99 Committee and the 62443 Standards

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Section Topics

- Committee Overview
- Committee Processes
- The 62443 Series



Committee Overview



Committee Overview

The International Society of Automation (ISA) Committee on Security for Industrial Automation & Control Systems (ISA99)

- Established 2002 with a handful of members
- Now over 900 volunteer members, representing companies across all sectors such as, but not limited to:
 - Chemical Processing
 - Petroleum Refining
 - Food and Beverage
 - Energy
 - Pharmaceuticals
 - Water
 - Manufacturing
- Global membership emphasized
 - Global reach and scope consistent with “International” Society of Automation

Committee Scope

“... industrial automation and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- environmental protection
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on entity, local, state, or national security”

Committee Processes



Collaboration

- Standards Development Organization (SDO)



- ISA/IEC 62443 is a series of standards developed by two SDO's
 - ISA99 develops ANSI/ISA-62443
 - IEC then develops IEC 62443
- ISA99 charged with developing the majority of the standards
 - The intent is for essentially the same standards to be issued by IEC
 - There may be a delay as IEC processes the standard
- Working closely in consultation with
 - ISO/IEC to be consistent with ISO/IEC 2700x series

Collaborating on Related Topics

- Process Safety (ISA84, IEC TC65)
- Wireless Communications (ISA100)
- Certification (ISCI and ISASecure®)
- Communications & Advocacy (Automation Federation)
- Industrial Control Systems Joint Working Group (ICSJWG)
- Security Framework (NIST)
- International Reach (IEC/ISO)



Active Work Groups

- WG 1 – Security Technologies
- WG 2 – Security Program Definition and Operation
- WG 3 – Concepts and Models
- WG 4 – Technical Requirements
- WG 5 – Committee Leadership
- WG 6 – Patch Management
- WG 7 – Safety and Security (Joint WG with ISA 84)
- WG 8 – Communication and Outreach
- WG 9 – IoT Implications
- WG 10 – Life Cycle and Use Cases
- WG 11 – IACS Security for the Nuclear Sector

Committee Participation

- NOT necessary to be a member of ISA in order to be a **member** of an ISA committee.
- Participation can take any of several forms...
 - Being a member of a work or task group that is developing or revising one or more work products (e.g., standards, technical reports)
 - Contributing to a "supporting" work activity, such as communications and outreach.
 - Reviewing and offering comments or feedback on draft work products
 - Assisting the committee in establishing joint working relationships with other committees and organizations

Membership Types

Type	Description
Information	<ul style="list-style-type: none">• Default classification.• Participates in one or more work or task groups• Comments on draft documents
Voting	<ul style="list-style-type: none">• Maximum of one per company• Nominated based on contributions• Approved by existing voting members• Expected to vote on draft documents
Alternate	<ul style="list-style-type: none">• Paired with a voting member• Able to vote if the primary voting member not available



Our Purpose is Standards

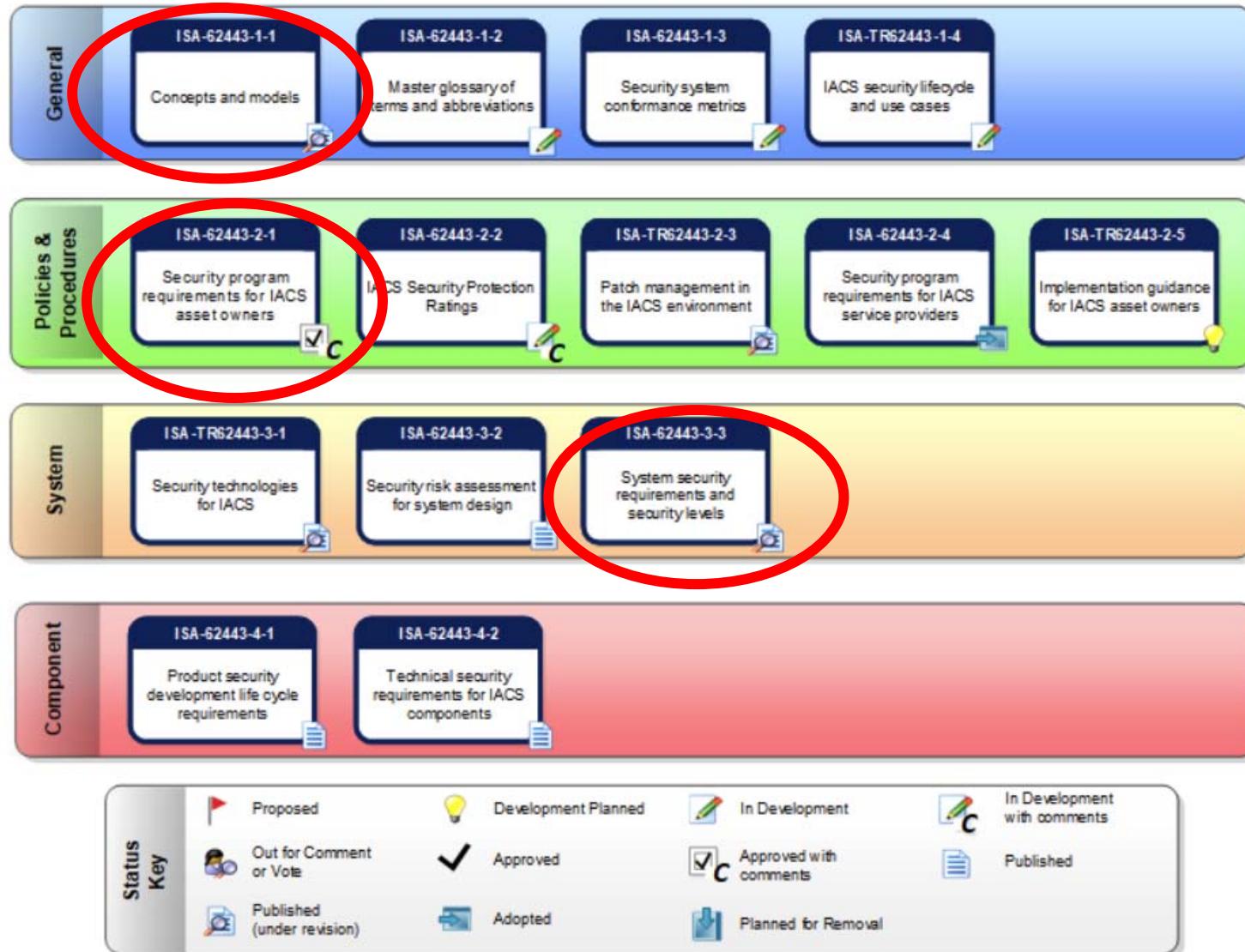
- It can take **several years** to create a standard
 - Content development
 - Reviews and comments
 - Votes
 - Publication
- Always looking for new participants
 - Subject Matter Experts (SME) in their area
 - Volunteering their time and efforts
- Join a standards committee link
 - <https://www.isa.org/forms/join-a-standards-committee/>
 - Get on mailing list
 - Access to SharePoint site
 - Not required to be an ISA member



The 62443 Series



Series Overview



Work Product Organization (Groups or Categories)



- First or top **General** group contains standards and reports that are general in nature
- Second group **Policies & Procedures** addresses the people and process aspects of an effective security program
- Third group **System** focus is on the technology related aspects of security
- Fourth group **Component** focuses on specific security related technical requirements of products and components

Work Product Highlights

- 14 Publications
 - 10 Standards
 - 4 Technical Reports (TR)
- Close to 400 normative requirements
 - Approximately 150 requirement enhancements
 - Published standards over 900 pages and counting
- Future direction of ISA 99 committee
 - Turning from defining what must be done
 - To providing direction on how it should be accomplished
 - Growing interest in measuring effectiveness and conformance

Introductory Clauses

CONTENTS

PREFACE	3
FOREWORD	10
0 Introduction	11
0.1 Overview.....	11
0.2 Purpose and intended audience	12
0.3 Usage within other parts of the ISA-62443 series	12
1 Scope	15
2 Normative references	15
3 Terms, definitions, abbreviated terms, acronyms, and conventions	15
3.1 Terms and definitions	15
3.2 Abbreviated terms and acronyms	21
3.3 Conventions	23
4 Common control system security constraints	24
4.1 Overview	24

ISA99 committee

- Committee web page <https://www.isa.org/ISA99/>
- Join here: <https://www.isa.org/forms/join-a-standards-committee/>
- Twitter: @ISA99Chair
- Committee Co-Chairs: isa99chair@gmail.com
 - Eric Cosman
 - Jim Gilsinn
- Managing Director
 - Joe Weiss
- ISA Staff Contact
 - Eliana Brazda ebrazda@isa.org



Section Recap

- ✓ Committee Overview
- ✓ Committee Processes
- ✓ The 62443 Series



Setting the Standard for Automation™

Section

Intro to the IACS Cybersecurity Lifecycle

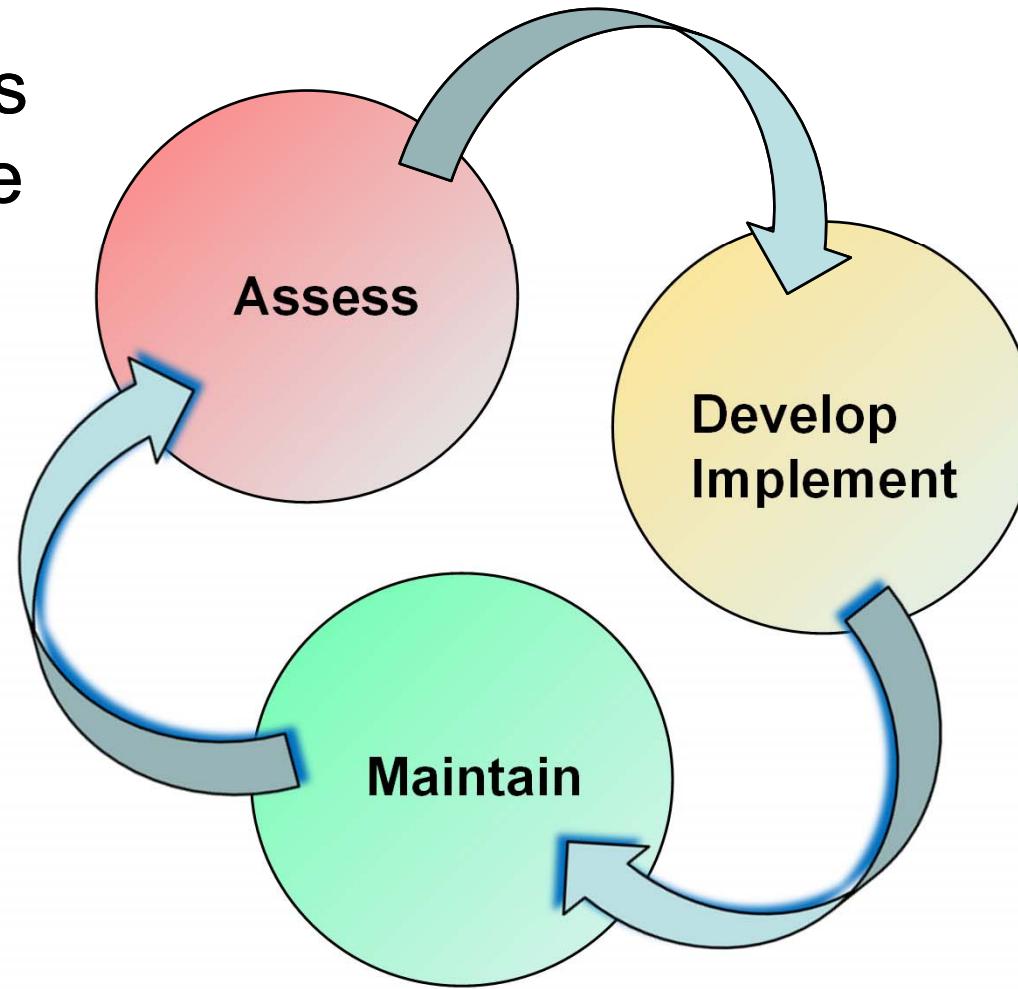
Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- IACS Cybersecurity Lifecycle
 - Assess
 - Develop & Implement
 - Maintain
- Continuous Process

Intro to the IACS Cyber Security Life Cycle

Assess
Phase



Develop &
Implement
Phase

Maintain Phase

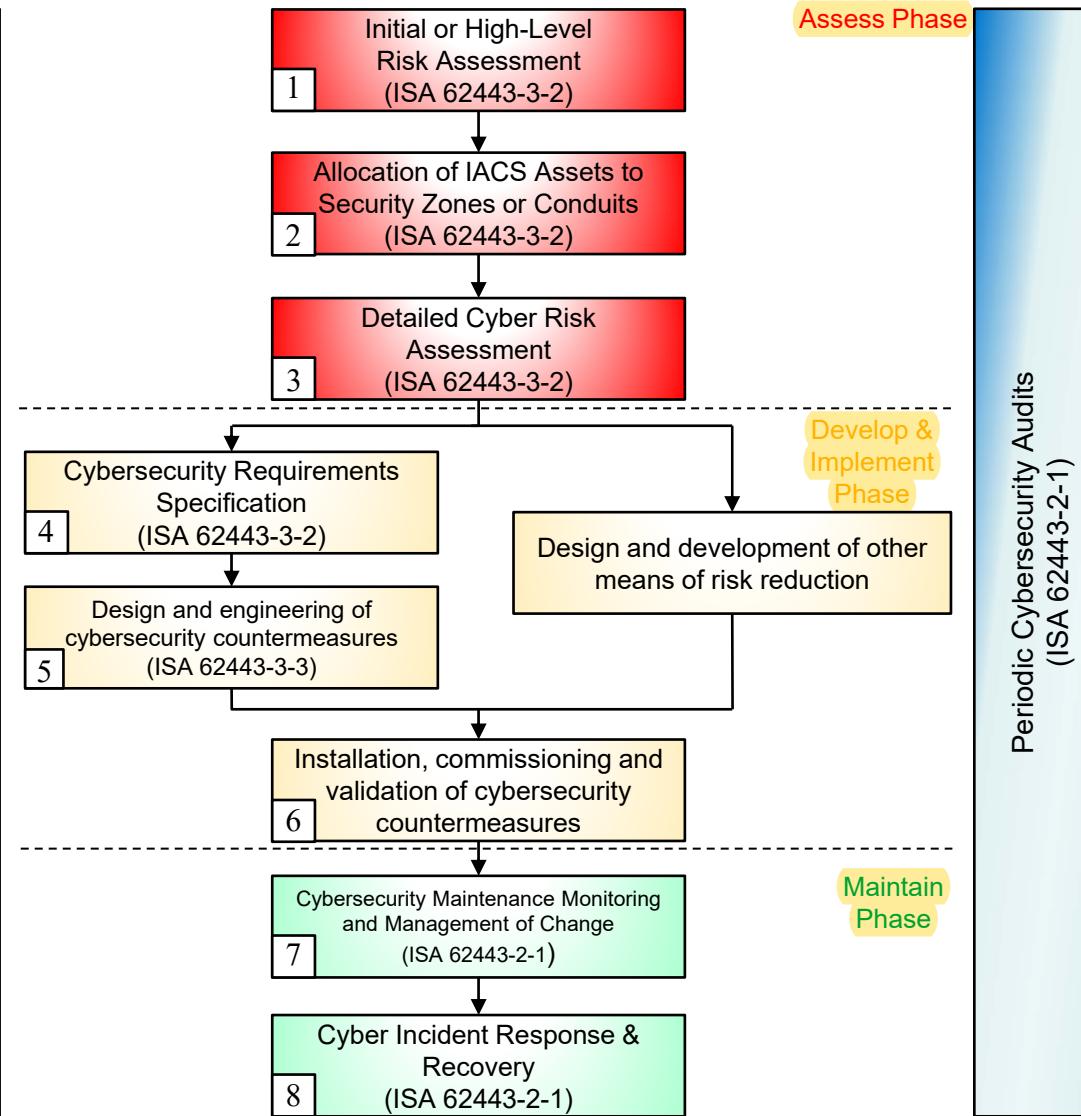
Intro to the IACS Cyber Security Life Cycle

- Assess phase--a zone is assigned a Target Security Level (SL-T)
- Develop & Implement phase--countermeasures are implemented to meet the Target Security Level (SL-T)
 - Achieved Security Level (SL-A) depends on various factors
- Maintain phase--ensures the Achieved Security Level (SL-A) is better than or equal to the Target Security Level (SL-T)
 - Countermeasures are audited and/or tested and upgraded if necessary, to reach and maintain Achieved Security Level (SL-A)

IACS Cybersecurity Lifecycle

Continuous Processes

Cyber Security Management System: Policies, Procedures, Training & Awareness
(ISA 62443-2-1)



Assess Phase

Section 1

Develop &
Implement Phase

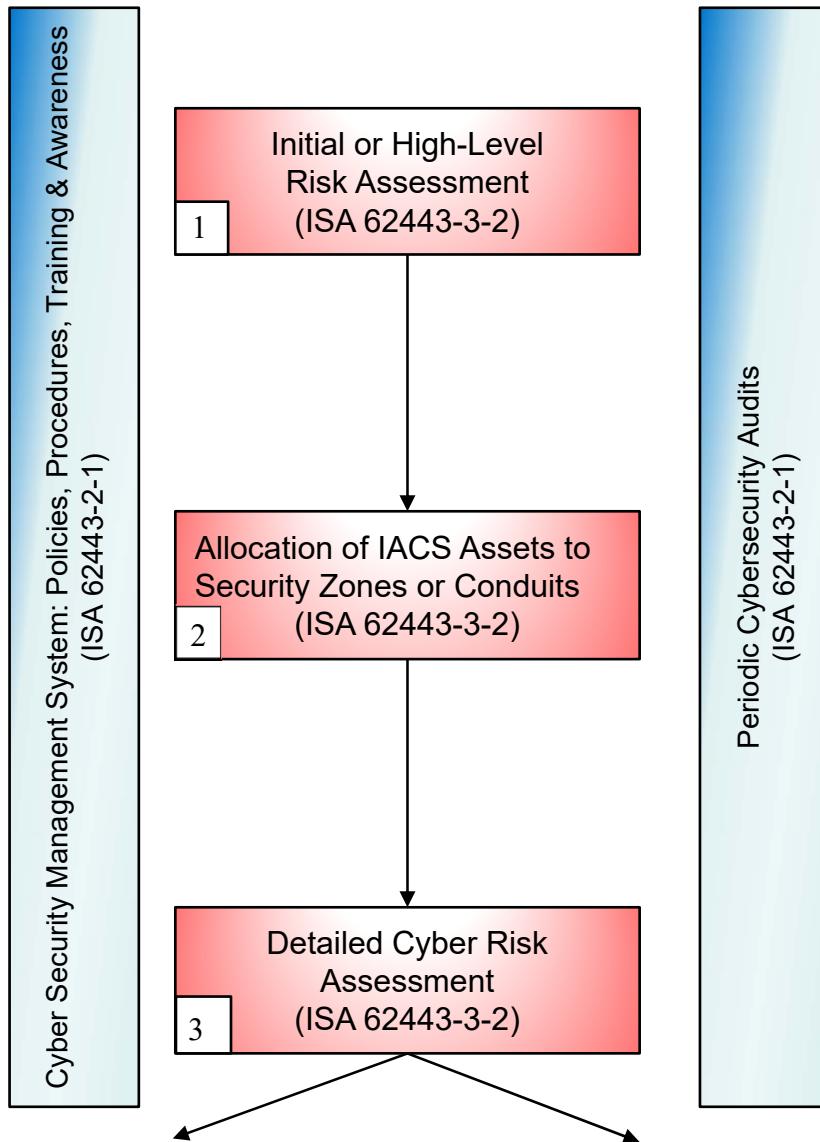
Section 2

Maintain Phase

Section 3

IACS Cybersecurity Lifecycle

Continuous Processes



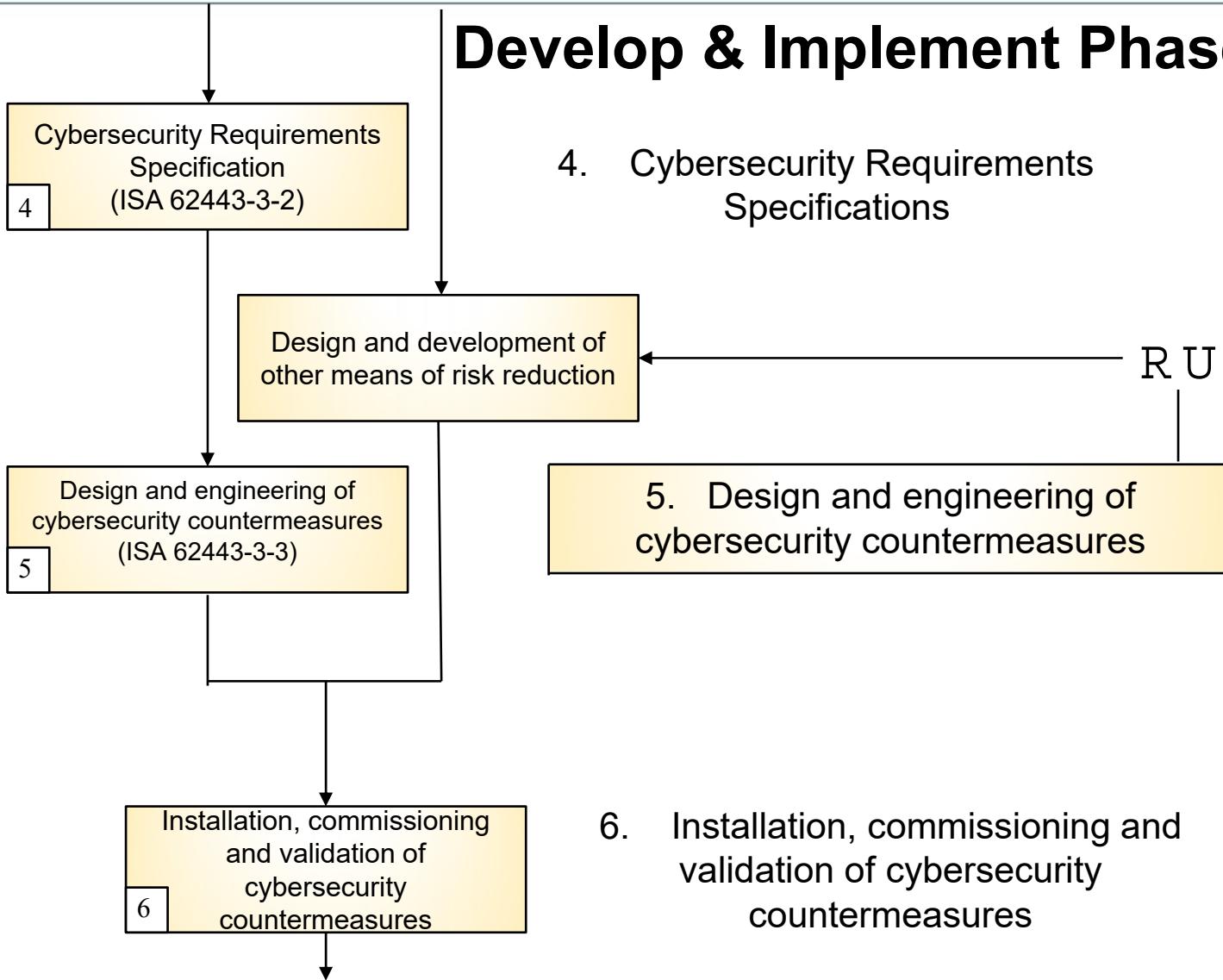
Assess Phase

1. Initial or High-Level Cyber Risk Assessment
2. Allocation of IACS Assets to Security Zones or Conduits
3. Detail Cyber Risk Assessment

IACS Cybersecurity Lifecycle

Continuous Processes

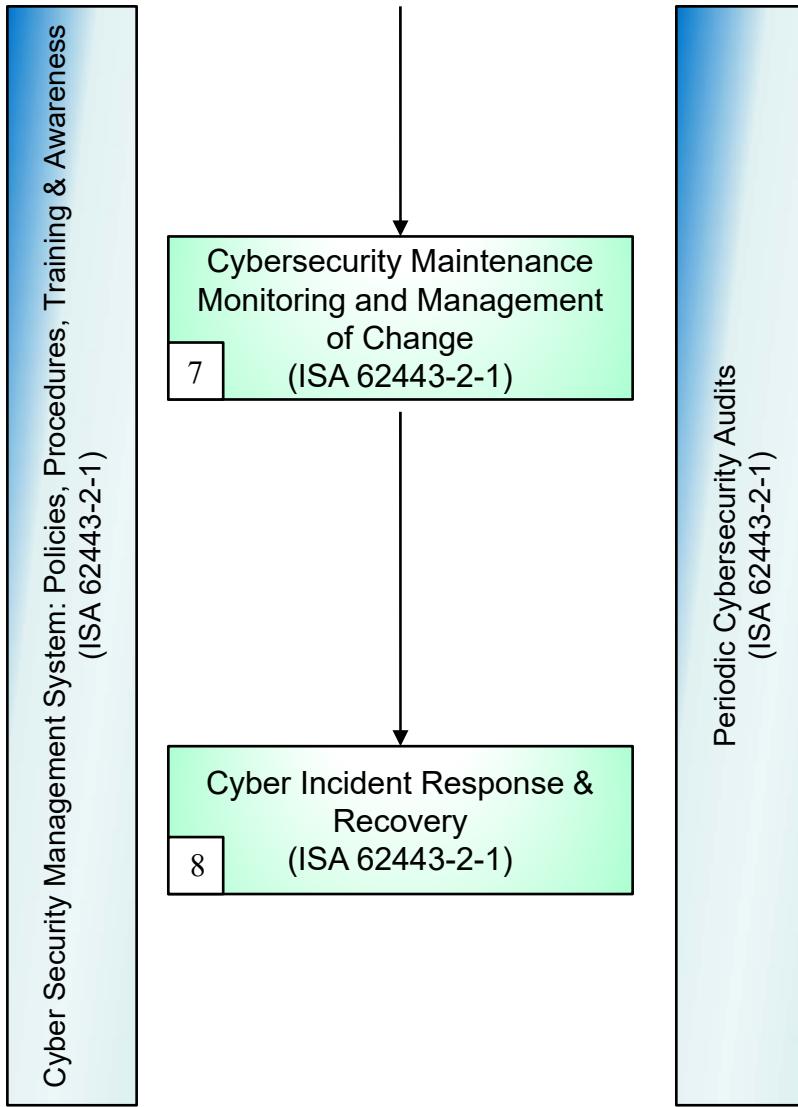
Cyber Security Management System: Policies, Procedures, Training & Awareness
(ISA 62443-2-1)



Periodic Cybersecurity Audits
(ISA 62443-2-1)

IACS Cybersecurity Lifecycle

Continuous Processes



Maintain Phase

7. Cybersecurity Maintenance, Monitoring and Management of Change

8. Cyber Incident Response & Recovery

Continuous Processes

Cyber Security Management System: Policies, Procedures,
Training & Awareness
(ISA 62443-2-1)

Periodic Cybersecurity Audits
(ISA 62443-2-1)

Recap

- IACS Cybersecurity Lifecycle
- Assess
- Develop & Implement
- Maintain
- Continuous Process



Week 3

Week 3



Setting the Standard for Automation™

Establishing an Industrial Automation and Control Systems Security Program

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

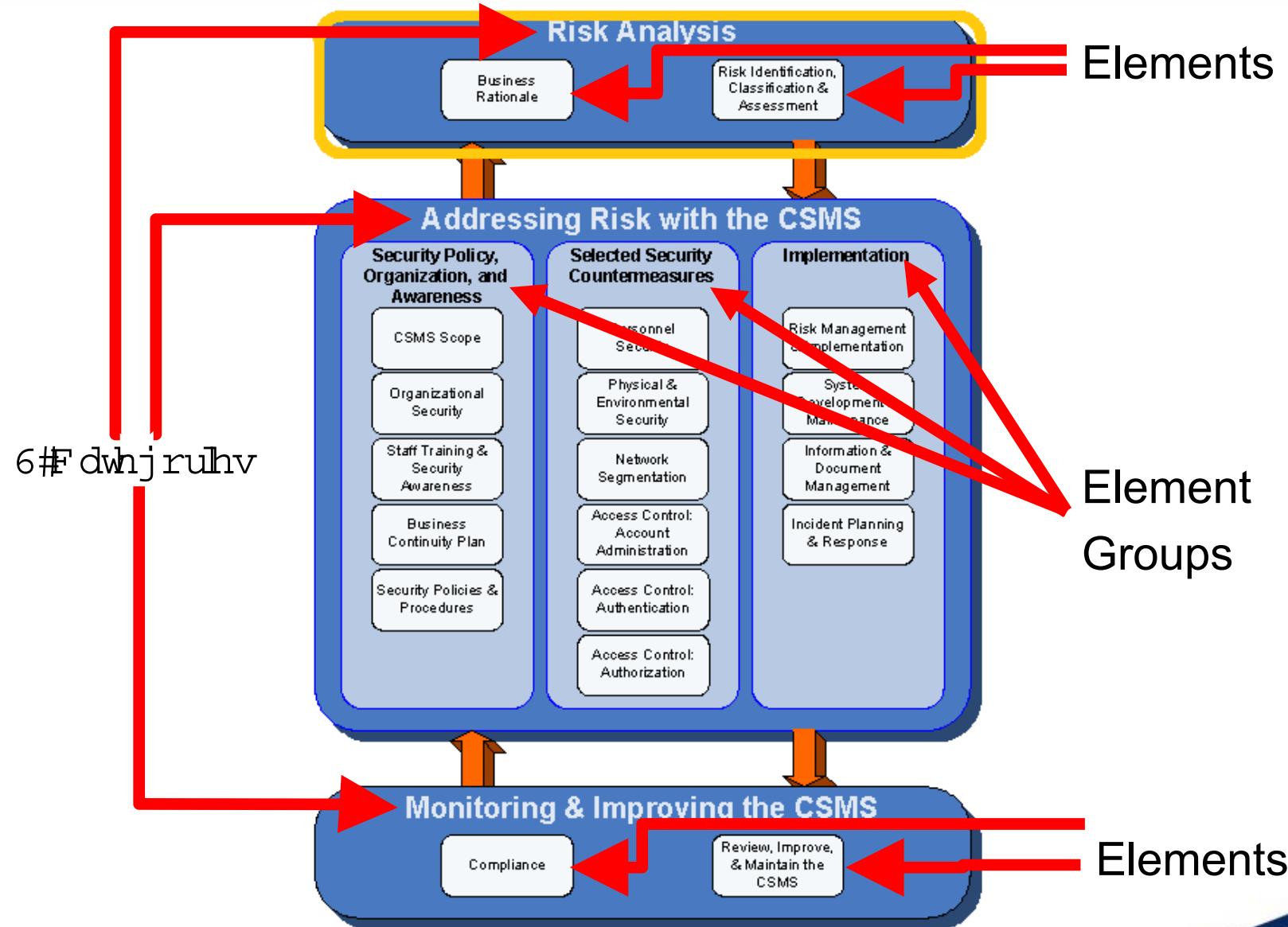
Introduction

- Policies & Procedures
- Cyber Security Management System (CSMS)
- Process to Develop a CSMS
- CSMS Six Top Level Activities

Series Overview



Cyber Security Management System (CSMS)

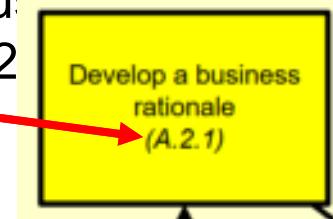


Cyber Security Management System (CSMS)

- Open up ANSI/ISA-62443-2-1, pg 22.
 - Normative Clause 4 Elements of a cyber security management system begins here
- Figure 1, pg 23 is the graphical view of elements of a cyber security management system
- Annex A, pg 47 is informative guidance for developing the elements of a CSMS
- Annex B, pg 155 is informative Process to develop a CSMS

Cyber Security Management System (CSMS)

- Clauses, subclauses, elements, sub-elements, Annexes can be overwhelming
 - Walk through “Element: Business rationale” and see how they tie together
 - See ANSI/ISA-62443-2-1
- Subclause 4.2.2, “Element: Business rationale”, pg 24
- Annex A (informative),
 - Guidance for developing the elements of a CSMS
 - “Elements: business rationale” (A.2.2), pg 49
- Annex B (informative),
 - Process to develop a CSMS “Develop a Business rationale”, pg 157
 - Refers to Annex A (A.2.1), should be (A.2.2)



Cyber Security Management System (CSMS)

- Three main categories
 - Risk Analysis
 - Addressing Risk with the CSMS
 - Monitoring and improving the CSMS
- Risk Analysis has two elements
 - Background information that feeds into many of the other elements
 - Business rationale
 - Risk identification, classification and assessment
- Addressing Risk with the CSMS has three element groups
 - Security policy, organization and awareness
 - Selected security countermeasures
 - Implementation
 - ANSI/ISA-62443-2-1, pg 23, Figure 1

Cyber Security Management System (CSMS)

- Monitoring and improving the CSMS has two elements
 - Conformance
 - Review, improve and maintain the CSMS
- Frequent mistake with cyber security is to initially address smaller pieces
 - Engineering approach is to break the problem into smaller pieces
 - Must address the entire set of IACS
 - Integrate physical, HSE and cyber security risk assessment results
 - Policies, procedures, practices and personnel come into play
 - May require organizational cultural change
- Security is balance of risk versus cost
 - All situations different
 - ANSI/ISA-62443-2-1, pg 11

Cyber Security Management System (CSMS)

- IACS risk may have an unrecoverable impact
 - Business risk may only be temporary financial setback
 - Control HSE Impacts may be permanent
- Cookbook approach using mandatory security practices
 - Overly restrictive and costly
 - Insufficient to realistically address the risk
 - Not a one-size-fits-all set of security practices exists
 - ANSI/ISA-62443-2-1, pg 11

Process to Develop a CSMS

- This section will focus on the ordering and iterative nature of activities associated with developing a CSMS
- Developing a Cyber Security Management System (CSMS) is a journey that may take months or years to achieve
- ISA 62443-2-1 contains detailed comprehensive integrated CSMS elements
 - Clause 4 contains the elements of a CSMS
 - Annex A contains guidance for developing the elements of a CSMS
 - Elements or sub-elements of this standard are referenced for researching more information about a particular topic
 - “Search or Find” is a useful tool for researching a topic
 - Guidance should be tailored to the organization’s requirements

Process to Develop a CSMS

- ISA 62443-2-1 contains a combination of SHOULD, MAY and SHALL requirements
 - Clause 4 elements state what shall and should be included in the CSMS
 - Guidance provided in this course is an example
 - User of the standard must read the requirements carefully
 - Policies & procedures need to be tailored to fit within the organization
- Elements of a CSMS list the following:
 - Objective
 - Description
 - Rationale
 - Requirements
- ANSI/ISA-62443-2-1, subclause 3.3, pg 21

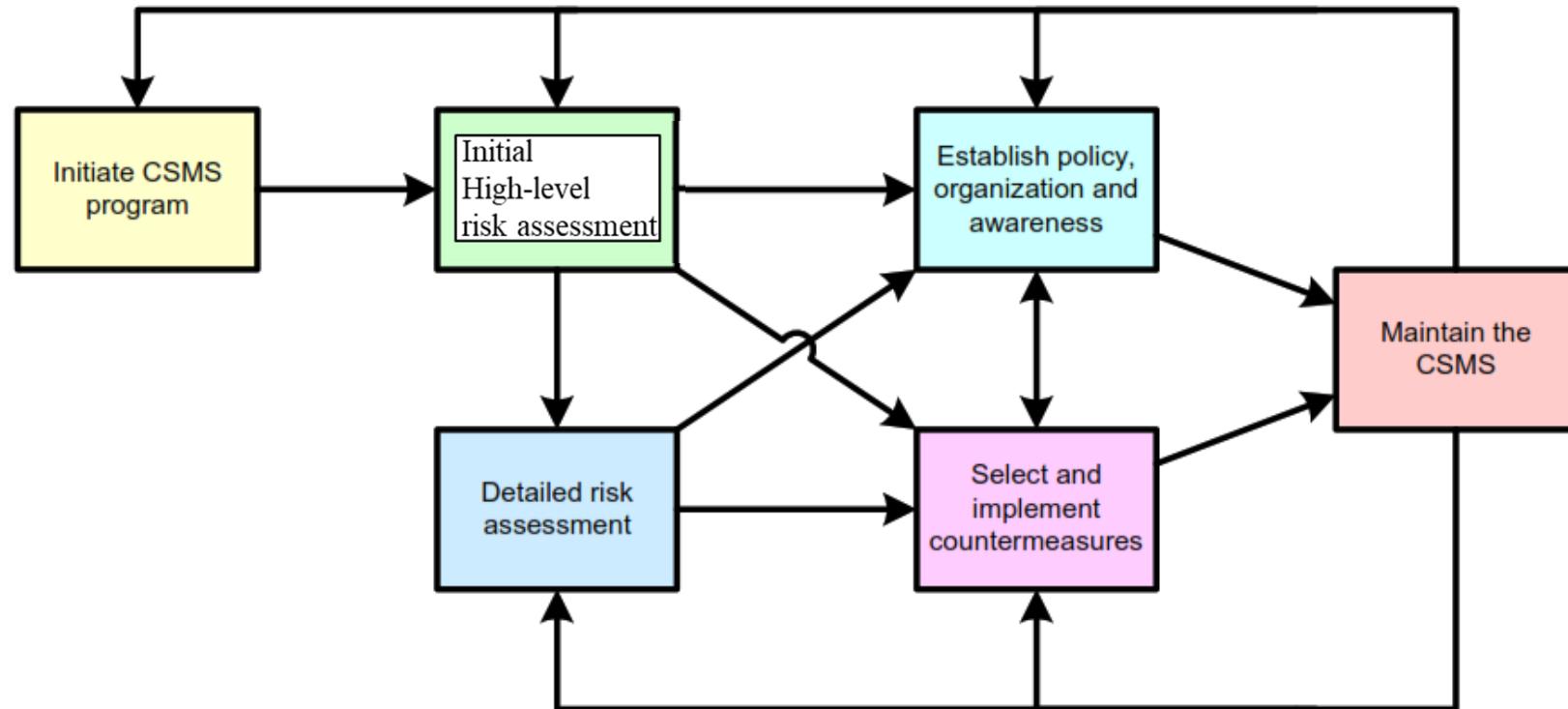


Setting the Standard for Automation™

CSMS Boils Down to Six Top Level Activities

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

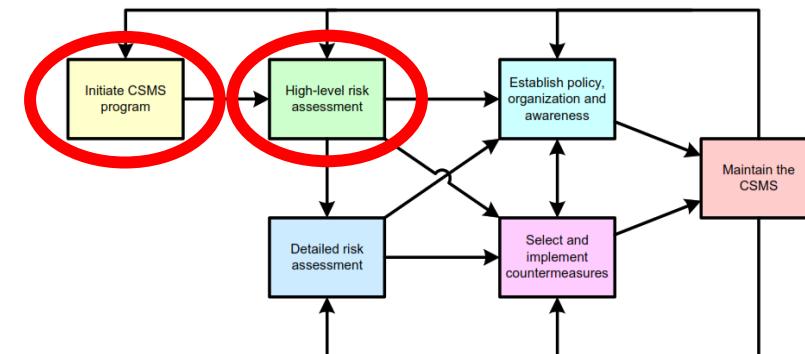
Description of the Process



ANSI/ISA-62443-2-1, Annex B, Figure B.1, pg 155

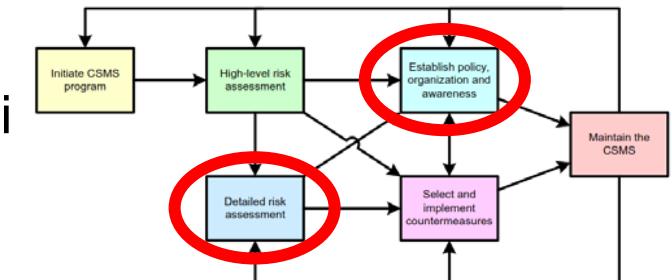
Description of the Process

- **Initiate CSMS**
 - Establish purpose
 - Organizational support
 - Resources
 - Scope
 - Initial scope may be smaller than desired
 - Can grow as the program matures
- **Initial/High-level risk assessment**
 - Drives the content of CSMS
 - Threats
 - Likelihood
 - Vulnerabilities
 - Consequences



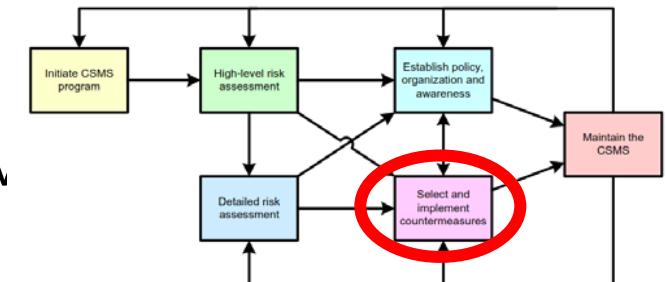
Description of the Process

- Address risk assessment at a high level
 - Resources needlessly expended if not kept high level
 - Overall higher-level risk context must be established
- Detailed risk assessment
 - Detailed technical assessment
 - Focus on vulnerabilities identified at high level
- Establish policy, organization and awareness
 - Driven by initial/high-level and detailed risk assessment results
 - Creation of policies and procedures
 - Assignment of organizational responsibilities
 - Planning and execution of training



Description of the Process

- Select and implement countermeasures
 - Defines and implements cyber security defenses
 - Technical
 - Non-technical
- Coordinated approach
 - High-level and low-level decisions driven by risk assessment results
 - Establish policy, organization and awareness
 - Select and implement countermeasures
 - Training
 - Essential to make countermeasure effective

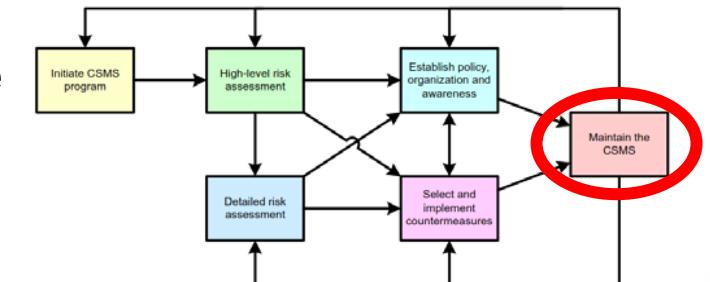


Description of the Process

- Maintain the CSMS

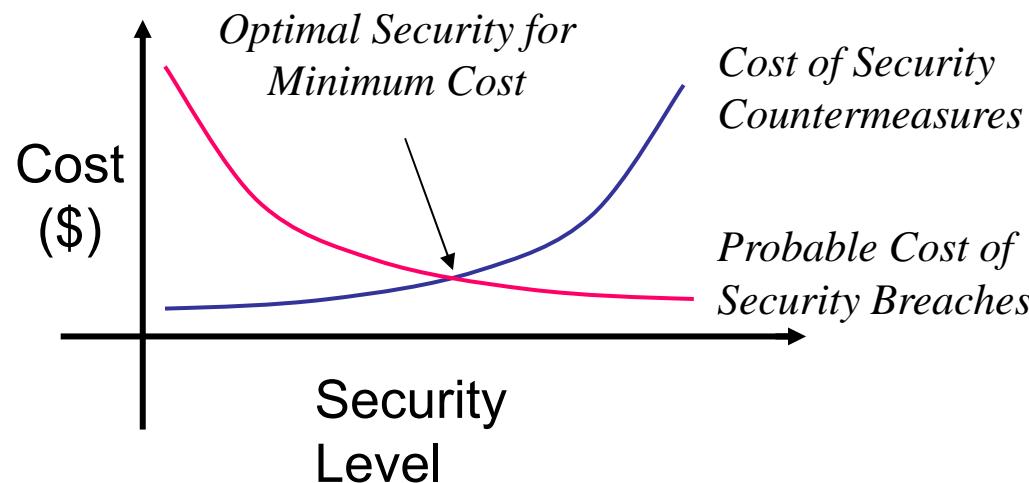


- Is organization maturing in its CSMS activities?
- Does organization conform to policies and procedures?
- Are cyber security goals met effectively?
- Do the goals need to change in light of internal or external events?
- Is a review of initial/high-level or detailed risk assessment required?
- Are there improvements identified and implemented?
- Are there training enhancements to make?
- Has enthusiasm and support waned?
- Have other priorities pushed CSMS to the

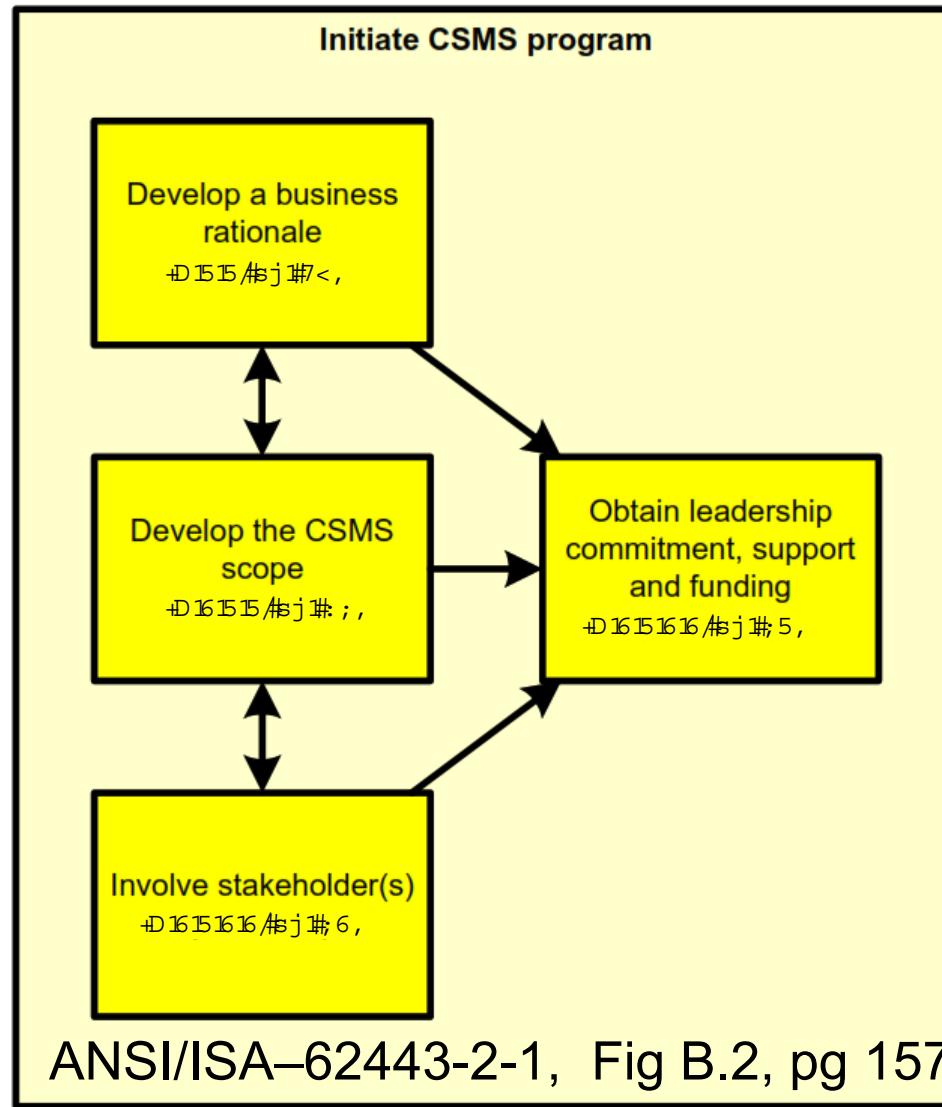


Description of the Process

- Fine balance
- We can't afford perfect security
- Risk reduction is balanced against the cost of security measures to mitigate the risk



Initiate the CSMS Program



ANSI/ISA-62443-2-1, Fig B.2, pg 157

Initiate the CSMS Program

- Obtain leadership commitment, support, and funding
 - Effective organizational framework has to start at the top
- First develop a business rationale that will justify the program to management
 - What particular business consequences will senior management find the most compelling?
- Second develop a proposed scope for the program
- Use rationale and scope to identify stakeholders up front
 - Identify integration points with support and service providers
- Stakeholders join effort to engage management for a commitment

ANSI/ISA-62443-2-1, Annex B.3, pg157

Initiate the CSMS Program

- Stakeholders should be cross-functional in nature:
 - Process control staff implementing/supporting IACS devices
 - Operations staff responsible for making the product
 - Safety management staff responsible for health, safety, and environmental incident prevention
 - IT responsible for network and server design and support.
 - Physical security staff
 - IT Security staff responsible for IT security
 - Additional resources may be needed
 - legal
 - human resources
 - customer support roles
 - order fulfillment roles
 - vendors
 - third party contractors

ANSI/ISA-62443-2-1, Annex B.3, pg157

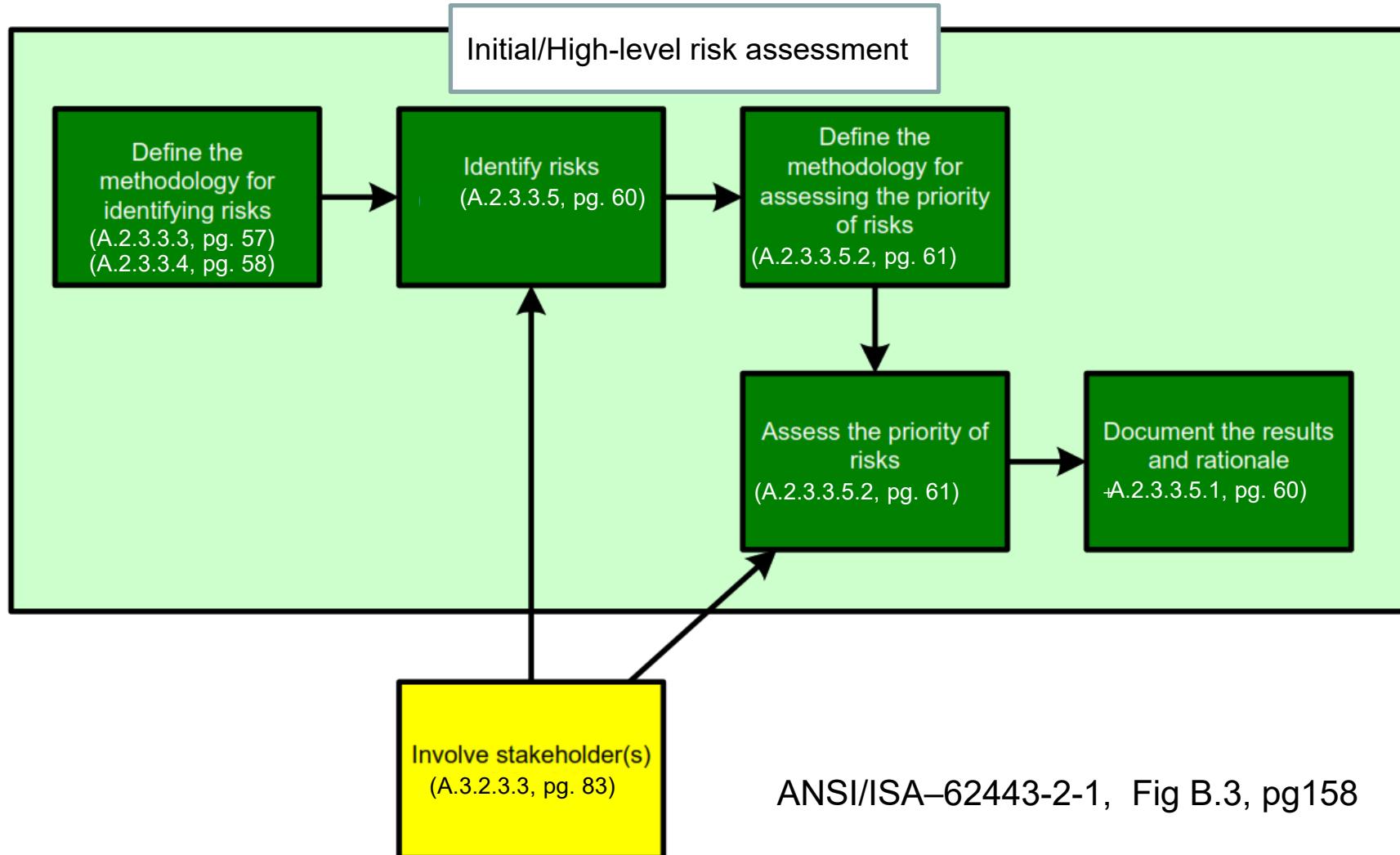
Initiate the CSMS Program

- Common pitfall is to initiate without a high-level rationale
 - Must relate cyber security to the mission of the organization
- What is your organization's mission statement?
- Why are we doing all of this “cyber security” work” in relation to the mission statement?
- Return on Investment (ROI) difficult to quantify when it comes to cyber
- What are we supporting?
- Cyber security requires organizational resources
 - Business rationale must be established in the beginning
 - Program may start with good intentions
 - Momentum quickly lost to competing demands



ANSI/ISA-62443-2-1, Annex B.3, pg157

Initial/High-level Risk Assessment



Initial/High-level Risk Assessment

- Involves selecting methodologies for identifying and prioritizing risks and then executing those methodologies
- It is important to define these methodologies up front so that they will provide structure for the rest of the risk assessment.
- Important to involve the stakeholders identified during Initiate step
- Common pitfall is to immediately jump into detailed risk assessment
 - Easy to do, especially with technical stakeholders
 - Avoid the “shiny object syndrome”

ANSI/ISA-62443-2-1, Annex B.4, pg158

ANSI/ISA-62443-3-2, 4.3, ZCR 2, pg 19

Initial/High-level Risk Assessment

- Documenting the results and rationale is important
 - Documentation establishes baseline
 - Will be found invaluable when the risk assessment needs to be confirmed or updated in the future
- Common pitfall documentation is insufficient or never completed
 - There needs to be a champion appointed for good follow up



ANSI/ISA-62443-2-1, Annex B.4, pg158

Initial/High-level Risk Assessment

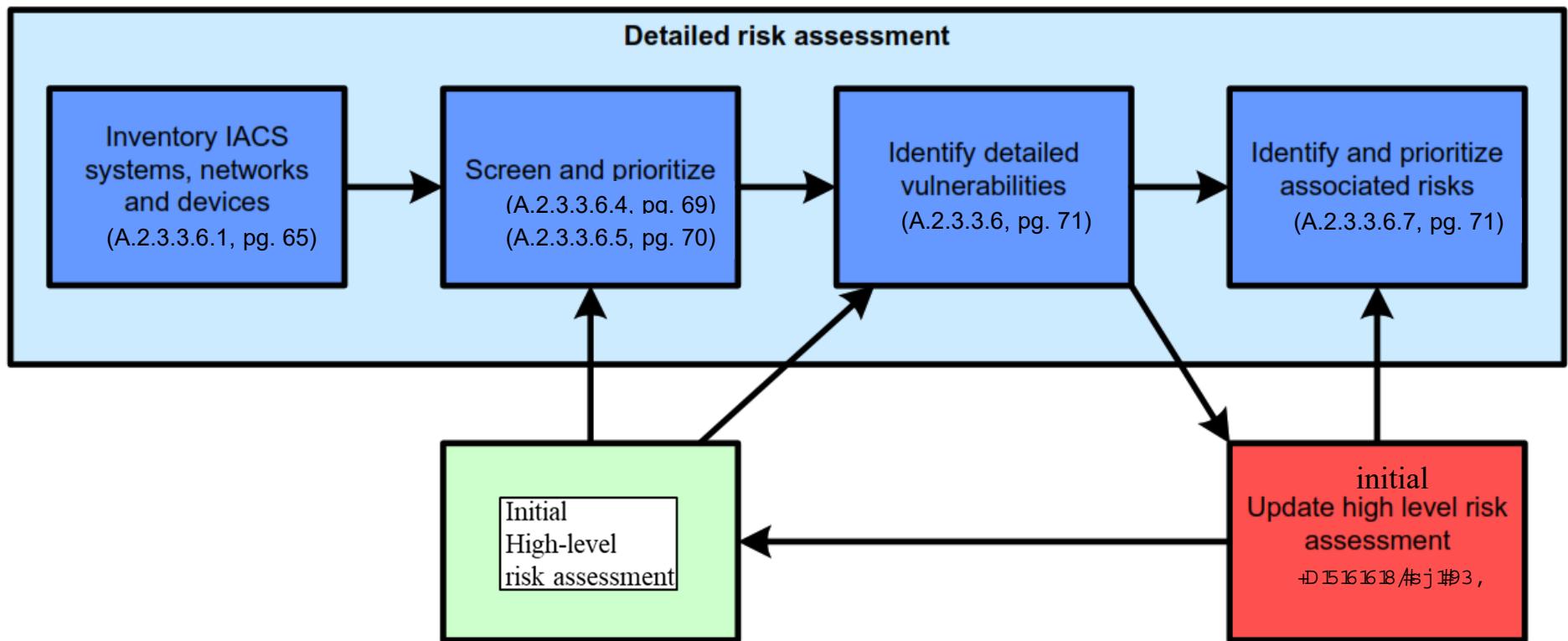
- Thresholds for tolerable risk are established by executive management
- Often communicated via a Risk Matrix



		Consequence category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

ANSI/ISA-62443-2-1, Table A.3, pg 64

Detailed Risk Assessment



ANSI/ISA-62443-2-1, Fig B.4, pg159

Detailed Risk Assessment

- Provide greater detail by first taking an inventory of specific IACS systems, networks, and devices
- Resource or time constraints may not allow detailed examination of all of these assets
 - Use threats, consequences, and types of vulnerabilities identified in the initial/high-level risk assessment to assist in setting priorities to focus on
 - Help desk or maintenance history can help determine focus
- Detailed vulnerabilities guided by the initial/high-level risk assessment vulnerabilities identified
 - Not limited to those high-level vulnerabilities

ANSI/ISA-62443-2-1, Annex B.5, pg158

Detailed Risk Assessment

- Detailed vulnerability assessment may uncover
 - New threats
 - New Likelihoods
 - New consequences
 - New risks
 - ANSI/ISA-62443-2-1, Annex B.5, pg 158
- Interrelationship with physical and environmental security measures
 - Do physical and environmental security measures complement cyber?
 - ANSI/ISA-62443-2-1, Subclause 4.3.3.3, pg 33
 - Are appropriate entry controls provided?
 - Annex A, subclause A.3.3.3, pg 97
 - Is there protection against environmental damage?

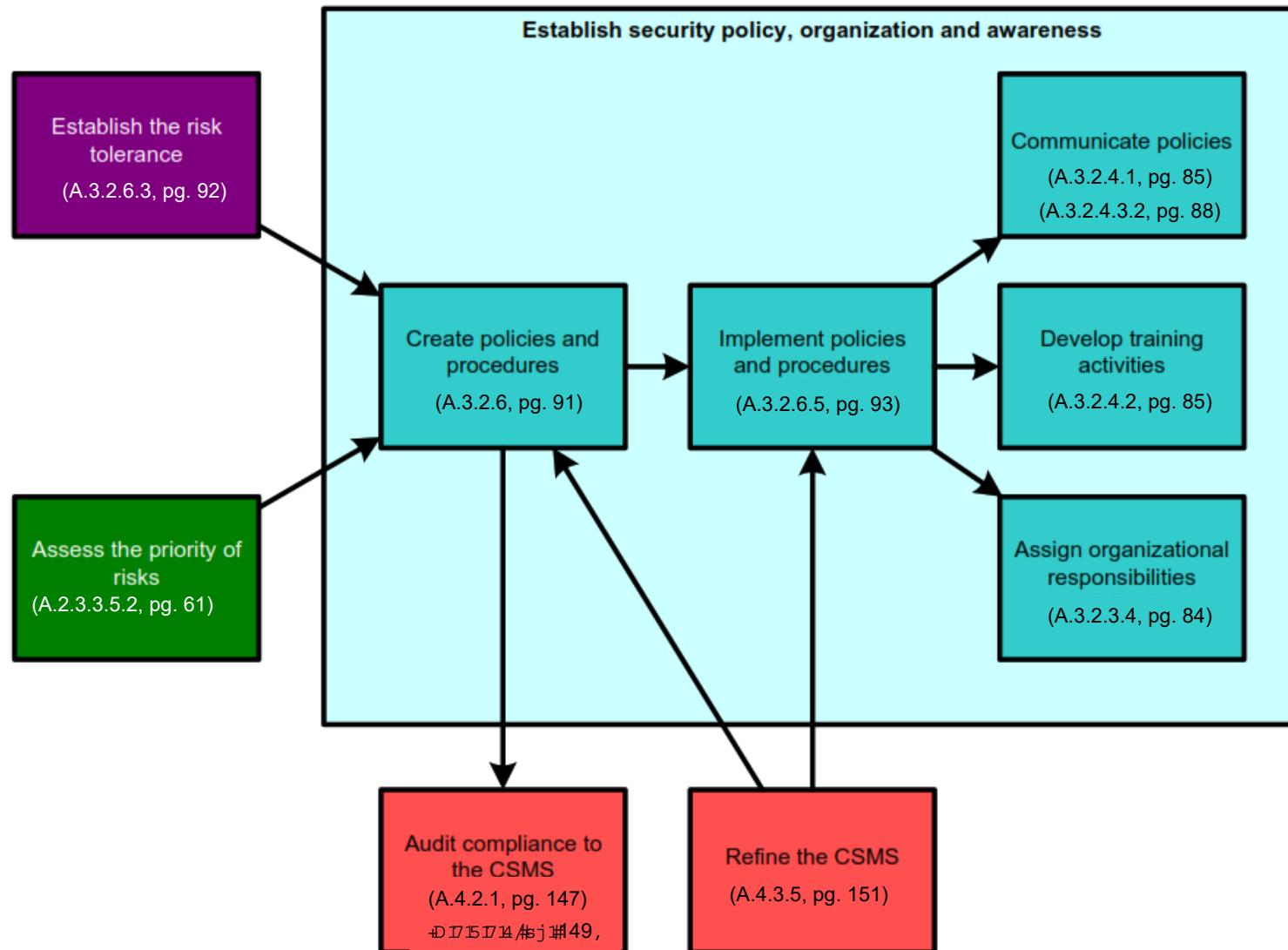
Detailed Risk Assessment

- May have to go back and update initial/high-level risk assessment
 - Identified vulnerabilities correctly matched up with specific risk
- Prioritize consistent with method used in initial/high-level risk assessment
- Common pitfall is failure to communicate before, during & after the risk assessment
 - Organizational lack of communication an issue
 - Lack of effective communications
 - Business unit silos



ANSI/ISA-62443-2-1, Annex B.5, pg158

Establish Policy, Organization & Awareness



ANSI/ISA-62443-2-1, Fig B.5, pg160

Establish Policy, Organization & Awareness

- Implementation of policy involves
 - Creating appropriate and cost-effective policy
 - Communicating the policy to the organization
 - Training personnel in the organization
 - Assigning responsibility for adherence to the policy
- Policies and procedures can impact any activity in the CSMS
 - Countermeasures used drive specific system and maintenance process implementation
 - All of these have a cost
 - Determining when risk is to be re-assessed

ANSI/ISA-62443-2-1, Annex B.6, pg 159-160

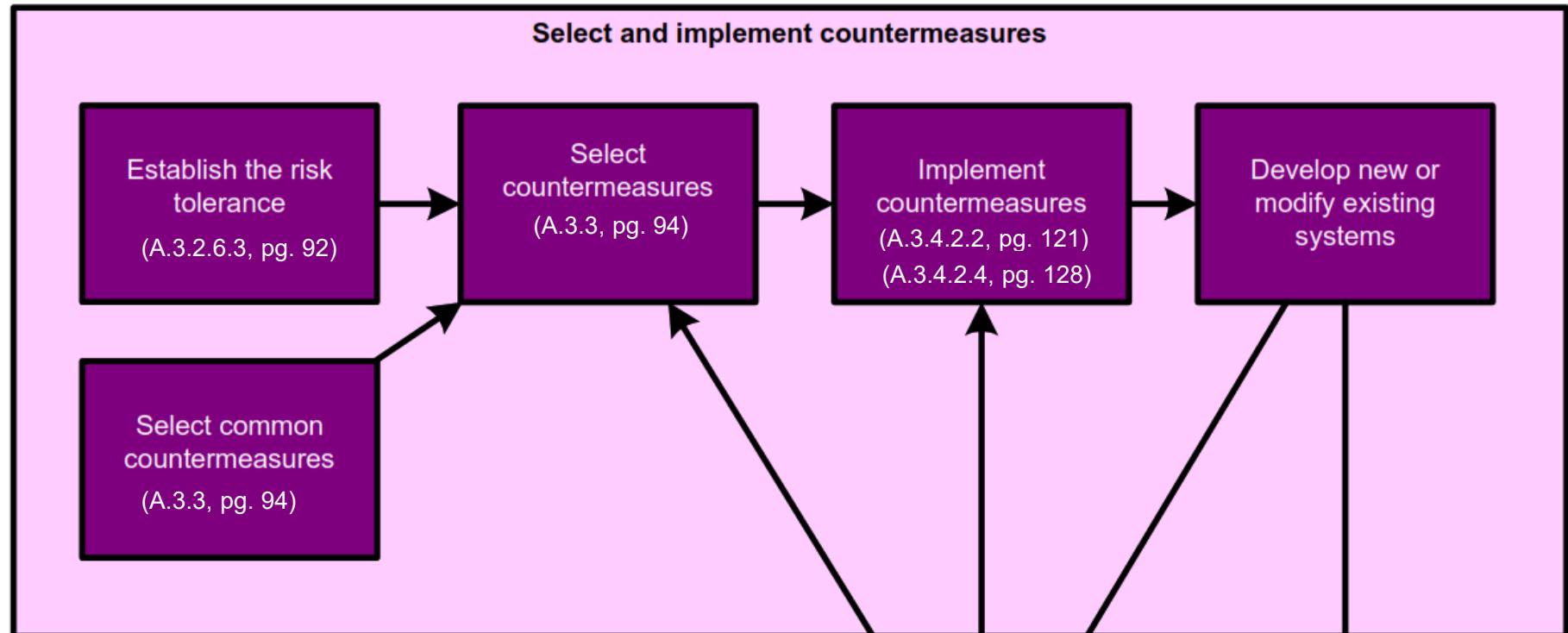
Training and Assignment of Responsibilities

- Develop training and assign organization responsibilities
- Over time all organizational responsibilities or training topics related to CSMS should be evaluated
- Part of the iterative process
- Lists may get smaller as program matures



ANSI/ISA-62443-2-1, Fig B.6, pg 161-162

Select and Implement Countermeasures



ANSI/ISA-62443-2-1, Fig B.7, pg 162

Select and Implement Countermeasures

- Selection of countermeasures is the technical process of risk management
- Driven by:
 - Organization's risk tolerance
 - Pre-selected common countermeasures
 - Results of initial/high-level risk assessment
 - Results of detailed risk assessment

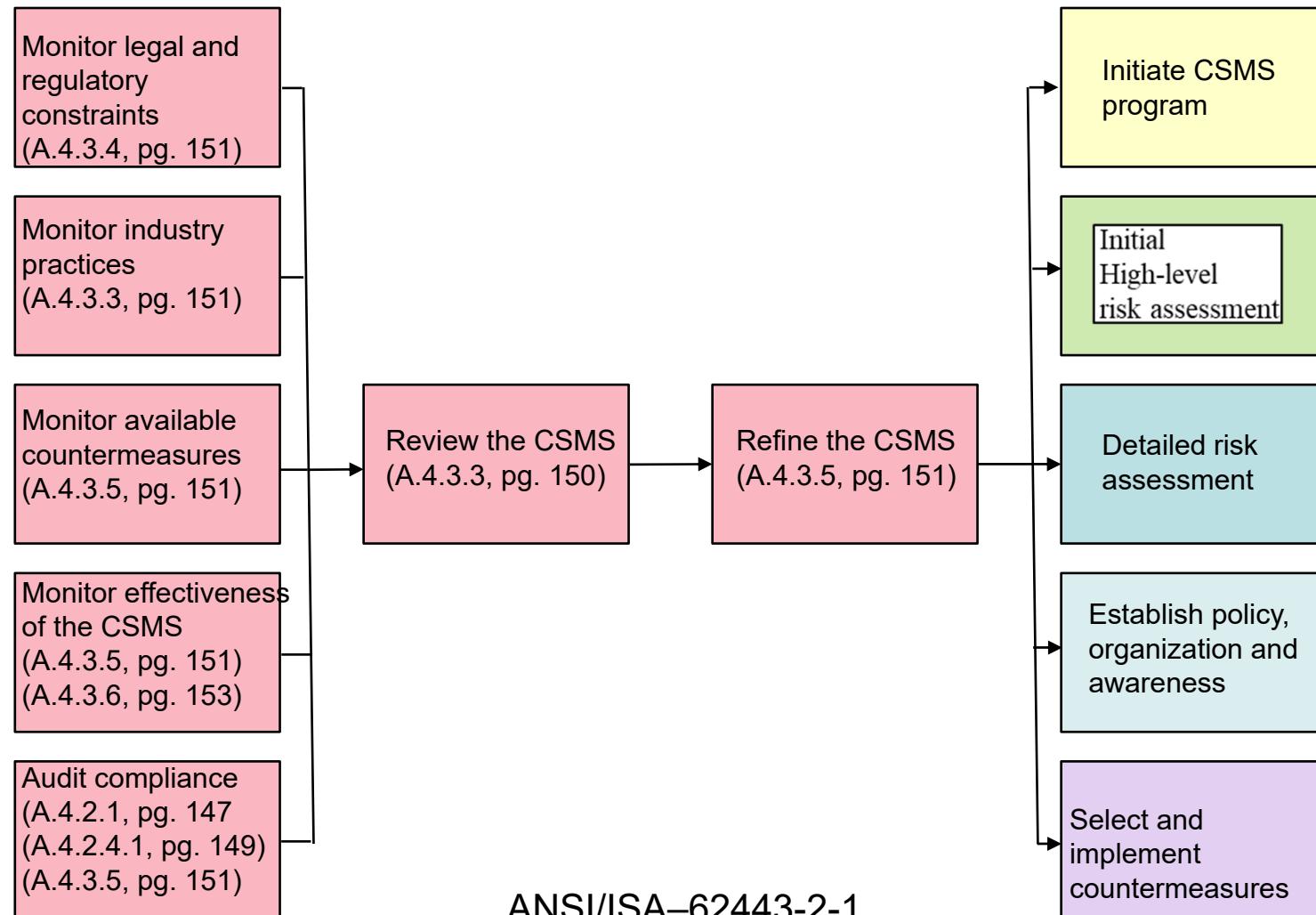
ANSI/ISA-62443-2-1, Annex B.7, pg 162

Select and Implement Countermeasures

- Implementing new or modifying an existing system
 - Update initial/high-level risk assessment
 - Update detailed risk assessment
 - Countermeasures selected based on updated risk info
- Development or modification of systems requires
 - Update to business continuity plan
 - Incident response plan
- Common pitfall is that required stakeholders are not invited
 - Collaborative processes within organization are immature
 - Walls and barriers within the organization exist

ANSI/ISA-62443-2-1, Annex B.7, pg 162

Maintain the CSMS



ANSI/ISA-62443-2-1,
Fig B.8, pg 163

Maintain the CSMS

- Maintenance over time requires review and refinement of the CSMS based on review results
- An unscheduled activity such as a security incident exposing unknown risk may trigger a review
- Major inputs to this review
 - Results from effectiveness measures
 - Audits of conformance from internal monitoring
- Other inputs to review
 - External information about available countermeasures
 - Evolving industry practices
 - New or changed laws, regulations and mandates

Maintain the CSMS

- Review identifies
 - Deficiencies
 - Proposes improvements
- Use review results to create refinements
- Refinements may take the form of
 - New countermeasures
 - Improvements in countermeasure implementation
 - Modify policies and procedures
 - Improve their implementation
 - Review of poor conformance

Maintain the CSMS

- Results may point out the need for improvements in
 - Training activities
 - Organizational responsibilities
- Common pitfall is lack of management support thus no resources allocated
 - Cyber Security fatigue
 - Overwhelmed by number of issues
- ANSI/ISA-62443-2-1
 - Annex A, A4.2, pg 147-149
 - Annex B, B.8, pg 162-163



Recap

- Policies & Procedures
- Cyber Security Management System (CSMS)
- Process to Develop a CSMS
- CSMS Six Top Level Activities



Week 4

Week 4



Setting the Standard for Automation™

Networking Basics: L1-L3

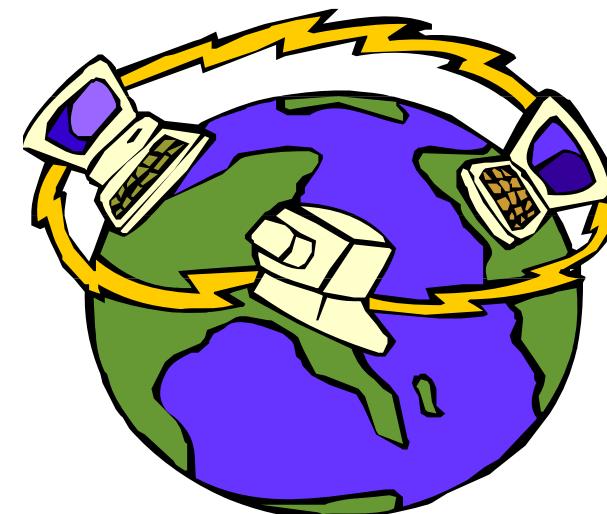
Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Network types
- ISO OSI/Reference Model
- Layers 1 - 3
- IPv4 Addressing/ARP Protocol
- IPv6 Addressing/ARP Protocol

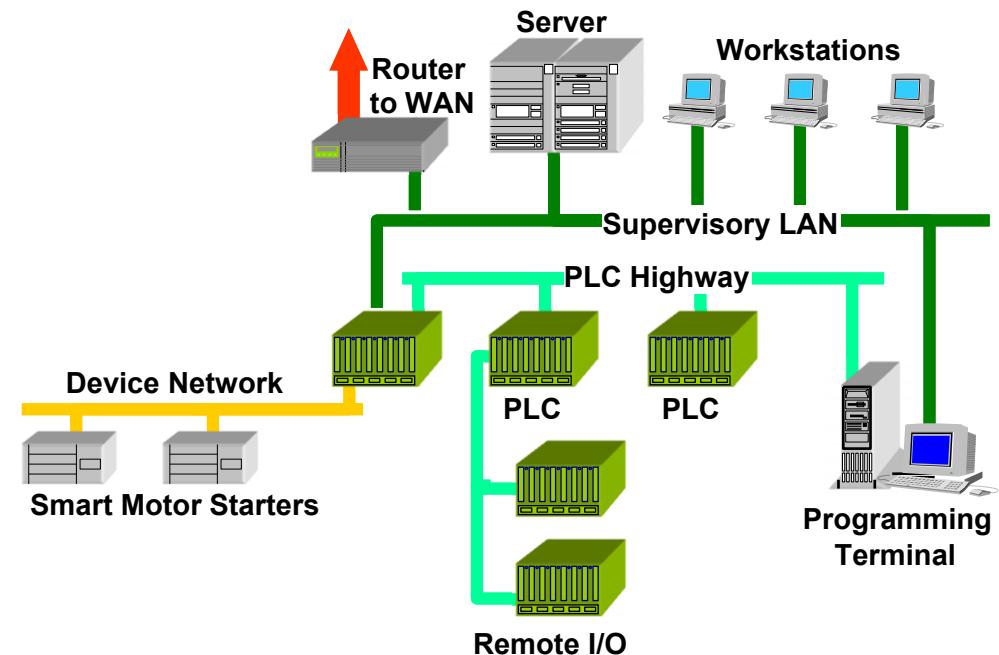
Network Types - WAN

- A wide area network (WAN) is a communications system that covers a large geographic area.
- Traditionally joined mainframes distributed across the country or world. Now usually joins two or more LANs.
- Often uses public networks, such as the telephone system. Can also use private lines, leased lines or satellites.
- Three WAN strategies:
 - Enterprise WANs
 - Carrier Managed WANs
 - Internet



Network Types - LAN

- A local area network (LAN) is a communications system that covers a limited distance (usually under 10 km), generally within a single facility.
- LAN technologies are used in the factory under many names:
 - Supervisory Networks
 - DCS Highways
 - PLC Highways
 - Fieldbuses
 - Device Networks



ISO OSI/Reference Model



Layer 1: Physical Layer

- The physical protocols define the physics of getting a message between devices like:

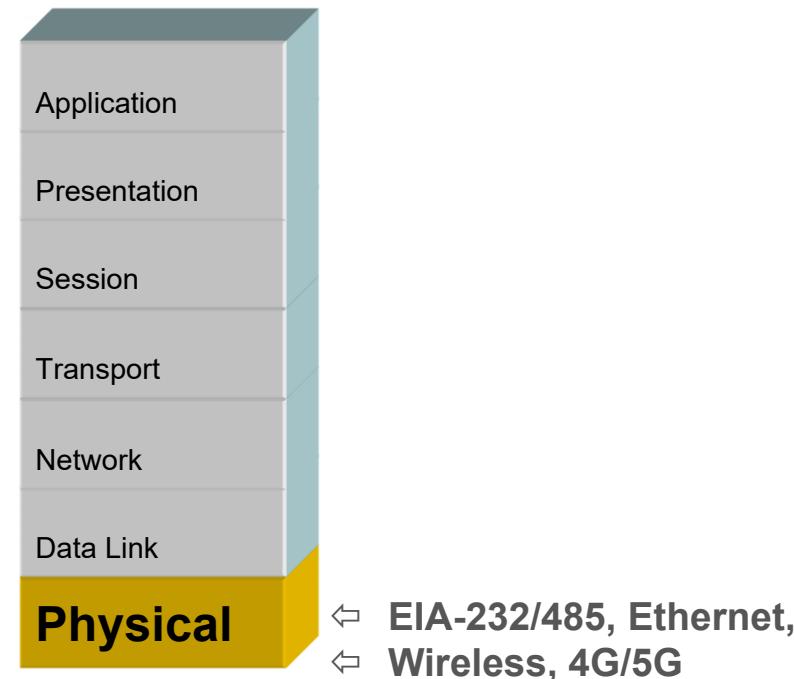
- Frequencies
 - Modulation

- Voltages

- Connectors

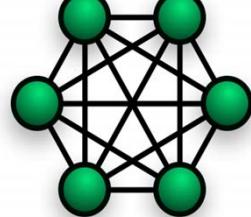
- Topologies
 - Cables

- This is the most important area in terms of both troubleshooting and operations

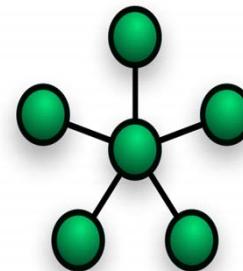


Layer 1: Physical Layer

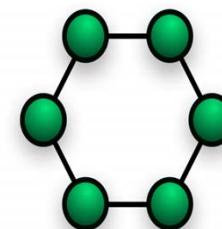
- Network Topologies



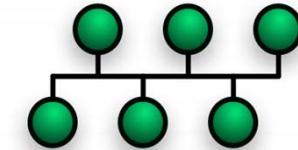
Mesh



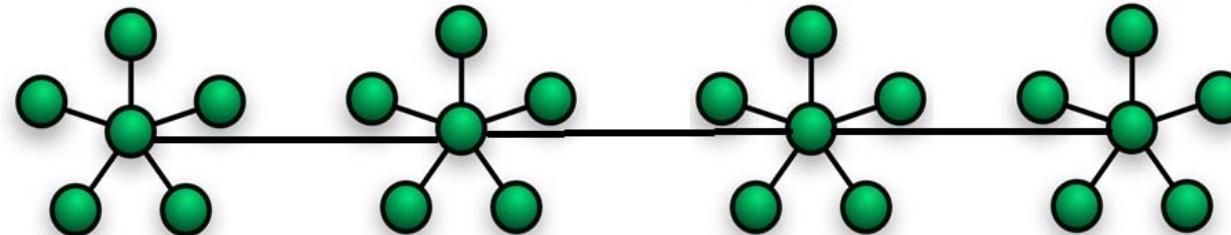
Star / Hub and
Spoke



Ring



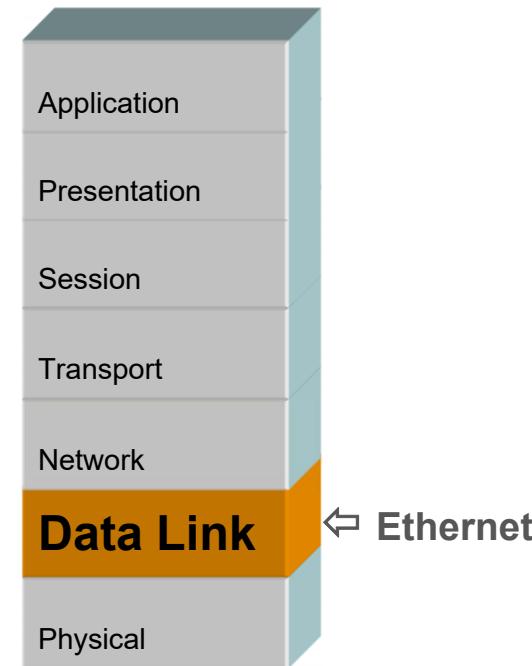
Bus



Hybrid

Layer 2: Data Link Layer

- Provides the rules for framing, converting electrical signals to data, error checking, physical and media access control (MAC) addressing
- MAC address format
 - 00 10 5A 3E 27 F3 (hexadecimal)
- Every communications network needs some data link protocols

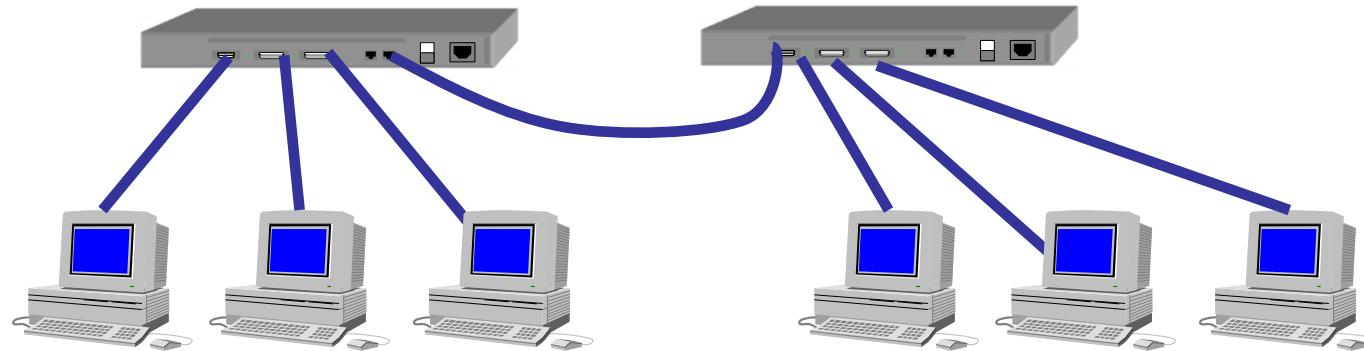


Layer 2: Data Link Layer

- 2 sublayers
 - Logical Link Control (LLC)
 - Media Access Control (MAC)
 - Physical Address
- DLL Protocols examples
 - Ethernet
 - Token Ring
 - Fiber Distributed Data Interface (FDDI)
 - IEEE 802.3
 - IEEE 802.11

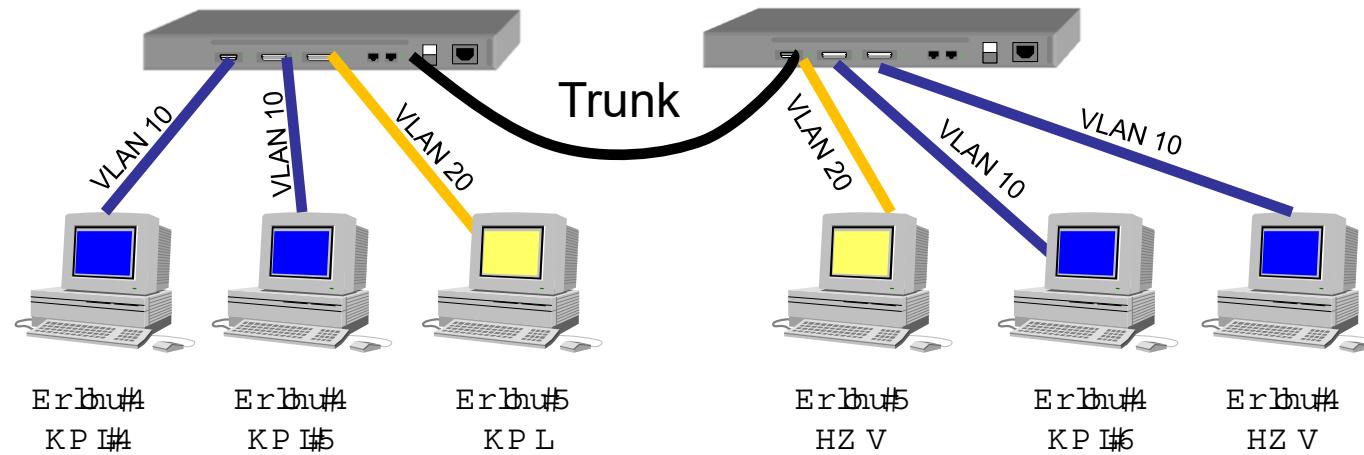
Layer 2 Switches

- Layer 2 Switches work at physical and data-link layer within a single LAN
- More advanced than a hub because a switch will only send a message to the device that needs or requests it
- MAC address used to decide where to forward frame
- Managed and unmanaged switches



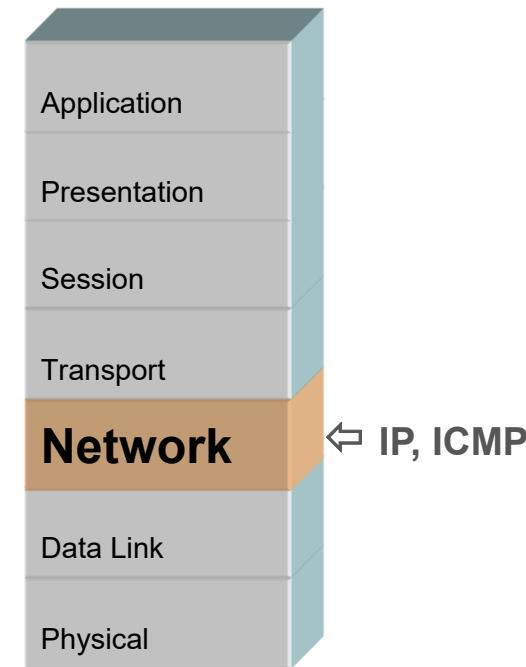
Virtual Local Area Network (VLAN)

- Partition a Layer 2 network (LAN) into multiple distinct segments or broadcast domains
- Enables grouping of hosts with a common requirements regardless of their physical location



Layer 3: Network Layer

- The protocols at the Network layer deal with routing of messages through a complex network
- Find the best route through a network
- IP of TCP/IP fame is one example of a network layer protocol



Layer 3: Network Layer

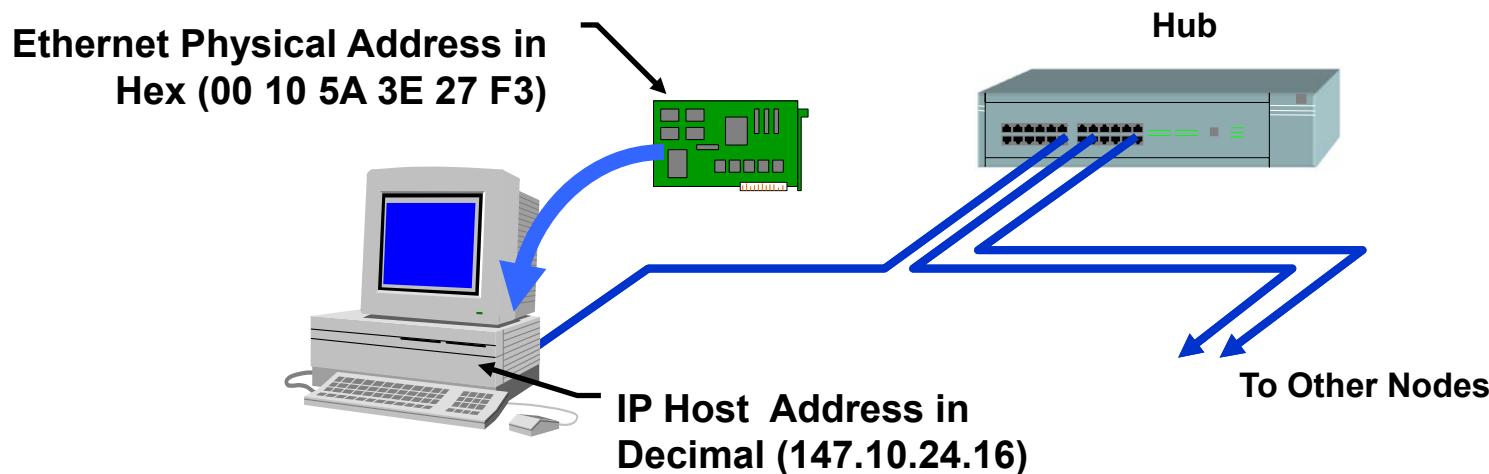
- The network layer is responsible for packet forwarding including routing through intermediate routers
- Routing Protocols – high level outside local network
 - RIP – Router Information Protocol
 - OSPF – Open Shortest Path First
 - BGP – Border Gateway Protocol
- Routable Protocols
 - IP (IPv4 and IPv6)
 - IPX = Internetwork Packet Exchange
 - ICMP = Internet Control Message Protocol
 - IGMP = Internet Group Management Protocol
 - IPSEC= Internet Protocol Security

Layer 3: Network Layer

- Router
 - Divides big network into logical sub-networks
- Layer 3 Switch
 - Will act like a switch when it is connecting devices on the same LAN
 - Local Area Network or subnet
 - Will act like a router to route traffic between different subnets

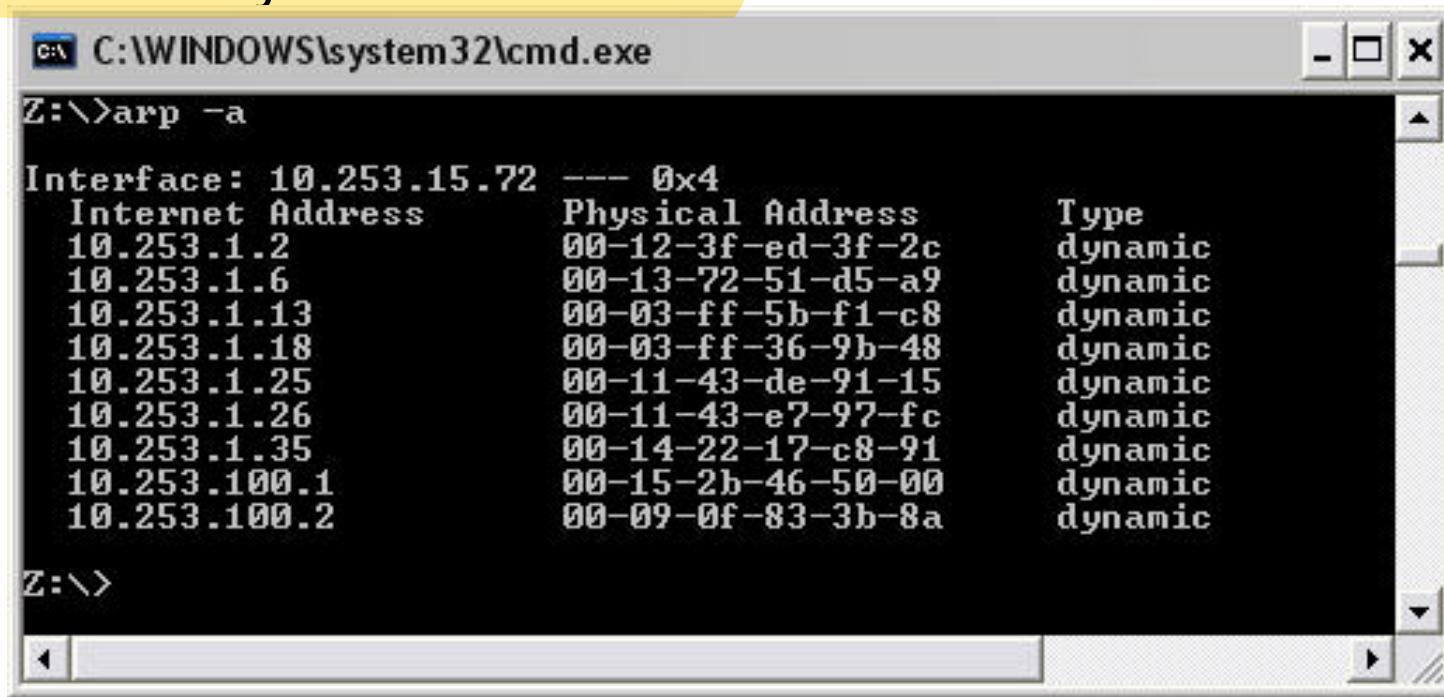
IPv4 Addressing

- Every device in a TCP/IP network needs a unique IP address
- IPv4 uses a **32-bit address** written in the quad-dotted form:
147.10.24.16
- Allows close to **4.3 billion** addresses (4.3×10^9)



ARP Protocol

- Address Resolution Protocol (IPv4)
- Resolve Network Layer IP addresses to Data Link Layer MAC or Physical Addresses



The screenshot shows a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The command "arp -a" is entered, and the output displays the ARP table (ARP Cache) for the interface 10.253.15.72. The table lists various IP addresses and their corresponding physical MAC addresses, all categorized as "dynamic".

Internet Address	Physical Address	Type
10.253.1.2	00-12-3f-ed-3f-2c	dynamic
10.253.1.6	00-13-72-51-d5-a9	dynamic
10.253.1.13	00-03-ff-5b-f1-c8	dynamic
10.253.1.18	00-03-ff-36-9b-48	dynamic
10.253.1.25	00-11-43-de-91-15	dynamic
10.253.1.26	00-11-43-e7-97-fc	dynamic
10.253.1.35	00-14-22-17-c8-91	dynamic
10.253.100.1	00-15-2b-46-50-00	dynamic
10.253.100.2	00-09-0f-83-3b-8a	dynamic

Typical ARP Table (ARP Cache) in a Windows PC

IPv6 Addressing & ARP Protocol

- Formalized in 1998 by the IETF due to IPv4 address exhaustion
- 128 bits allows over 3.4 undecillion addresses (3.4×10^{36})
 - Displayed as 8 groups of 4 hexadecimal digits
 - Address example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- No ARP--uses Neighbor Solicitation
 - Typical response to “Netsh int ipv6 show neighbor”
 - 2001:db8:192:0:24b8:55b8:eb04:c651 40-61-86-e1-6e-1c Reachable
- Slow roll out
- Pretty much every IACS network device will have to be updated to make IPv6 work seamlessly



Recap

- Network types
- ISO OSI/Reference Model
- Layers 1 - 3
- IPv4 Addressing/ARP Protocol
- IPv6 Addressing/ARP Protocol



Setting the Standard for Automation™

Networking Basics: L4-L7

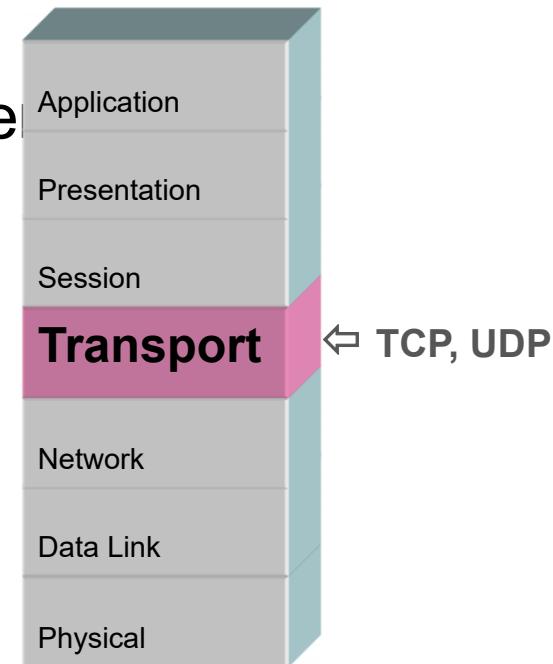
Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Layers 4-7
- Problems with OSI Model
- Intro to Network Discovery and Security Auditing Tools

Layer 4: Transport Layer

- Provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control.
- It ensures complete data transfer
- Numbers packets to keep them in order
- TCP of TCP/IP fame is one example of a transport protocol



Layer 4: Transport Layer

- Transport Layer Functions
 - Flow Control
 - Multiplexing
 - Virtual Circuit Management
 - Error Checking and Recovery
- Transport Layer Protocols

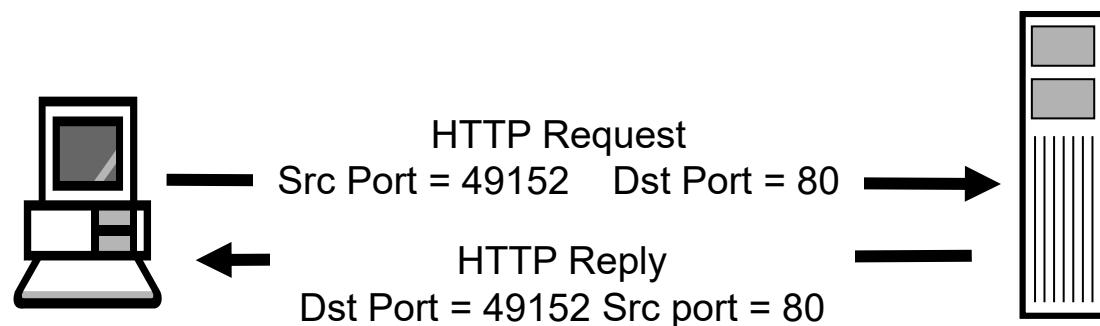
Protocol	Name	Use
TCP	Transmission Control Protocol	Connection based
UDP	User Datagram Protocol	Send and forget
DCCP	Datagram Congestion Control Protocol	Connection setup & teardown
SCTP	Stream Control Transmission Protocol	UDP with TCP delivery assurance
RSVP	Resource Reservation Protocol	A control protocol

TCP / UDP Port Numbers

- TCP/UDP port numbers identify the application that will handle a packet inside the host

Client
Web Browser - Port 49152

Server
Web Server - Port 80

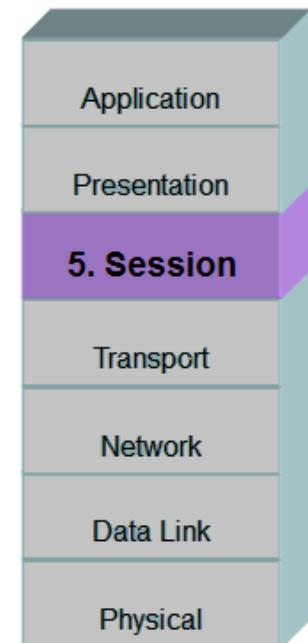


Port Number Assignments

- Port numbers are assigned based on three ranges:
 - System or Well-Known Ports (0-1023)
 - User or Registered Ports (1024-49151)
 - Dynamic or Ephemeral or Private Ports (49152-65535)
- Service Name and Transport Protocol Port Number Registry
 - Exists as online database
 - <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

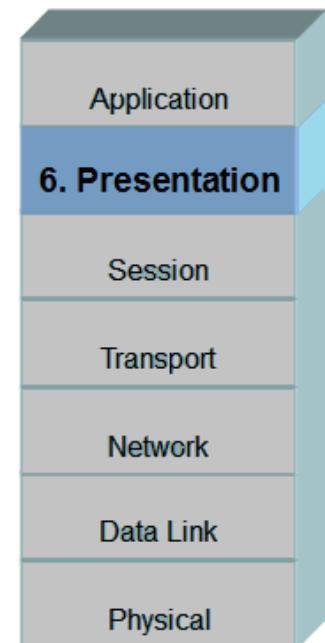
Layer 5: Session Layer

- Session is a persistent logical linking of two software application processes
- Provides the mechanism for opening, closing and managing a session between end-user application processes
 - Associated with TCP/UDP port numbers
- Each OS handles session data differently
- Example protocols:
 - Layer 2 Tunnelling Protocol (L2TP)
 - Point-to-Point Tunnelling Protocol (PPTP)
 - Remote Procedure Calls (RPC)



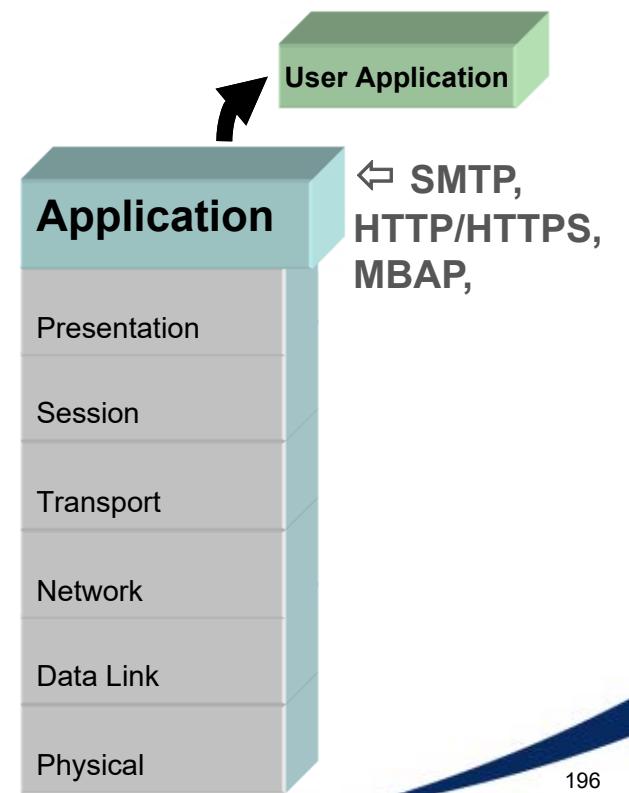
Layer 6: Presentation Layer

- Presentation layer functions are generally handled in the Application layer (FTP, SMTP, Telnet, etc.)
- Deals with data format conversion and possibly with encryption and security
 - Associated with Secure Sockets Layer (SSL)
- Responsible for the delivery and formatting of info to the application layer for further processing or used)



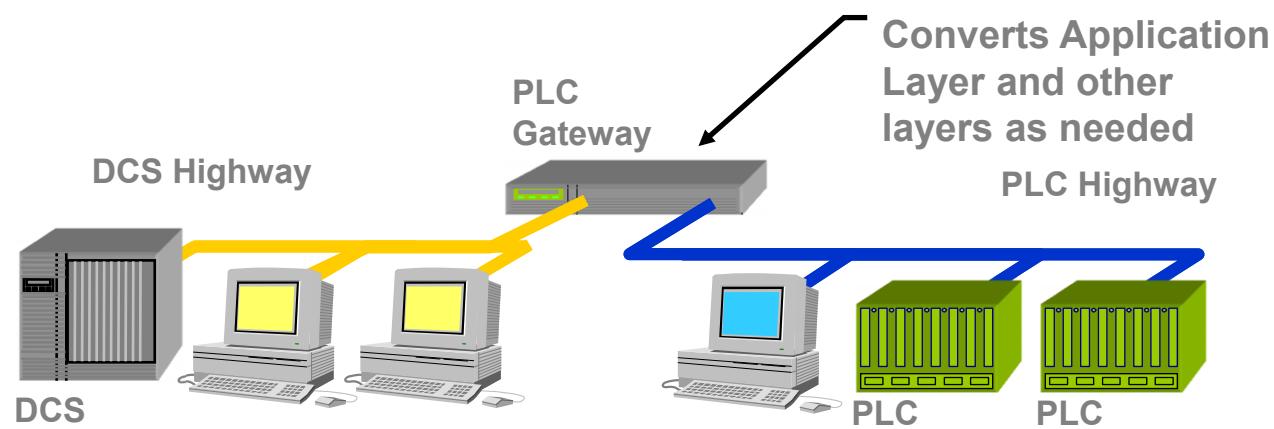
Layer 7: Application Layer

- Does not include user software applications like word processing or operating systems like Windows XP or Windows 7, Windows 10
- Interacts with software applications that implement a communicating component
- Protocols specific to network applications such as email, file transfer, reading data registers in a PLC



Layer 7 Gateways

- Gateways are a layer-seven device
 - This is not the “default gateway” network interface card setting
- Gateways connect two completely differing network systems (e.g. DCS to PLC, Allen Bradley to Foxboro, Cloud to Cloud)
- Also used to provide application layer conversions (e.g. between two different email systems)



Problems with the OSI Model

- OSI layer specifications are functional only
 - What to do is defined
 - How to do it is not
- Two protocol families that are "ISO compatible" won't necessarily communicate
- It is too complex for many applications (such as industrial fieldbuses) so layers are skipped, typically L5 & L6
 - PLC, DCS have unique OS, memory management, scan management
- But it does give us a good starting point to organize all those protocols...



Intro to Network Discovery and Security Auditing Tools

- Many free and open-source tools such as
 - Nmap
 - SuperScan
- Tools useful for tasks
 - Vulnerability Scanner
 - Network inventory
 - Managing service upgrade schedules
 - Monitoring host or service uptime
- Tools also useful by unauthorized personnel 😞
 - Scan and “fingerprint” network
 - Services (application name and version)
 - Operating systems (and OS versions)
 - Type of packet filters/firewalls in use

Intro to Network Discovery and Security Auditing Tools

Caution

- Tools may adversely affect hazardous materials, operations or equipment
- Tools like vulnerability scanners can disrupt a control network and should not be used on live systems
- Safety systems could be triggered by scanning tools
- Obtain appropriate clearances, coordination and asset owners' permission to run any tools

Recap

- Layers 4-7
- Problems with OSI Model
- Intro to Network Discovery and Security Auditing Tools

3.7 The Basic “Ethernet Design Rules”

The “5-4-3-2” rule states that the maximum transmission path is composed of 5 segments linked by 4 repeaters; the segments can be made of, at most, 3 coax segments with station nodes and 2 link [10BASE-FL] segments with no nodes between.

Exceeding these rules means that some (though not all) nodes will be unable to communicate with some other nodes. You should check your design to ensure that no node is separated from any other node by more intermediate devices than the table below indicates.

Table 3-3. Maximum Transmission Path Between Any Two Nodes

5 segments 4 repeaters 3 link segments 2 coax segments	OR	5 segments 4 repeaters 3 coax segments 2 link segments
-----------------------------------------------------------------	----	-----------------------------------------------------------------

Note: This table is a popular simplification of the actual 802.3 rules.

3.8 “Would Somebody Please Explain This 7-Layer Networking Model?” (Adapted from *Sensors Magazine*, July 2001, ©Advanstar)

Networks, and the information that travels on them, are most easily understood in layers. For many years the International Standard Organization/Open Systems Interconnection (ISO/OSI) model (Figure 3-2) has been used as a way to represent the many layers of information in a network, particularly the low-level transport mechanisms. From top to bottom, these are the layers and how these layers relate to your product design (Table “Layer 1”).

Please note that most networks do not actually use all these layers, only some. For example, Ethernet and RS-232 are just

physical layers—layer 1 only for RS-232 and layers 1 and 2 for Ethernet. TCP/IP is a protocol, not a network, and uses layers 3 and 4, regardless of whether layers 1 and 2 are a phone line, a wireless connection, or a 10BASE-T Ethernet cable.

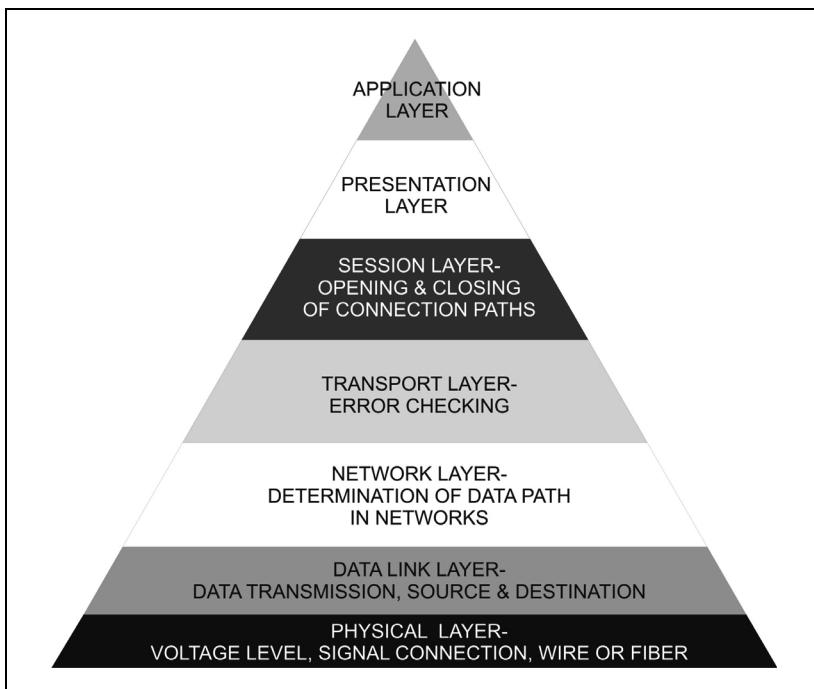


Figure 3-2. The 7-Layer Network Concept

Layer 7: Application

The application layer defines the meaning of the data itself. If you send me a .PDF file via email, the application that is used to open it is Adobe Acrobat. Many layers of protocols are involved, but the application is the final step in making the information usable.

In a sensor design, this is the software component that exchanges process data between the sensor elements (and their associated A/D converters, etc.) and the communications pro-

cessor. It recognizes the meaning of analog and digital values, parameters, and strings.

J1939 and CANopen are application layers on top of CAN. FOUNDATION Fieldbus HSE is an application layer on top of Ethernet and TCP/IP. Modbus is an application layer on top of RS-232/485.

Layer 6: Presentation

The presentation layer converts local data into a designated form for sending and for converting received data back to the local representation. It might convert a character set such as MacRoman to ASCII for transmission. Encryption can happen in this layer.

Layer 6 is usually handled by application software and is not usually used in industrial networks.

Layer 5: Session

The session layer creates and maintains communication channels (sessions). Security and logging can be handled here.

Layer 5 is handled by software and is not commonly used in industrial networks.

Layer 4: Transport

The transport layer controls transmission by ensuring end-to-end data integrity and by establishing the message structure protocol. It performs error checking.

Layer 4 is usually handled in software (e.g., TCP/IP).

Layer 3: Network

The network layer routes data from node to node in the network by opening and maintaining an appropriate path. It may also split large messages into smaller packets to be reassembled at the receiving end.

Layer 3 is done in software.

Layer 2: Data Link

The data link layer handles the physical transmission of data between nodes. A packet of data (data frame) has a checksum, source, and a destination. This layer establishes physical connection between the local machine and the destination, using the interface particular to the local machine.

Layer 2 is almost always done in hardware with application-specific integrated circuits (ASICs). Low-speed networks can perform layer 2 functions in software.

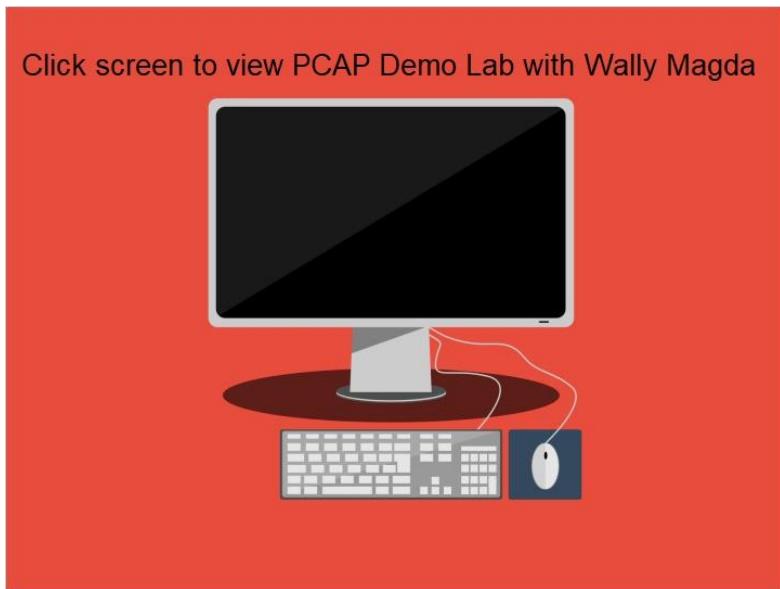
Layer 1: Physical Layer

Layer 1 defines signal voltages and physical connections for sending bits across a physical media and includes opto-isolation, hubs, and repeaters. Physical media refers to the tangible physical material that transports a signal, whether copper wire, fiber, or wireless.

The data to be transferred starts out in the application layer and is passed down the seven layers to the physical layer, where it is sent to the receiving system. At that end, it is passed up through the layers to the remote application layer, where it is finally received by the user.



1.4 Lab Video



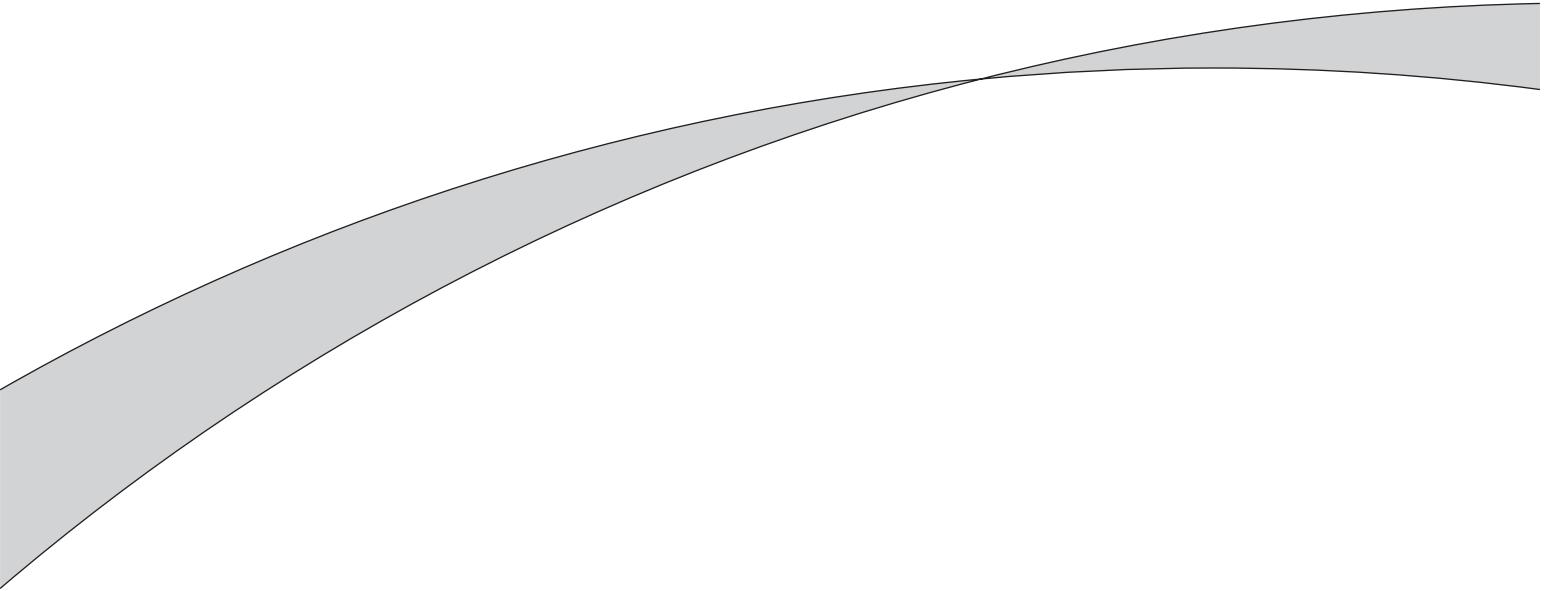


Setting the Standard for Automation™

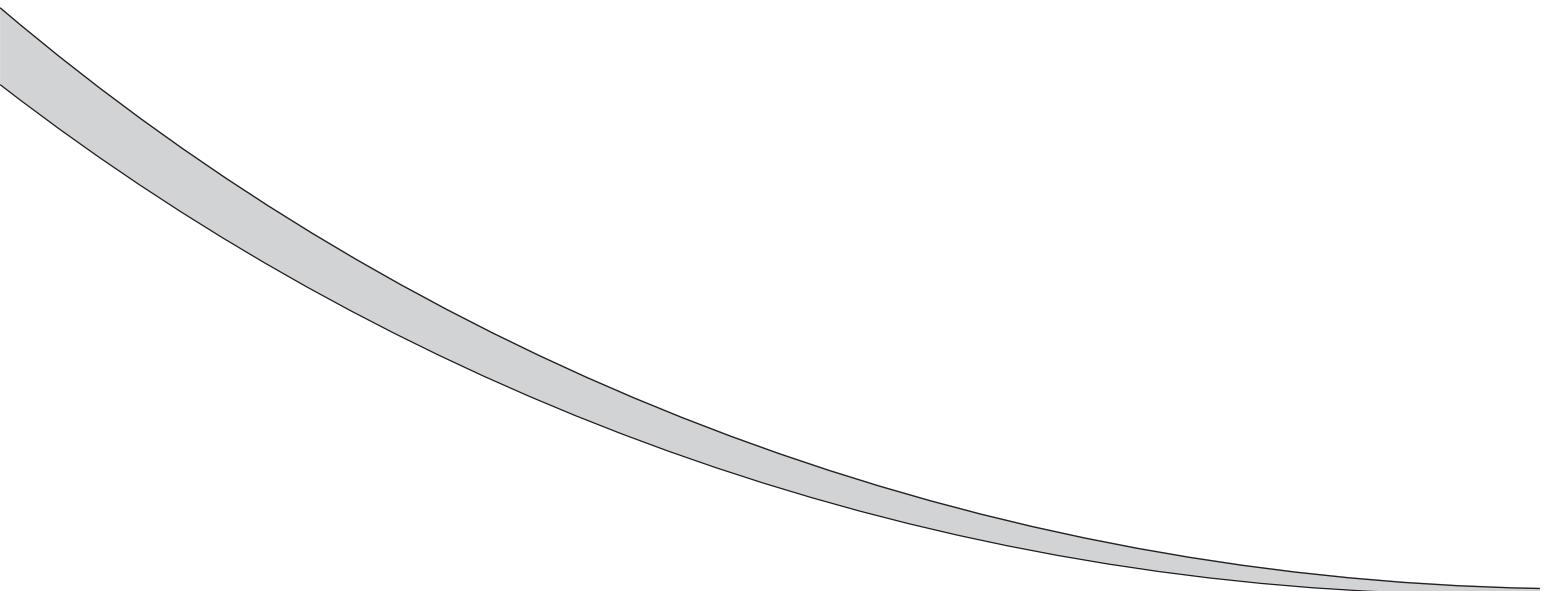
Thank you for completing this module!

Demonstration Lab PCAP Analysis

Exit



Week 5



Week 5

Week 5



Setting the Standard for Automation™

Section Network Security Basics

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Why we need to address security
- Firewalls



Setting the Standard for Automation™

Why We Need To Address Security

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Fundamental Issue

- TCP & IP were not designed to be secure
 - They were designed to ensure that communications work
- PLCs were designed to replace relays
 - Their primary function is to service I/O
 - Ethernet was an afterthought.
 - They were not designed to be secure



Network attack methods (threats)

- Known vulnerabilities not patched
- Storms/Floods
- Spoofing
- Man-in-the-Middle
- Replay attacks
- Sniffing
- Session hijacking
- Buffer or stack overflow
- Brute force or dictionary



Network Security Technologies

- Network Security Devices
 - Switches/Routers
 - Firewalls
 - Unidirectional Gateways (Data Diodes)
- Network Architectures
- Cryptography
 - VPN
 - Hashes
 - Secure Protocols
- Intrusion Detection Systems
 - Network
 - Host





Setting the Standard for Automation™

Firewalls

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

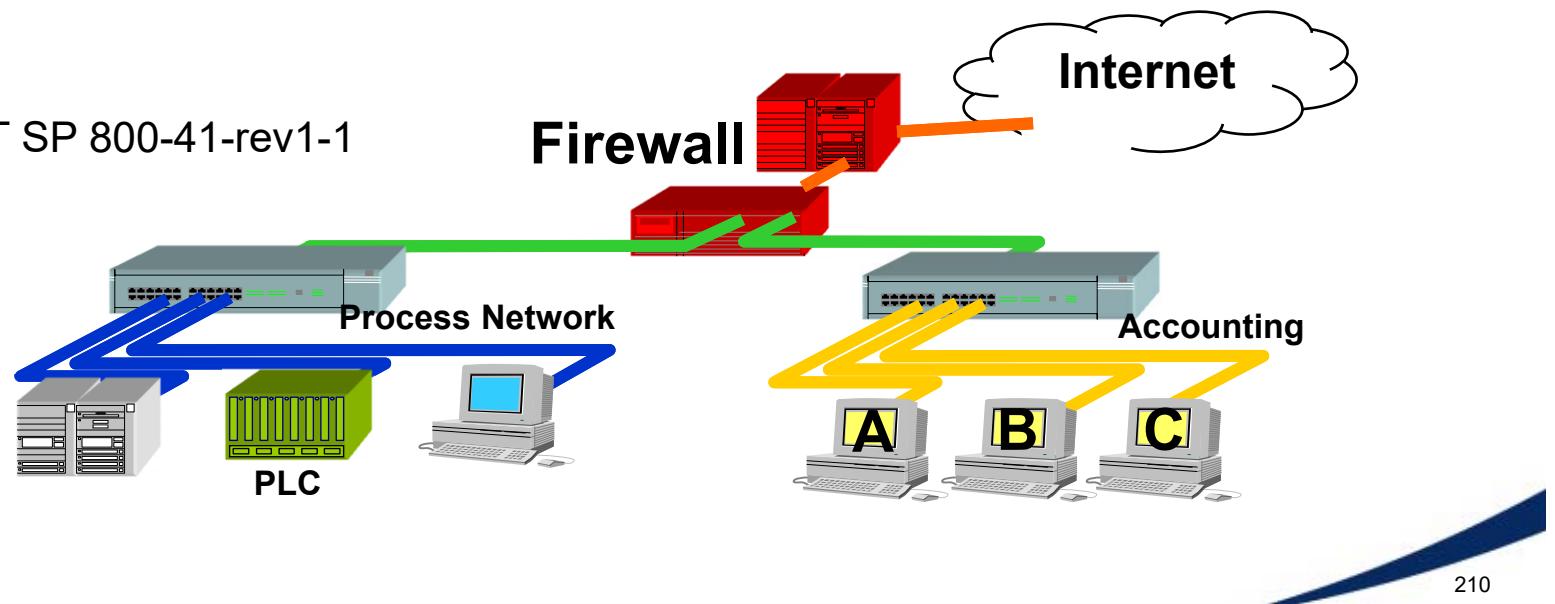
What is a firewall?

- Inter-network connection device that restricts data communication traffic between two connected networks
 - Filters network traffic
- Application installed on a general-purpose computer
- Dedicated platform (appliance)
 - Forwards or rejects/drops packets on a network.
- Typically, firewalls are used to define zone borders
- Firewalls generally have rules restricting which ports are open.

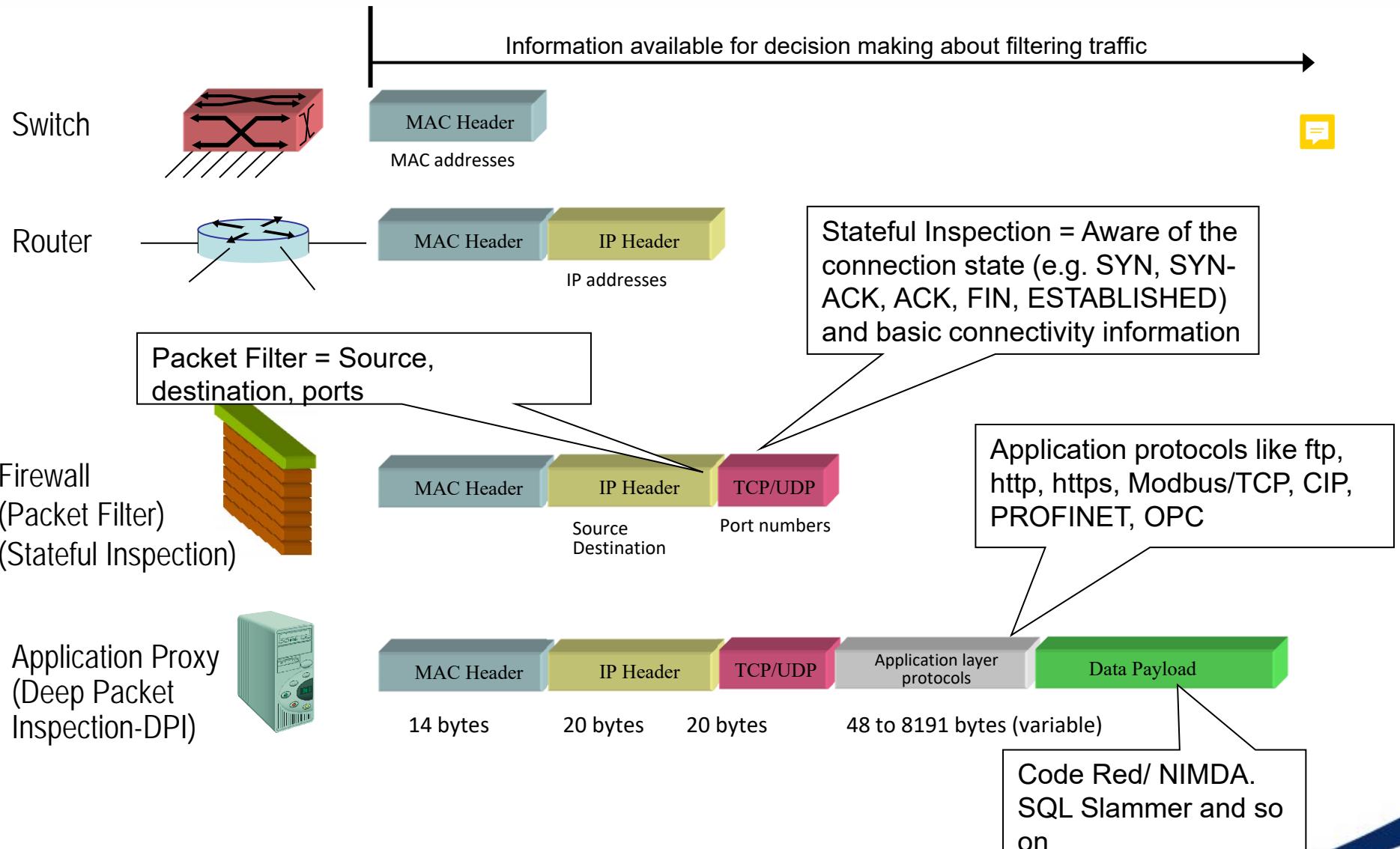
Hardware firewalls

- A firewall is a mechanism used to control access to and from a network for the purpose of protecting it and the equipment attached.
- Is a gateway through which all traffic passes.
- Three general classes:
 - Packet Filter
 - Stateful Inspection
 - Application Proxy and Deep Packet Inspection (DPI)

Reference NIST SP 800-41-rev1-1

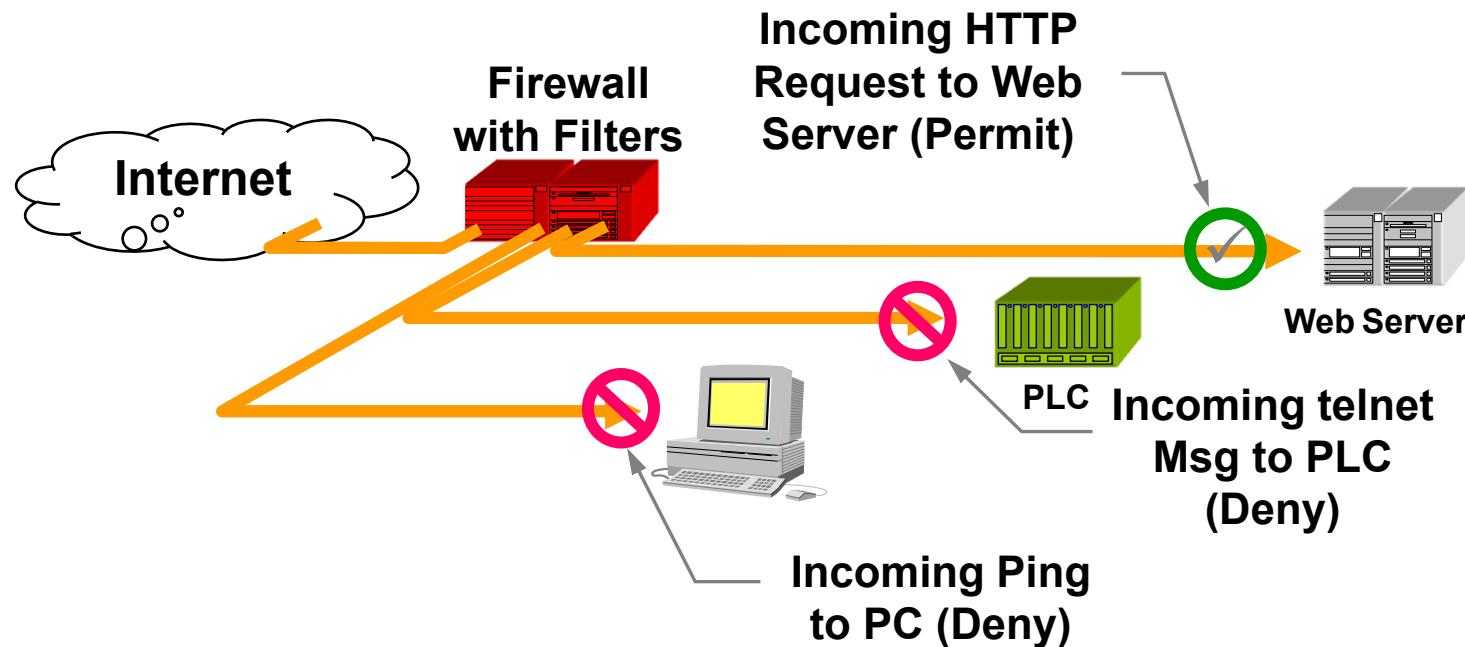


Device Decision Basis



Firewall Policy

- A firewall is relatively easy to install.
- Configuring is more difficult.
- Deciding how it should be configured is most difficult
- A firewall is only as good as its rules!!!



IACS Firewall Configuration Best Practices

- Default rule
 - Block all traffic by default
 - Explicitly allow only specific traffic to known service
 - Ingress and Egress (inbound and outbound)
 - IACS devices should not be allowed to access the Internet
 - Prevent traffic from transiting directly from the IACS network to the enterprise network
- Clean up unused rules
- Rules must be exhaustively tested before deployment
- Management/Out of Band ports secured

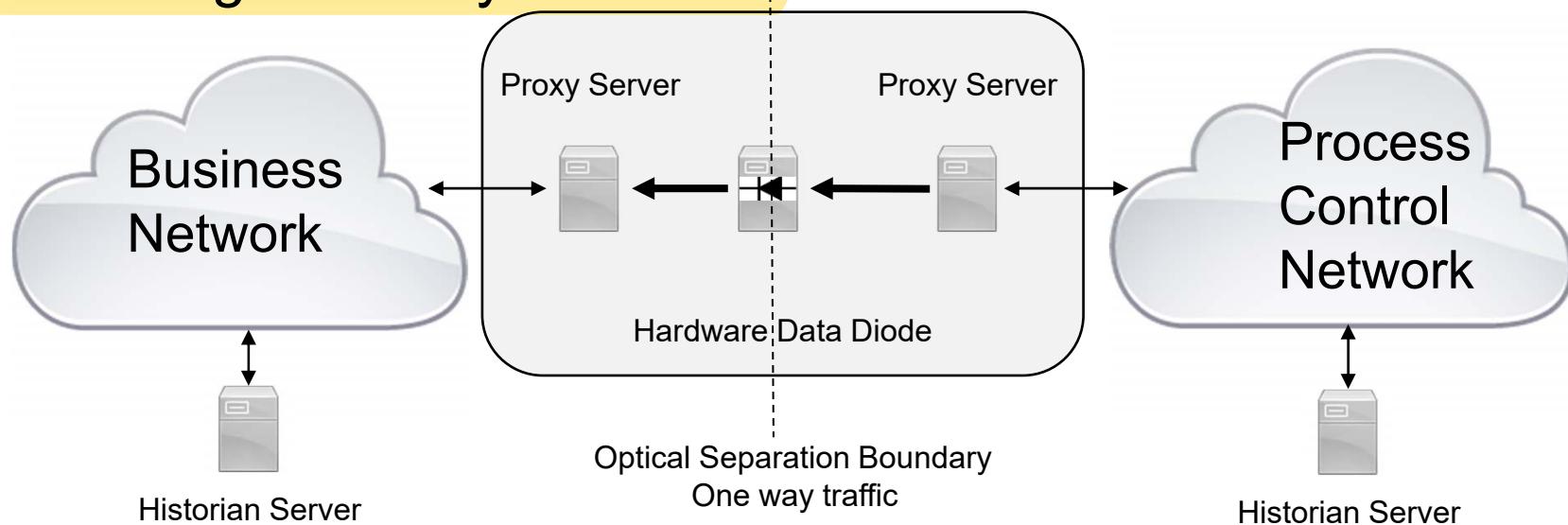
IACS Firewalls

- Companies now offering IACS firewalls to protect vulnerable devices such as PLCs and DCS controllers
 - Industrial form factor and robustness
 - Electrician / Control Tech friendly
 - Knowledge of industrial protocols
 - Extensibility beyond just packet filtering
- Sample of IACS Appliance Vendors:
 - Tofino (Belden)
 - Hirschmann Eagle (Belden)
 - Moxa (Moxa)
 - Zenwall (Secure Crossing)
 - mGuard (Phoenix Contact)
 - Scalance S (Siemens)
 - Connexium (Schneider Electric)
 - Stratix—Cisco product (Rockwell)



Unidirectional Gateway (Data Diode)

- Network device allowing data to travel only in one direction
- Normal flow control SYN ,SYN-ACK, ACK must be emulated
- Defense and nuclear power plants
- Finding their way into IACS



Recap

- Why we need to address security
- Firewalls



Setting the Standard for Automation™

Section: Industrial Protocols

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Industrial Protocols
- Modbus
- Profibus
- CIP
- OPC



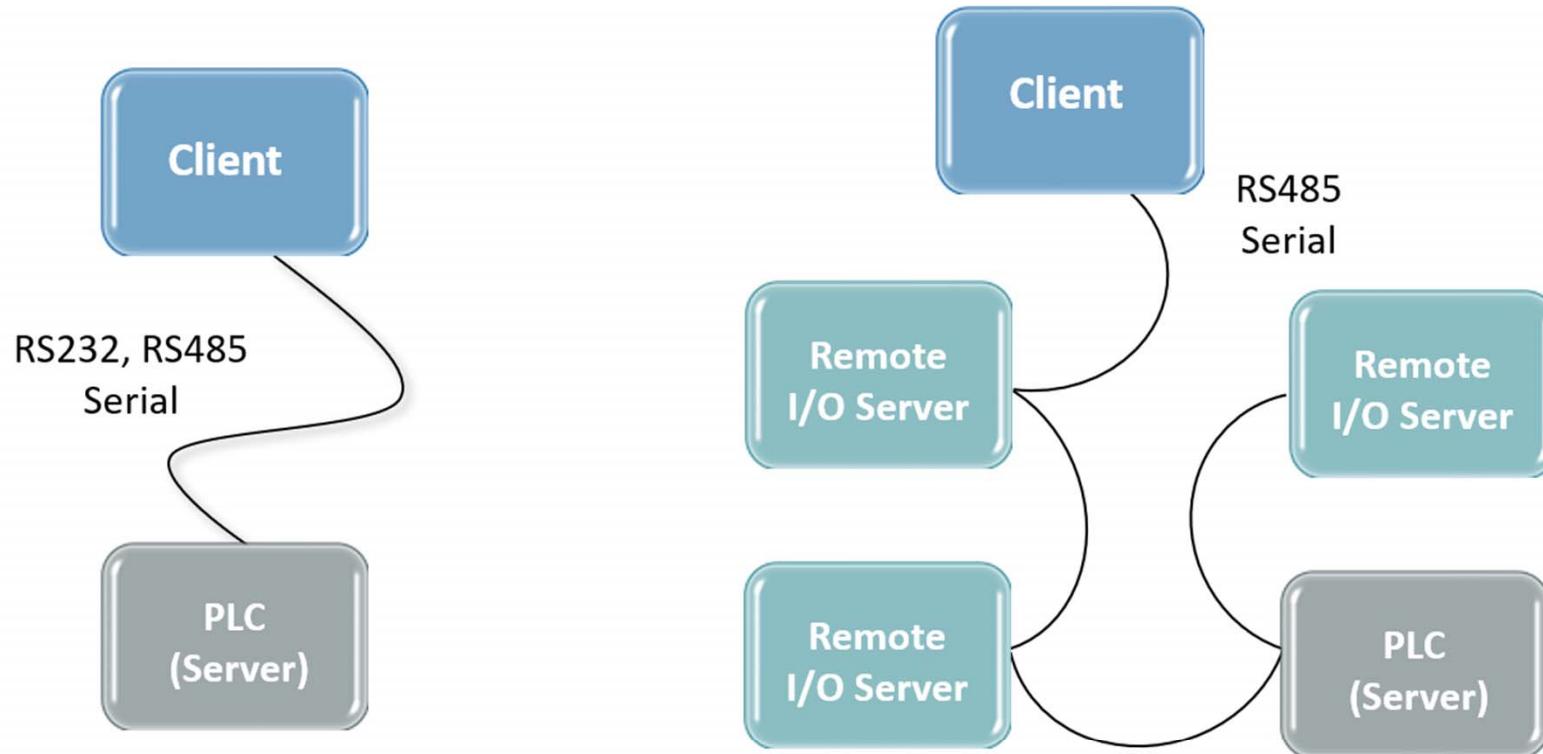
Industrial Protocols

- Protocol
 - Set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems
- Multitude of industrial protocols (e.g.)
 - MODBUS -DNP3
 - PROFIBUS -IEC 61850
 - OPC -HART
 - CIP -BACnet
- Wonderware
 - Over 900 industrial protocol device drivers
- Kepware
 - Over 130 industrial protocol OPC Unified Architecture (UA)

MODBUS

- Serial communications protocol originally published in 1979 by Modicon (now Schneider Electric)
- De facto standard, openly published and royalty free
- Widely used network protocol in the industrial manufacturing environment (over 7 million nodes)
- Basic functions support reading and writing of PLC registers and I/O
- Variants exist

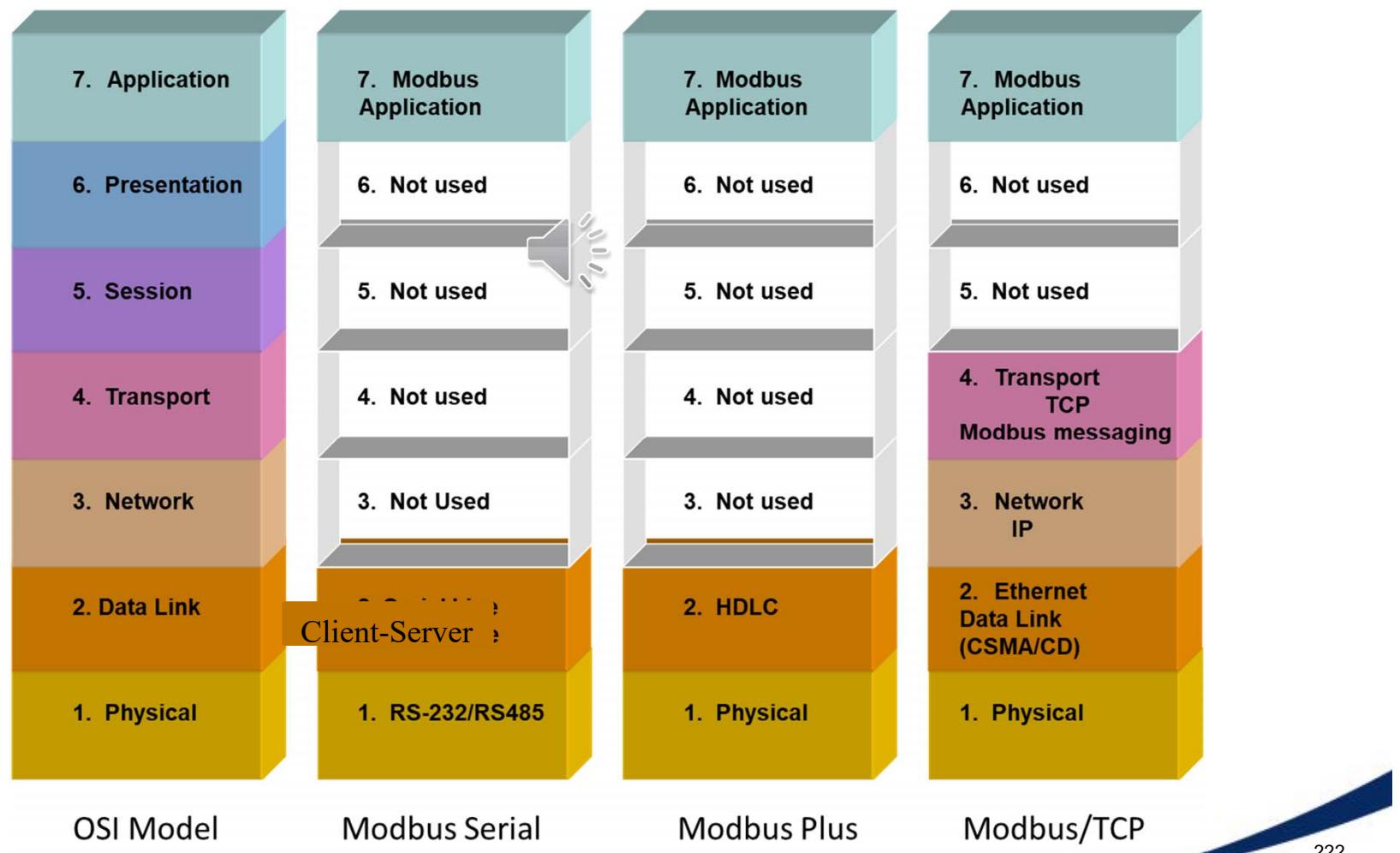
MODBUS



- Depicted are Modbus communication nodes per the Modbus serial specification
- In other topologies, nodes can be clients or servers; some can be a combination of both

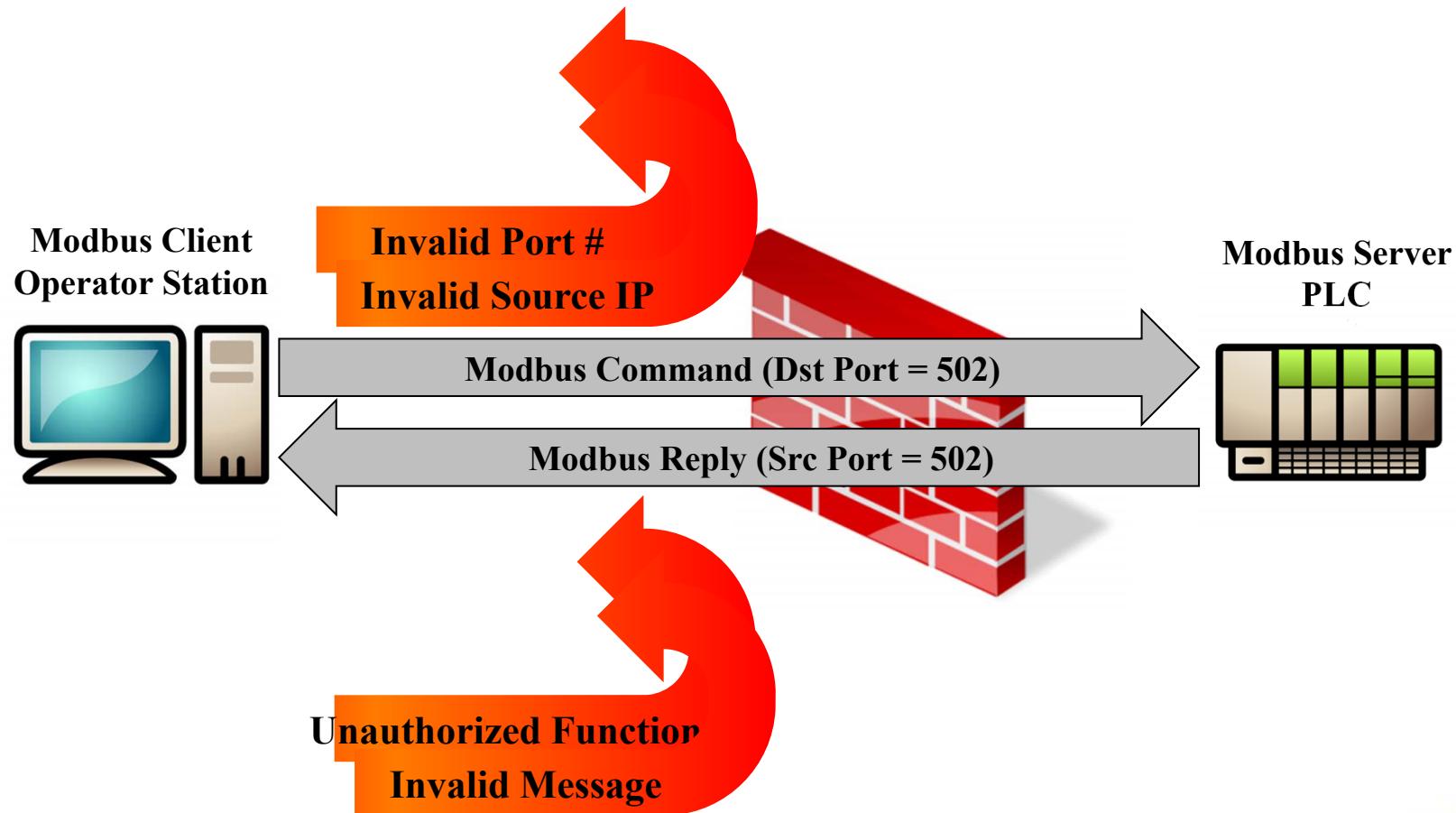
MODBUS TCP

- An open Modbus TCP/IP specification was developed in 1999



Securing MODBUS

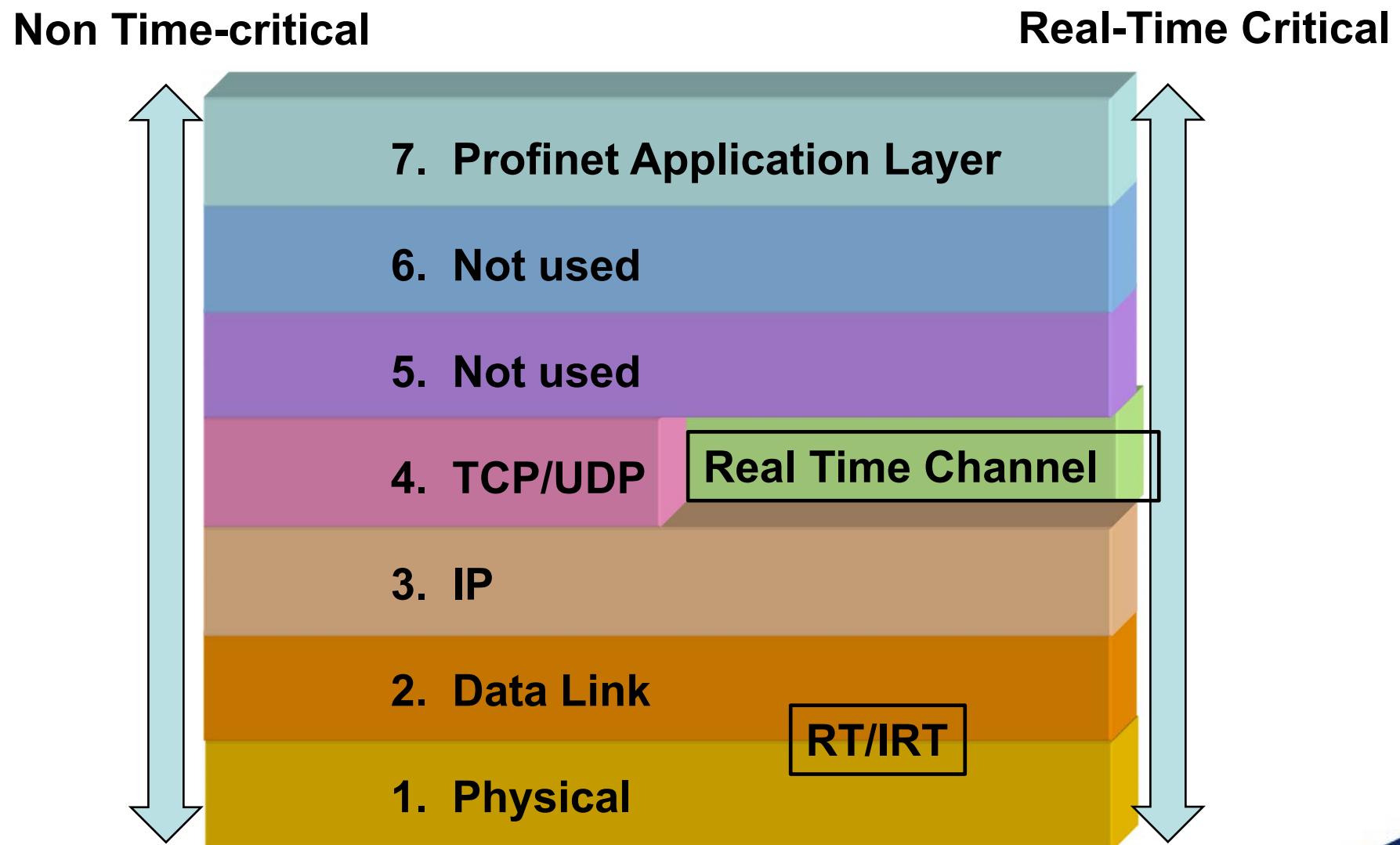
- Easily firewalled (source IP, destination IP, TCP Port 502)
- MODBUS aware firewalls can inspect packets and reject specific function codes



PROFIBUS

- PROFIBUS (Process Field Bus) is a standard for field bus communication in automation technology
- Developed by Siemens around 1989
- Many variations:
 - PROFIBUS DP (Serial)
 - PROFIBUS PA (Serial)
 - PROFISAFE (Safety)
- PROFINET (TCP - Ethernet)

PROFINET OSI Model

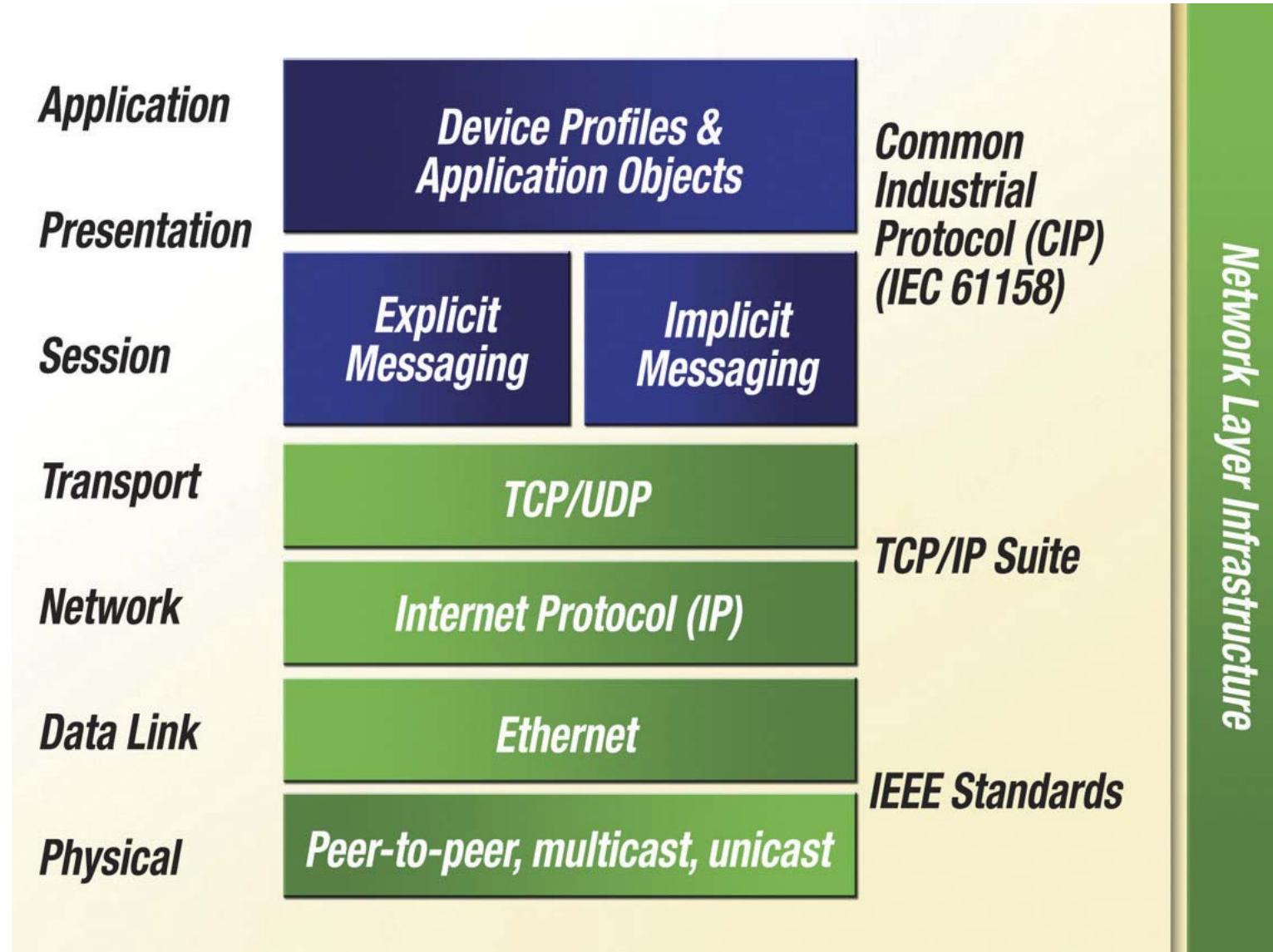


Common Industrial Protocol (CIP)

- The Common Industrial Protocol (CIP) is an industrial protocol for industrial automation applications (formerly Control & Information Protocol)
- Developed by Rockwell Automation
- Supported by Open DeviceNet Vendors Association (ODVA)
- Underlying protocol for:
 - DeviceNet
 - ControlNet
 - EtherNet/IP

– “IP” = “Industrial Protocol” not “Internet Protocol”

EtherNet/IP OSI Model



Ethernet/IP

- Uses two communications mechanisms and two ports
- Implicit messaging
 - Port 2222
 - Producer/Subscriber
 - Typically I/O messages
 - Time critical applications
 - Uses UDP Multicast and Unicast for IO transfer.
- Explicit messaging
 - Port 44818
 - Client Server – HMI to PLC
 - Not time critical
 - Uses TCP Unicast for administration and data transfer.

OPC

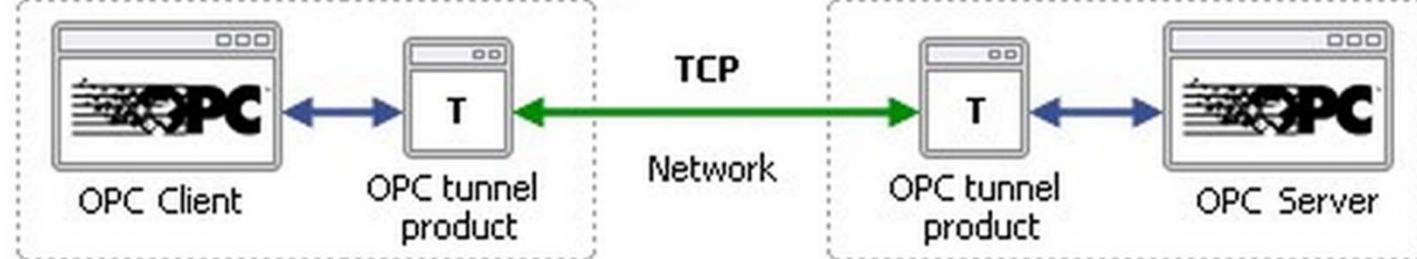
- OPC stands for Open Platform Communications
- Initially Object Linking and Embedding (OLE) for Process Control
- Communication standard developed in 1996 by an industrial automation industry task force
- Based on Microsoft OLE, COM, and DCOM technologies
- Specifies the communication of real-time plant data between control devices from different manufacturers
- The OPC Foundation maintains the standard

Many OPC Specifications

- OPC Data Access (OPC Classic)
- OPC Alarms and Events (AE)
- OPC Historical Data Access (HDA)
- OPC Batch
- OPC Data eXchange
- OPC Security
- OPC XML-DA
- OPC Unified Architecture (UA)

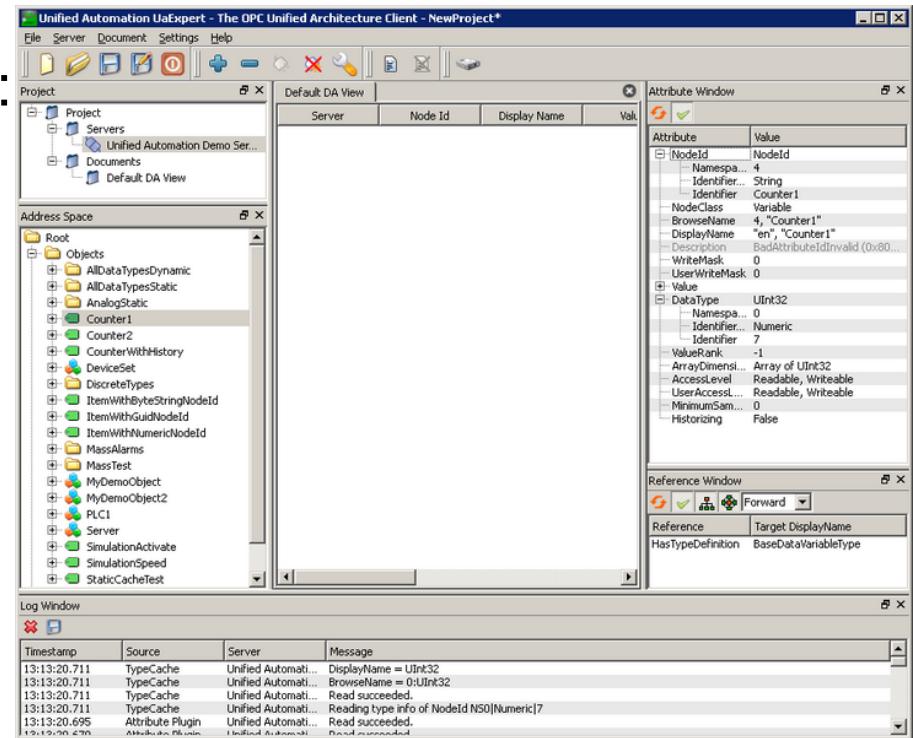
OPC Classic is difficult to firewall

- Because OPC Classic uses DCOM and DCOM is free to use any port between 1024 and 65535 it is “IT firewall unfriendly”
 - Both server and client will negotiate dynamic ports after initial contact
- Solutions:
 - OPC-Classic Aware Firewalls that analyze the DCOM protocol to momentarily open the correct port
 - OPC Tunnel Applications that use a local client and server with a single port between to get the data through the firewall



OPC Unified Architecture

- Not using DCOM anymore, just normal sockets using one (1) port.
 - OPC directly on the IACS device
 - Siemens, Rockwell and other have OPC Servers directly on the device
- A Browsable Namespace with:
 - Folders
 - Classes
 - Objects
 - Methods
- Companion Specifications
 - Specific namespaces
 - Like XML Schema Definitions



OPC Unified Architecture

- Designed from the ground up to be secure
 - Session Encryption: messages are transmitted securely at 128 or 256-bit encryption levels
 - Message Signing: messages are received exactly as they were sent
 - Sequenced Packets: exposure to message replay attacks is eliminated with sequencing
 - Authentication: each UA client and server is identified through OpenSSL certificates providing control over which applications and systems are permitted to connect with each other
 - User Control: applications can require users to authenticate (login credentials, certificate, etc.) and can further restrict and enhance their capabilities with access rights and address-space “views”
 - Auditing: activities by user and/or system are logged providing an access audit trail

Recap

- Industrial Protocols
- Modbus
- Profibus
- CIP
- OPC

8.0

Ethernet Industrial Protocols, Fieldbuses, and Legacy Networks

I can't tell you how many times over the years I've had someone ask "what is the best Ethernet protocol?" That's like asking who has the best pancakes, what is the most exciting sporting event, and what is the best Christmas movie of all time? (FYI, the answers are: 1. Pancake Place in Green Bay, Wisconsin, 2. NCAA Basketball Tournament, and 3. *It's a Wonderful Life*.)

The truth, of course, on the question of factory floor protocols is simply "it depends." Do you want to move I/O data or information? How fast do you need to move the data? How much data do you need to move? How many devices have the data now? There is no end to the questions you should ask and answer.

In practice, it is not that complicated. In the great majority of cases, it just comes down to the brand of programmable logic controller (PLC) used in your building, or used by the majority of your customers, that drives the Ethernet protocol. If you are using Siemens PLCs, the "best" Ethernet protocol is PROFI-

NET IO. If you're using a Rockwell ControlLogix or CompactLogix, it is EtherNet/IP. If you want to keep everybody happy, or at least not too unhappy, use Modbus TCP.

From a purely technical standpoint, Ethernet and any of these Ethernet protocols are not necessarily more ideal for automation applications than any other network. Even if there was one that was superior to the others, the nature of capital equipment is still such that no one is going to rip out existing equipment and wiring just because something better exists.

But ignoring the PLC brand issue, there is a series of questions that you could ask to determine if you should use an Ethernet protocol or another type of industrial communication system (CAN, Modbus Serial, PROFIBUS DP, etc.). These questions include:

- What is the distance requirement?
- What kind of physical cabling arrangement makes sense for this application? All the Ethernet formats except 10BASE2 and 10BASE5 use a star topology. This is fine for applications where devices are clustered together in groups but for others, such as a long conveyor with many nodes spaced 20 m apart, it is quite inconvenient. For the conveyor, a trunk/drop topology (such as that used by DeviceNet™ and CANopen) is much better.
- What is the actual speed (response time) requirement for the most time-critical devices? Do all of the devices require that level of speed or should some devices have a higher priority than others?
- Does your application require that you prioritize messages?

- Do the devices you want to use support the same network standard? Are there open versus closed architecture considerations?
- If you are developing a network-capable product, what is the hardware bill of materials and the cost of software development for that network?
 - How much electrical noise is present in the application and how susceptible is the cabling?
 - What is the maximum required packet size for the data you are sending? If the data can be fragmented over several packets, how fast does a completed message have to arrive?
 - What types of device relationships are desired (master/slave, peer-to-peer, broadcast)?
 - Does the network need to distribute electrical power? If yes, how much current?
 - What kind of fault tolerance must be built into the network architecture?
 - What is the total estimated installed cost?

With the answers to these questions you can make a reasonably good choice on an industrial networking protocol.

8.1 The Two Most Important Points to Understand

This chapter describes the leading industrial automation protocols. To understand those protocols, you need to understand two key points that apply to all industrial Ethernet protocols. The first key point is that the most important differentiator from one Ethernet protocol to another is the data representation. The data representation—how data is organized in

devices and implemented in the address space of the protocol—is what makes the protocol unique. It is the key to a genuine understanding of any of these technologies. Everything else that describes the protocol—how data is transported, how connections are made, and what services exist to provide one device (usually the client) with access to the data in the address space of another device (usually the server)—is actually similar from protocol to protocol. For example, both EtherNet/IP and PROFINET IO use synchronous messaging and both EtherNet/IP and Modbus TCP make more extensive use of TCP. There are a lot of commonalities but the way data is accessed in the address space of a device is the key differentiator.

The second key point is that industrial Ethernet protocols are simply a way of defining messages that pass through the “pipe” known as the *TCP/IP stack*. You can think of a TCP/IP connection between two devices as a phone connection. The connection can exist even if no one is talking (sending data) over the connection. That is why these Ethernet protocols are known as *application layer protocols*, they are the “applications” that uses the TCP/IP stack.

Each of the industrial protocols make use of the TCP/IP stack and TCP/IP connections in different ways, but they all send messages through the pipe in one way or another. All protocols use the IP layer. Some solely use TCP (Modbus TCP), some use both TCP and UDP (EtherNet/IP), and one uses TCP but also has another channel that bypasses the TCP/IP layer.

When reading the following sections on these Ethernet application layer protocols, make special note on how the data is organized, the object model of the protocol, and how each protocol makes use of the services of the TCP/IP stack.

8.2 Modbus and Modbus TCP

Saying that you want to discuss Modbus can sometimes bring to mind chats about buggy whips, the rotary telephone, or that new innovation, the color television. What is there to say? What hasn't been said about Modbus over the last 40 years?

Modbus is hardly a new technology. Historians can disagree about its actual birth, but it is certainly a product born in the 1970s. Success is such a trite word for how well it has done over those 40 years. Modbus has found its way into hundreds of thousands—if not millions—of devices. You can find it in everything from valve controllers, to motor drives, to human-machine interfaces (HMIs), to water filtration systems. It would be difficult indeed to name a product category in industrial or building automation that does not use Modbus.

Yet even in the automation world, Modbus isn't just old technology. *It is ancient technology.* Modbus is like that lovable old uncle that comes over every Thanksgiving. He's retired now, he putters around his garden, he's no longer the handsome debonair man of 40 years ago, but he's there when we need him and that is why we love him.

Prior to Modbus, all we had was electrical signaling. Modbus changed that. In fact, Modbus changed everything. Modbus introduced the concept of data on the factory floor. Modbus made it possible to connect an entire group of devices using only two wires on the controller. That alone saved a massive investment in wire, labor, and installation time. Instead of miles and miles of wire connecting hundreds of devices, a simple two-wire pair could be used to daisy-chain devices together. It was revolutionary for its time.

It wasn't just that Modbus was the first serial protocol. Modbus was the right technology at the right time. Remember that the first microprocessor wasn't invented until shortly before the birth of Modbus. Do you remember what those microprocessors were like? Simple 8-bit processors with severely limited code space and memory.

Modbus is the most pervasive communications protocol in industrial and building automation and the most commonly available means of connecting automated electronic devices. Why did that happen? Why did Modbus have such an impact on the industrial automation industry that it has survived for over 40 years and is to this day one of the leading industrial networks of the twenty-first century? There are three primary keys to its success:

- **Modbus Is an Open Standard** – Modicon, the inventor of Modbus, did not keep the standard proprietary. They released it as a nonproprietary standard and welcomed developers, even competitors, to implement it. They rightly assumed that it would be best for everyone, including them, if Modbus became successful in the marketplace. Because of this thinking, Modbus became the first widely accepted fieldbus standard. In a short time, hundreds of vendors implemented the Modbus messaging system in their devices and Modbus became the de facto standard for industrial communication networks.
- **Modbus Uses Standard Transports** – The transport layer for Modbus remote terminal unit (RTU) commands is simply RS-485, a differential communication standard that supports up to 32 nodes in a multi-dropped bus configuration. The RS-485 standard provided noise immunity that was superior to that in the RS-232 electrical standard.

The transport layer for Modbus TCP commands is TCP and only TCP.

- **Modbus is a Simple Protocol** – Modbus is quite easy to understand (see Figure 8-1). Its primary purpose is to simply move data between an RTU master device (a *client* in Modbus TCP) and one or more RTU slave devices (*servers* in the Modbus TCP world). There are only two kinds of data to move, register data, and coil data. Registers are 16-bit unsigned integers. Coils are single bits.

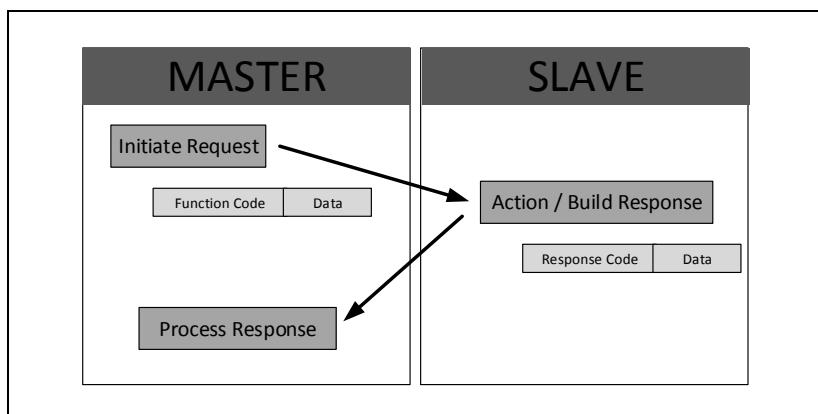


Figure 8-1. RTU Master/RTU Slave Modbus Architecture

Modbus uses a straightforward request/response command structure. A Modbus master requests or sends data to a slave and the slave responds. There are simple commands to read a register, read a coil, write a register, and write a coil

Modbus TCP and Modbus serial use *exactly* the same byte sequences to implement the command / response. The typical components of a Modbus message are presented in Table 8-1.

Table 8-1. Modbus Message Components

Function Code (FC)	The function code identifies the request to the Modbus slave. There are a large number of possible message requests, but about eight that are commonly used. These are the function codes that are detailed in this chapter.
Starting Address	The starting address is the index into the data area in the Modbus device. If the function code targets coils, this field specifies the index into the coils (bits) of the coil address space. If the function applies to registers, this field specifies the index into the registers for that part of the address space. Note: Modbus address spaces are one-based—the first register or coil is one. The Modbus protocol is zero-based. The first register or coil is zero. The address on the wire is always one less than the address in the Modbus data request.
Bit Length	The number of bits to read or write.
Word Count	The number of registers to read or write.
Byte Count	The number of data bytes included in the message request or response.
Response Code	This byte indicates the successful completion of the message request. It is identical to the original message request.
Exception Response (FC)	An exception response is indicated by combining the response code of the original Modbus function request with 80 hexadecimal. For example, a Modbus exception response to function code 3 is 83 hexadecimal. A single data byte value with the Modbus error code always follows the exception response byte.

For Modbus TCP, this set of message components is inserted as the data bytes of a standard TCP message as shown in Figure 8-2.

Modbus messages can be encoded, meaning turned into a series of bits, in one of two ways: Modbus ASCII or Modbus RTU. Modbus ASCII is a relic of the days of teletypes; every

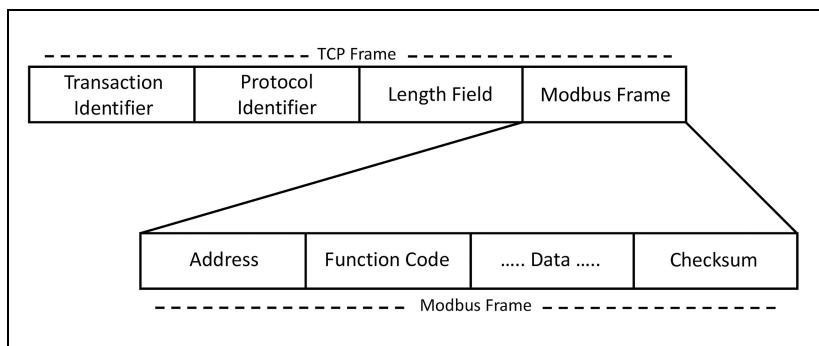


Figure 8-2. Format of a Modbus/TCP Frame (Courtesy Schneider Automation, www.modbus.org)

byte is transmitted as two ASCII characters. Few devices today use Modbus ASCII. Modbus RTU, on the other hand, is very popular and almost all Modbus serial and Modbus TCP devices use it. Modbus RTU encodes each byte of a message as a binary data value, which greatly enhances performance over Modbus ASCII. Modbus TCP devices always use Modbus TCP.

Modbus on a *serial* network is not fast—response times of a fraction of a second are not at all uncommon. Which, of course, is why Ethernet is an attractive alternative to serial—10, 100, or even 1,000 Mb performance is possible. Also, the simple Modbus protocol does not support complex objects and sophisticated device profiles. The master/slave orientation does not prevent peer-to-peer communication, but it requires separate “sessions” to be opened up between devices.

The power of Modbus has always been its simplicity. Modbus fit well in the era of limited RAM and FLASH. It required little code space (FLASH), often as little as 1K. Memory (RAM) varies with the size of the Modbus data space that you needed to represent the device’s data. Simple automation devices with little bits of data—imagine a photo eye—could be implemented with hardly any RAM space. These devices could now, for the

first time, send their data to a control system as part of a daisy-chained 485 network, avoiding hardwired point-to-point communications.

The simplicity of Modbus has been both a blessing and a curse over the years. The simplicity has led to an incredible amount of activity and propagation of Modbus into many different industries around the world. There is probably no product category in the last 40 years that has not had an offering without Modbus.

The simplicity of Modbus has also led to many companies expanding the message structure, data representation, and transports. Some vendors have imposed any number of advanced structures and data types on the basic Modbus address structure. Others have used Modbus in other ways that go beyond the basic specification. These implementation extensions are not expressly prohibited by the specification, but they do not always make Modbus easily portable to many different applications.

8.3 EtherNet/IP

EtherNet/IP is an industrial Ethernet application layer protocol used by Rockwell Automation (Allen-Bradley) programmable controllers. EtherNet/IP uses standard Ethernet to organize the task of configuring, accessing, and controlling industrial automation devices. What does that mean? It means that EtherNet/IP is the highly structured protocol that uses Ethernet to move inputs from industrial end devices into an Allen-Bradley programmable controller and moves outputs generated by the control logic of an Allen-Bradley programmable controller to devices that map those outputs to real world physical outputs.

EtherNet/IP is based on the Control and Information Protocol (CIP) used in DeviceNet, CompoNet™, and ControlNet™. CIP provides a common, standardized mechanism for representing data, sending messages, and defining common device types for the component technologies that use the CIP core protocol. CIP is a media-independent protocol, which means that CIP messages can be sent over any communication media including CAN, Ethernet, and even something like FireWire. Sending CIP messages over CAN forms the basis for the DeviceNet protocol. Sending CIP messages over the ControlNet communication bus is the basis for ControlNet. Sending CIP messages over Ethernet TCP and UDP is the basis for EtherNet/IP. CIP provides the core technology used in each of these application layer protocols.

CIP defines two kinds of messages: explicit and implicit. Explicit messages are asynchronous, request/response type messages. A sender builds a request and sends it to a receiver. The receiver receives the request, opens it, decodes it, and sends a response. It is the traditional mechanism for communication between two devices. Implicit messages are synchronous messages that are continuously passed back and forth between the sender and receiver. Unlike explicit messages, the contents of implicit messages are simply raw data. Both the sender and the receiver have to have prior knowledge of how to construct and decode that raw data. How the sender and receiver map that implicit data is described later in this section.

The CIP protocols—EtherNet/IP, ControlNet, and DeviceNet—all define a type of controller device and some type of end device. Unlike other CIP protocols that use the terms master and slaves, the “master” device in EtherNet/IP is labeled a *scanner* and end devices, instead of slaves, are labeled as *adapters*. Scanners, typically programmable controllers, open connections with adapters, configure the timing of the asyn-

chronous implicit messaging with the adapters, and send explicit messages to adapters when needed. Adapter devices are typically industrial I/O devices, such as valves, I/O blocks, drives, scales, meters, and other end devices you might find in an automation system. An adapter has one job: send the scanner an implicit message with the status of its real world inputs and set its real world outputs as directed in the implicit output message received from the scanner.

EtherNet/IP uses TCP/IP for explicit messaging. Explicit messages (messages that are sent asynchronously) are sent over TCP. Examples of explicit messages include: changing the ramp time on a drive, setting a tare weight on a scale, and reading a barcode using TCP as the initiator of the message. By using TCP, the initiator automatically gets delivery acknowledgement for these important messages. On the other hand, implicit messages (messages that are delivered synchronously) are sent over UDP because they do not require delivery notification. By definition, a lost synchronous message is going to be replaced quickly by the next message in the sequence.

One of the most important features of EtherNet/IP (and CIP in general) is how it models device data in adapter devices. EtherNet/IP devices—in fact all CIP devices—are modeled as a collection of objects, each containing related data (a model of an EtherNet/IP device is illustrated in Figure 8-3). Objects are composed of data values or *attributes* in CIP terminology. Attributes values can be assigned a type with any one of a large number of EtherNet/IP types to model the specific data in the device.

The object nature of EtherNet/IP does not imply that the device implements the object structure internally, only that the device looks to the EtherNet/IP network as a collection of objects each with one or more attributes. These attributes form

the available data that an EtherNet/IP device exposes to the outside world. Scanners can access these attributes using explicit or implicit messaging.

There are two kinds of objects in every EtherNet/IP device: required objects and application objects (see Figure 8-3).

Required objects must be present in every EtherNet/IP device while application objects are particular to the function of the end device. For example, every EtherNet/IP device must have an identity object, an Ethernet object, a TCP object, a router object, and a connection object. Each object provides attributes that describe the specific functionality of the device. The identity object, for example, presents identity information to the network by making available attributes like the vendor ID, the product code, the software revision, and other information that specifically identifies that device and its application. The TCP object provides information on the TCP connection like the TCP/IP address of the device. The connection object provides information on the current connections to a controller.

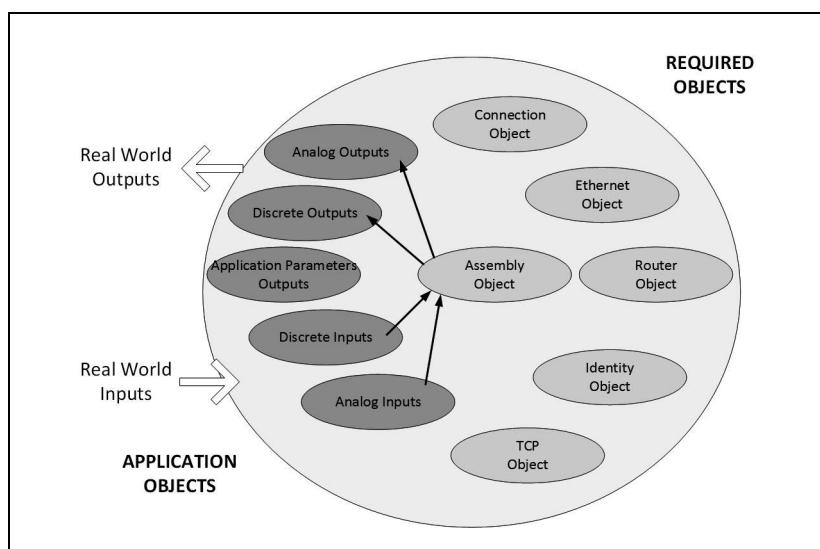


Figure 8-3. EtherNet/IP Object Representation

The object number and attribute numbers of required objects are predefined and identical in every EtherNet/IP device.

Object 1 is always the identity object, Object 2 is defined to be the router object and so on. Attributes for the required objects are also predefined. Attribute 1 of the identity object is always the vendor ID, Attribute 2 is the device type and so on. By pre-defining the object numbers and attribute numbers for all the required objects, a controller or a PC tool always knows exactly how to get specific information about an EtherNet/IP device or, in actuality, any CIP device.

Application objects are the set of objects that model the I/O data of the adapter device. The set of application objects can be simple or complex. The object model for a simple device like an 8-channel valve might simply be one application object with one 8-bit attribute containing the current status of the valve states and one 8-bit attribute containing the commanded state of each valve as currently specified by the scanner. For a more sophisticated device, like a motor drive, there might be tens or even hundreds of objects to provide access to all the functionality of that device. The complexity of the object model in an EtherNet/IP device is directly related to the complexity of the data being exposed to the network through the object interface.

These application layer objects are predefined for a large number of common device types. All CIP devices with the same device type (drive system, motion control, valve transducer, etc.) must contain the identical series of application objects. The series of application objects for a particular device type is known as the *device profile*. A large number of profiles for many device types have been defined. Supporting a device profile allows a user to easily understand and switch from a vendor of one device type to another vendor with that same device type.

A device vendor can also group application layer objects into assembly objects (Figure 8-4). These super objects contain attributes of one or more application layer objects. Assembly objects form a convenient package for transporting implicit messages between devices. For example, a vendor of a temperature controller with multiple temperature loops may define an assembly for each temperature loop and an assembly with the data for all temperature loops. The user can then pick the assembly that is most suited to the application.

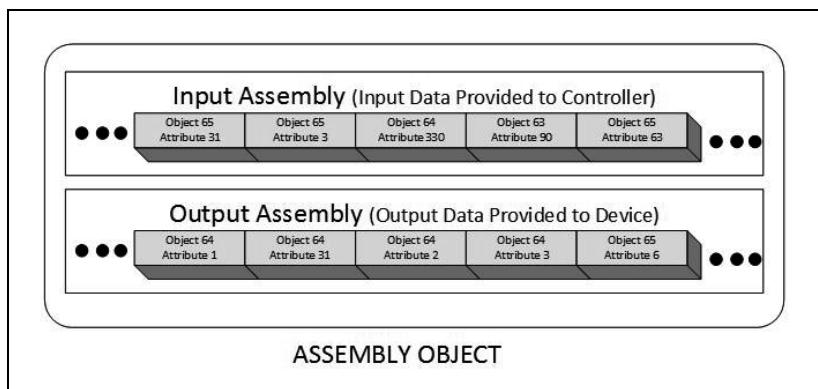


Figure 8-4. Assembly Object Structure

Assemblies are what is transferred in the implicit message. The input assembly is the set of attributes that are delivered to the scanner each time the implicit message is triggered. The output assembly is the set of attributes that are received from the scanner on each implicit output message. The contents of these assemblies are specified in an EDS or Electronic Data Sheet. The EDS can be used by the engineer configuring the controller to assemble the data to deliver in the output assembly and decode the data received in the input assembly. Another mechanism to decode the implicit message assemblies is the Add-On Profile (AOP). The AOP is a way of electronically configuring a

Rockwell Controller to know how to encode and decode messages for a specific device.

The Open Device Vendor Association (ODVA), headquartered in Ann Arbor, Michigan, is the vendor trade association that manages all CIP technologies, including EtherNet/IP. ODVA members, some of the world's leading automation companies, work to advance the development of CIP technologies and promote interoperability among vendor devices. One of the most important jobs of the association is conformance testing. Vendors manufacturing EtherNet/IP devices must submit each new device for conformance testing at the ODVA test lab. In the test lab, each device is exercised independently and in a rack containing a multitude of other vendor devices. The long sequence of tests verifies not only that the device adheres to the ODVA specification, but that it interoperates with other EtherNet/IP devices from other manufacturers. Once certified, the manufacturer can exhibit the conformance logo (Figure 8-5) indicating to users that the device is certified.

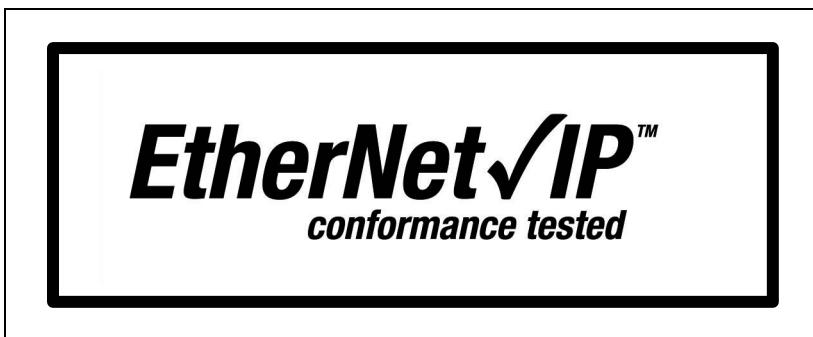


Figure 8-5. EtherNet/IP Conformance Tested Logo

EtherNet/IP is a widely implemented protocol with numerous advantages. First, Ethernet/IP uses the tools and technologies of traditional Ethernet. It uses all the transport and control protocols of standard Ethernet including the Transport Control

Protocol (TCP), the User Datagram Protocol (UDP), and the media access and signaling technologies found in off-the-shelf Ethernet. Building on these standard IP technologies means that EtherNet/IP works transparently with all standard off-the-shelf Ethernet devices (switches, routers, diagnostic tools, etc.) found in today's marketplace. It also means that EtherNet/IP is easily supported on standard PCs and all their derivatives. But even more importantly, because EtherNet/IP is based on a standard technology platform, EtherNet/IP will move forward as the base technologies evolve in the future. Secondly, as discussed above, Ethernet/IP is a certifiable standard. Devices are tested in a lab to verify that they meet the EtherNet/IP standard, which ensures interoperability between devices from multiple vendors and the consistency and quality of field devices. This ensures the consistency and quality of field devices. Third, EtherNet/IP is built on the widely accepted CIP protocol layer. Finally, and most importantly, EtherNet/IP is the industrial application layer protocol that is used by Rockwell Logix programmable controllers to communicate with Ethernet-enabled field devices. With Rockwell programmable controllers having a significant share of the programmable controller market in North America, EtherNet/IP will continue to dominate the industrial application landscape for years to come.

8.4 PROFINET

This is the PROFIBUS Trade Organization's answer to the need for interoperability between automation devices and subsystems that are linked together via Ethernet.

To understand what PROFINET is, you must understand what it is not. PROFINET is not the PROFIBUS protocol on Ethernet in the same way that Modbus/TCP is the old familiar Modbus

on Ethernet. PROFINET is not really a “fieldbus” as the term is normally understood, either.

PROFINET is not even Ethernet-specific; it links via TCP/IP and occupies layers 3 and above in the ISO/OSI model. Other physical layers, such as modems, WANs, VPNs, or the Internet may be employed so long as a PROFINET device is linked to the network via TCP/IP. An analogy to the office environment may help you understand what it is intended to do.

The PC in your office at work is networked with a dozen other PCs and a file server. Your office LAN (Ethernet 100BASE-T) is also linked to a T1 Internet line. You open Microsoft Word and create a complex document. You write some text and create some tables. Your coworker Jeff has a PowerPoint presentation on his PC; you open it via the network and copy and paste two graphics images into your Word document—the images are transferred intact as objects. Your other coworker Leslie has an Excel spreadsheet that you also open remotely and embed in your document—it is as simple as cutting and pasting. In this case, the Excel data is not static, it is live. Leslie updates this spreadsheet every Tuesday, and every time you open your document it will retrieve the latest data from her document on her PC. Finally, you access the Internet, copy and paste text and graphics from one website to your document, and then insert hyperlinks to other websites.

Behind this transparency among applications is a very complex object model created by Microsoft. Savvy PC users are accustomed to this level of sophistication and its benefits. This expectation naturally extends to the integration of business applications throughout an entire company and, of course, to devices in an automation system. This is the expectation that

PROFINET was engineered to satisfy. The OLE¹ for Process Control (OPC) software standard (www.opcfoundation.org) was developed to create transparency between hardware devices (e.g., network and I/O cards) and software applications (operator interface and programming tools). PROFINET uses components of OPC (COM and DCOM) and extends this transparency to all devices on a TCP/IP network, further defining object models for many kinds of device and programming parameters.

Rather than being specific to only one manufacturer's hardware or software (as is often the case with Microsoft), PROFINET is an industry standard available to all PROFIBUS members. PROFINET is an open communications and multi-vendor engineering model. This means that a preconfigured, preprogrammed, and pretested machine such as a transport conveyor can be set up using the vendor-specific electrical devices and applications as it has been in the past.

With PROFINET, the entire vendor-specific module (machine, electrical, and software) is represented as a vendor-independent PROFINET component. This PROFINET component is described within a standardized XML file that can be loaded into any PROFINET engineering tool, and interconnections between the PROFINET objects can be established by connecting lines from object interface to object interface.

In regards to communication and physical topology, established protocols such as TCP/IP, RPC, and DCOM are used. Data access to the PROFINET objects is standardized via OPC. As for physical device connections, not only can devices be connected via an integrated PROFINET interface, but existing

1. OLE stands for Object Linking and Embedding, a standard developed by Microsoft.

intelligent devices that are currently used with fieldbus networks, such as PROFIBUS, can be connected to Ethernet through a gateway device called a PROFINET *proxy server*.

Every PROFINET object is described by an XML file that defines these parameters so that every defined data type in the system is accessible by name throughout the PROFINET network. Integrators do not have to link devices at the bit level. It is expected that PROFINET proxies for each different fieldbus system (PROFIBUS, DeviceNet, Modbus, ControlNet, and others) will be developed over time, extending the transparency of large systems.

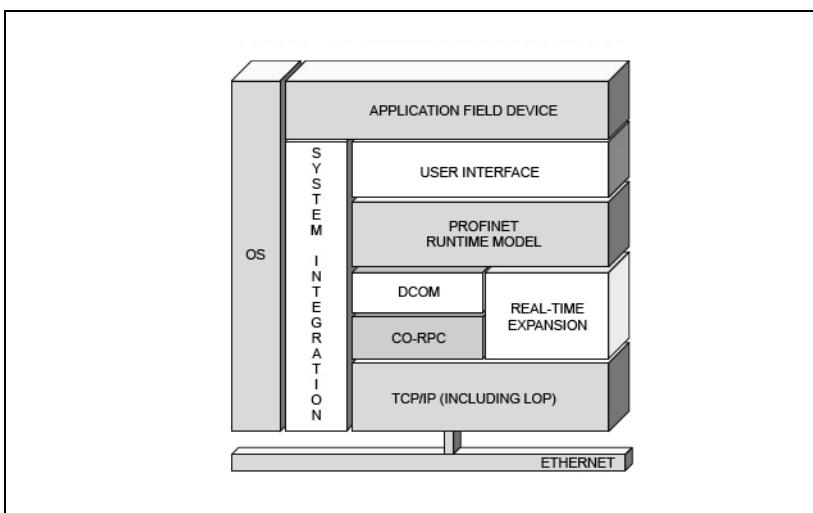


Figure 8-6. The Communication Layers of PROFINET

To delve into the internals of PROFINET as described in Figure 8-6 is beyond the scope of this book. However, more information is available at www.PROFIBUS.com, and PROFIBUS organization members can download the specification and source code at the site.

8.5 FOUNDATION Fieldbus High-Speed Ethernet

This protocol uses the FOUNDATION Fieldbus H1 process control protocol on TCP/IP. FOUNDATION Fieldbus H1 is a sophisticated, object-oriented protocol that operates at 31.25 Kbps on standard 4–20 mA circuits. It uses multiple messaging formats and allows a controller to recognize a rich set of configuration and parameter information (device description) from devices that have been plugged into the bus. FOUNDATION Fieldbus even allows a device to transmit parameters relating to the estimated reliability of a particular piece of data. FOUNDATION Fieldbus uses a scheduler to guarantee the delivery of messages, so issues of determinism and repeatability are solidly addressed. Each segment of the network contains one scheduler.

FOUNDATION Fieldbus high speed Ethernet (HSE) is the same as the H1 protocol, but instead of 31.25 Kbps, it runs on TCP/IP at 100 Mbps. It provides the same services and transparency of network objects but operates at a higher level.

FOUNDATION Fieldbus is specifically focused on the process control industry and will likely be the dominant Ethernet I/O standard there.

Installations in this segment of the world typically have the following characteristics:

- Very large campuses (e.g., chemical refineries) with many nodes
- Data does not have to move quickly, but there is a lot of it to move (large packets)
- Large quantities of analog data
- Hazardous area classifications such as Class I, Division 2



Week 6

Week 6

Week 6

Week 6

Week 6

Week 6



Setting the Standard for Automation™

ISA/IEC 62443 Models

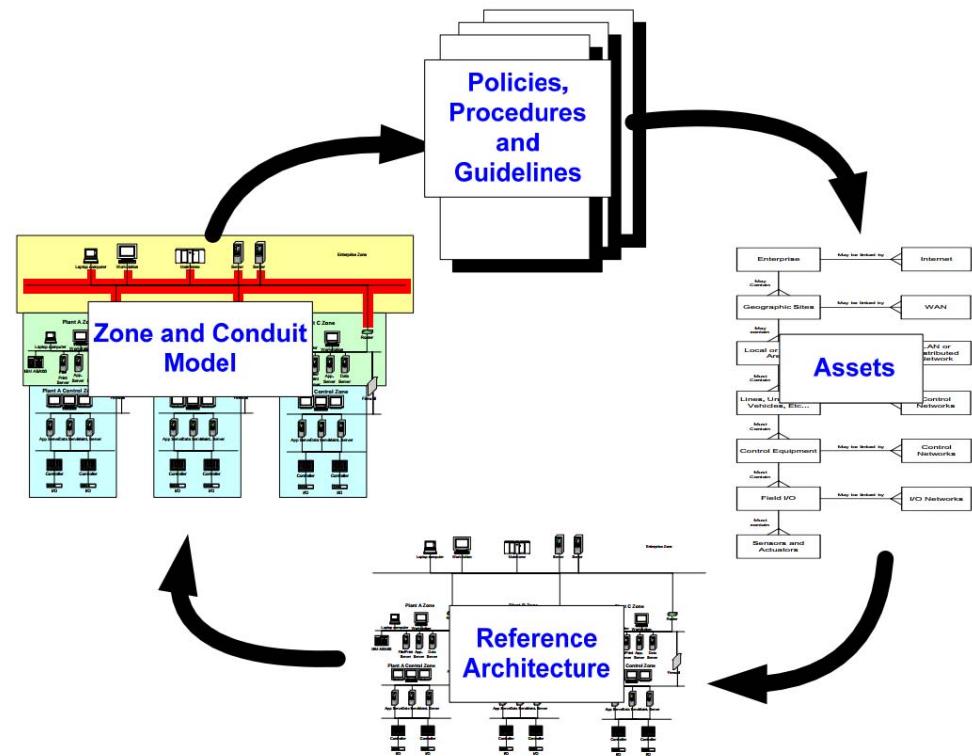
Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Models

- Reference models provide the overall conceptual basis
- Asset model describes relationships between assets within an industrial automation and control system
- Reference architecture describes the configuration of assets
- Zone model groups reference architecture elements according to defined characteristics (zone and conduits)
- This provides a context for the definition of policies, procedures, and guidelines, applied to the assets
 - ANSI/ISA-62443-1-1, clause 6, page 69

ISA99 Model Relationships

- Policies, Procedures and Guidelines
- Assets
- Reference Architecture
- Zone and Conduit Model
- Related to one another
- Make up a security program



Reference Model Levels

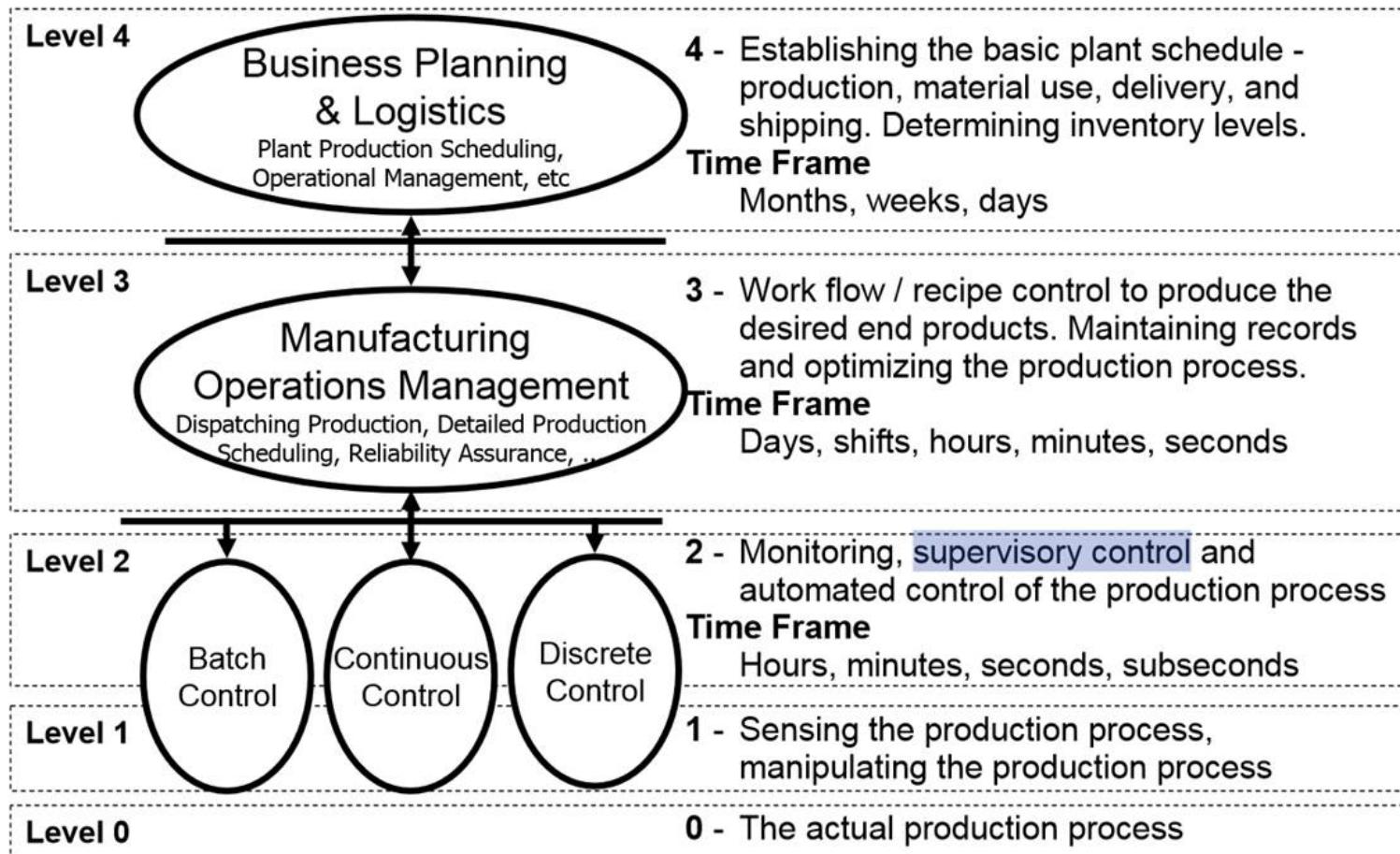
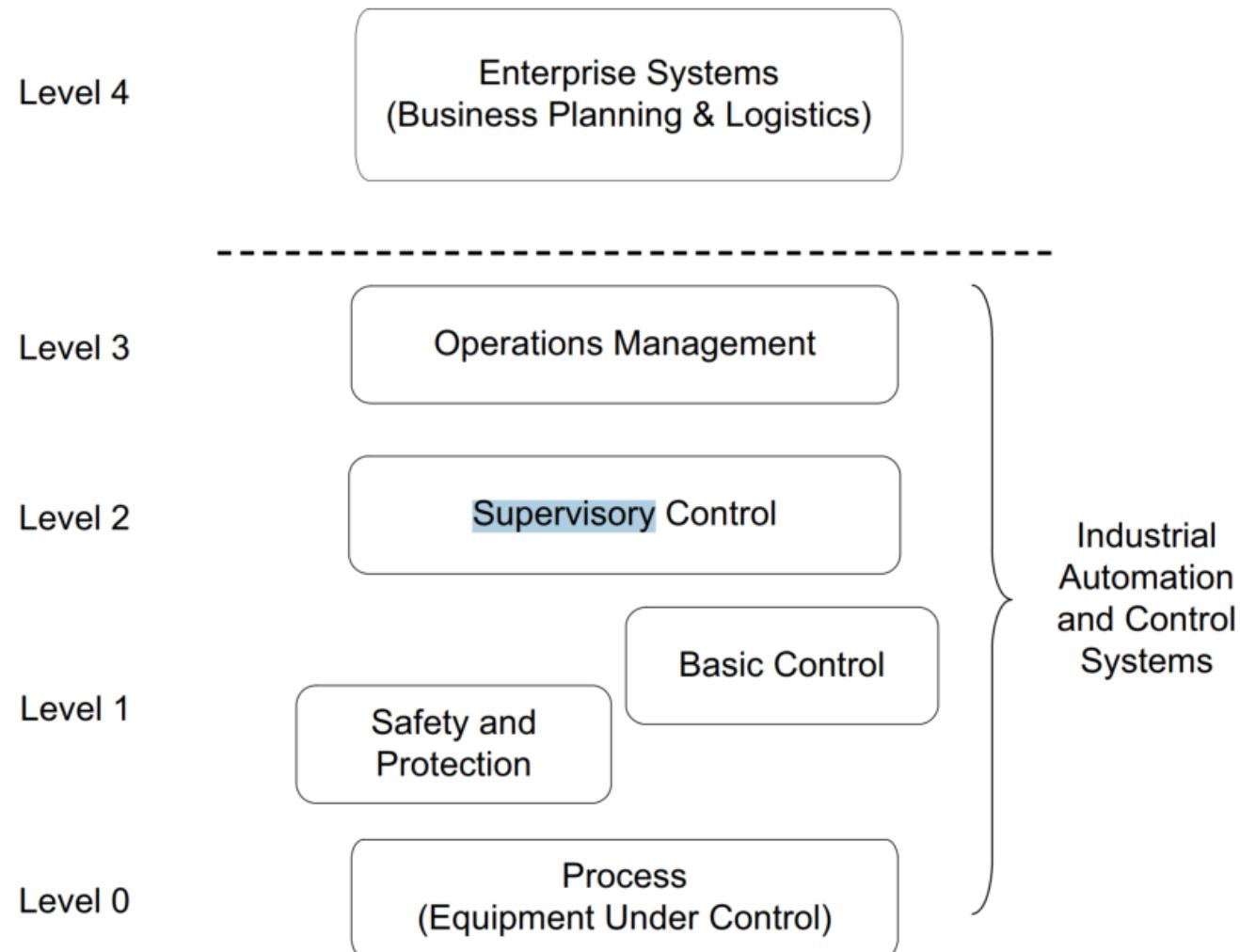


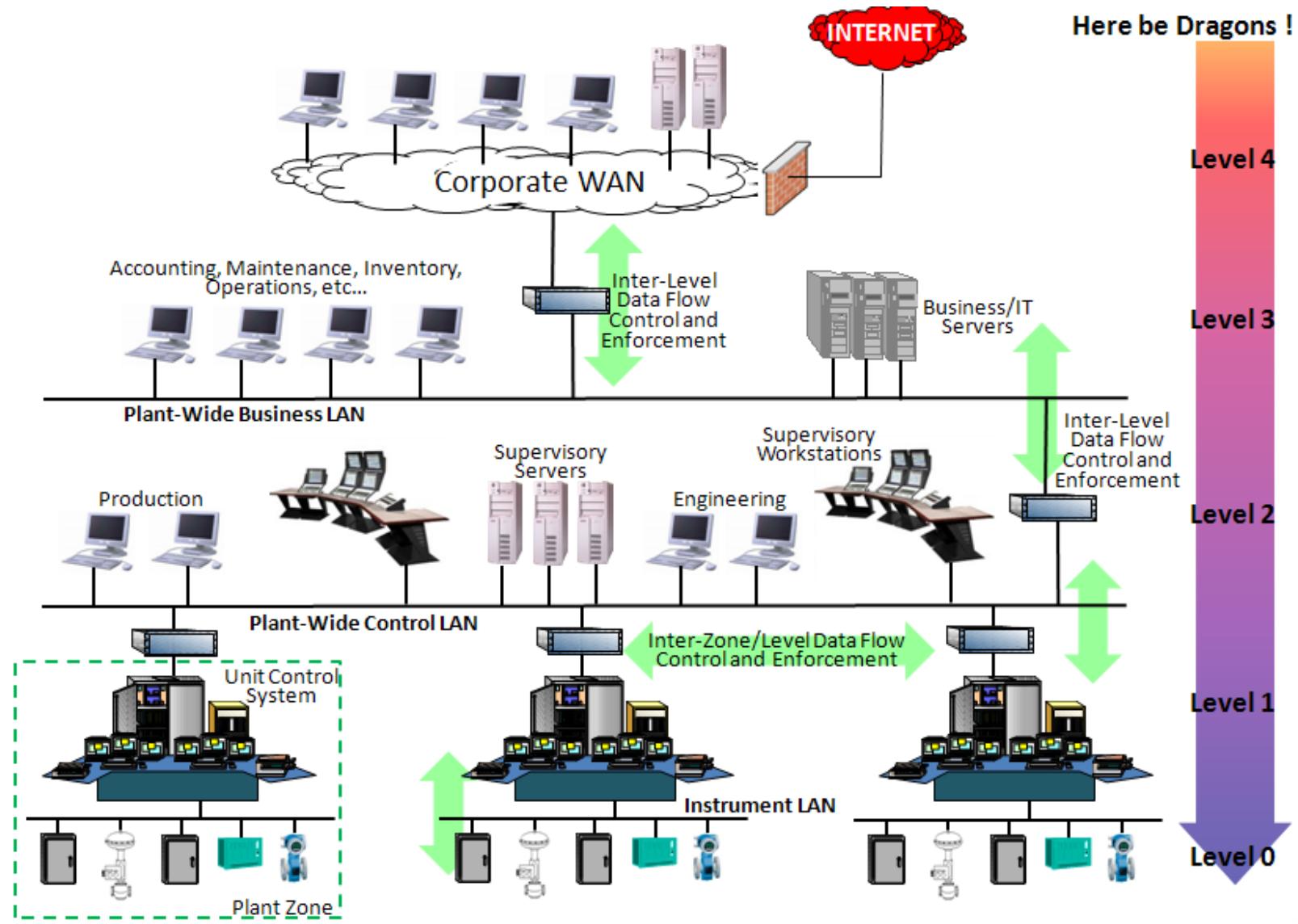
Figure 3 – Functional hierarchy

ANSI/ISA-95

Reference Model for ISA99 Standards



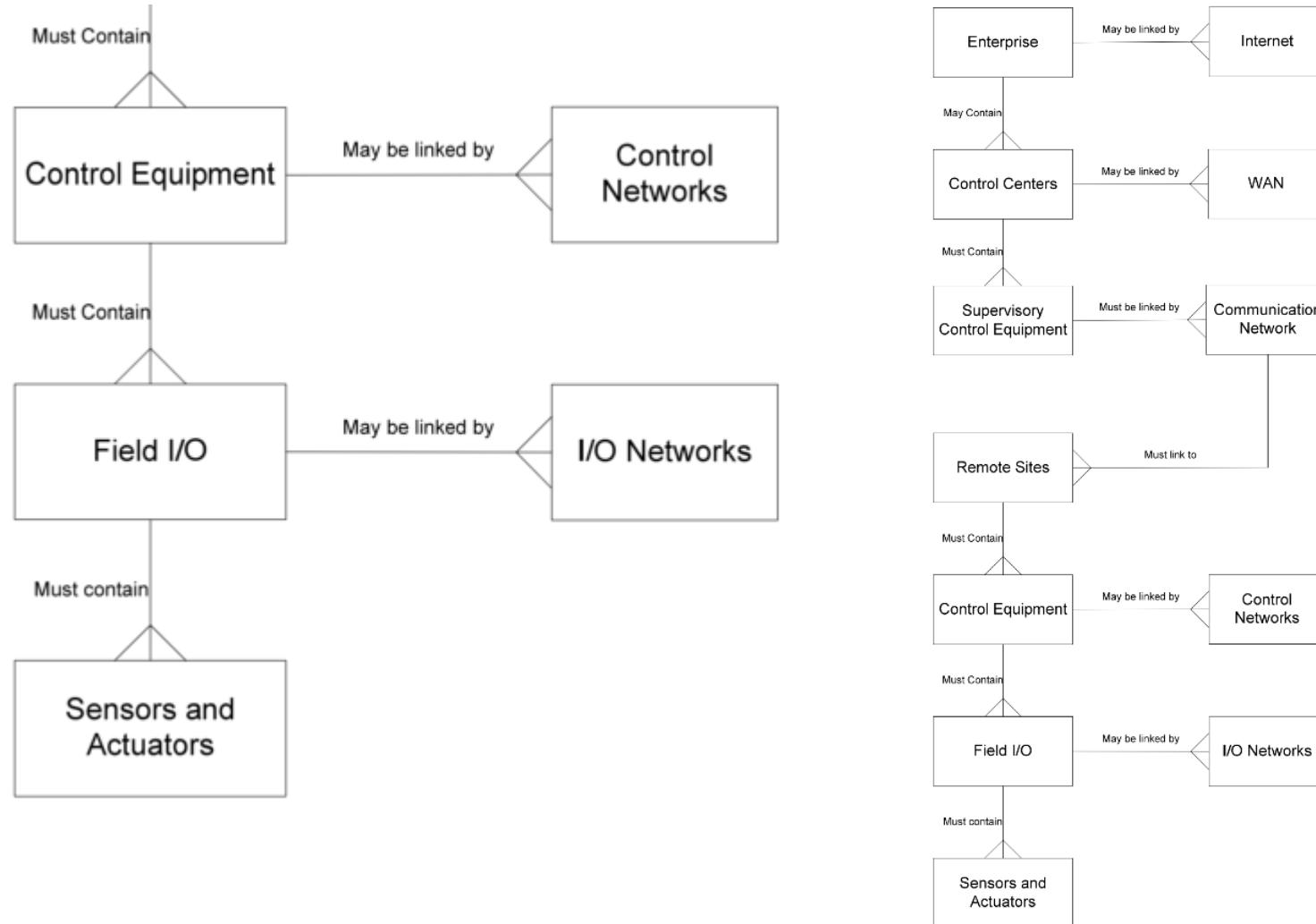
Generic Reference Model



Asset Models

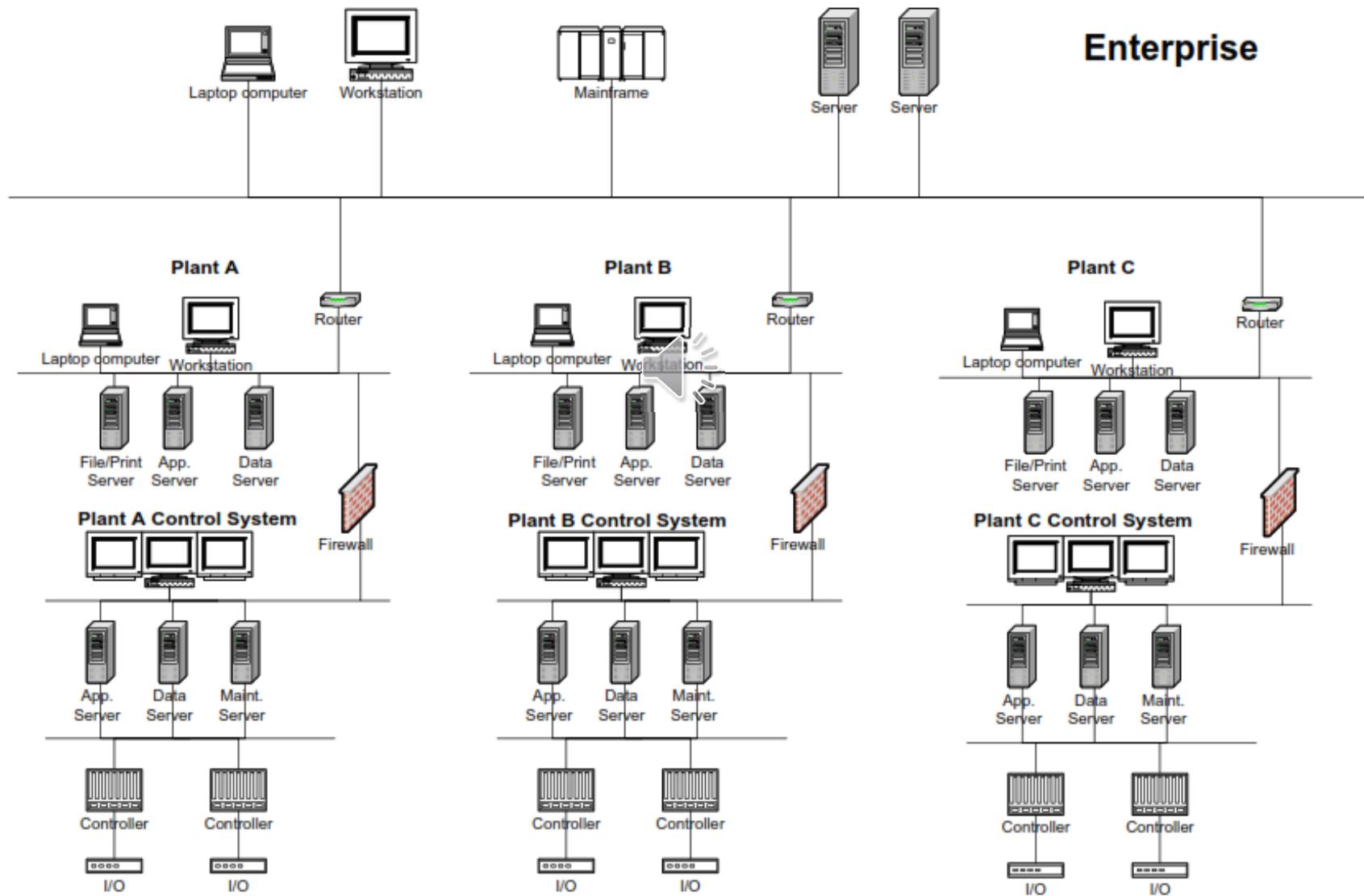
- Asset model starts at a high level
- Includes all ANSI/ISA-95 Level 0, 1, 2, 3, 4 equipment and information systems
- Explicitly includes networks and ancillary equipment
- Generic enough to fit the many situations where control systems are deployed

Asset Model SCADA system example



Refer to ANSI/ISA-62443-1-1, Figure 15, page 75

Reference Architecture Example



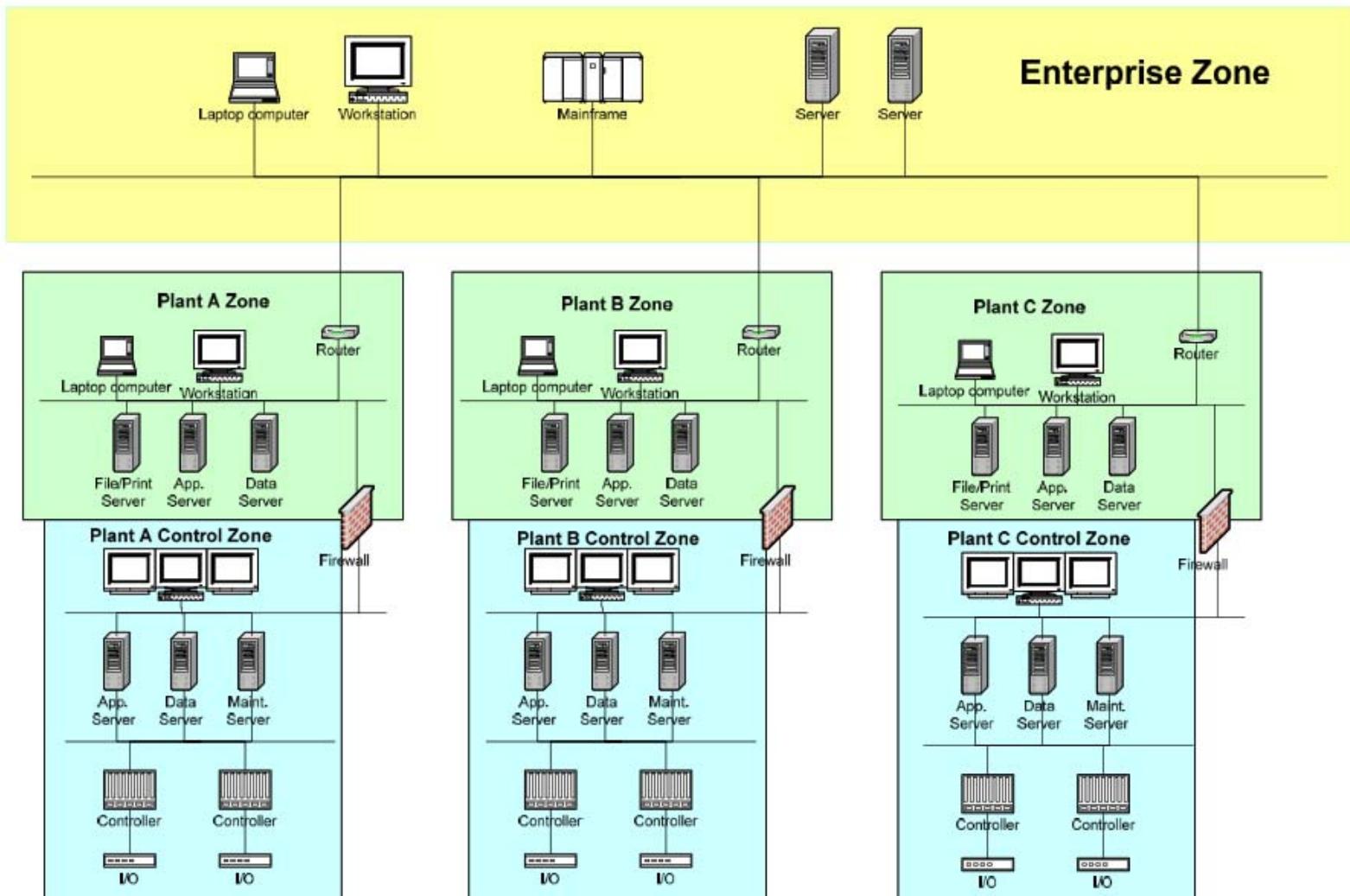
Security Zones

- Security zone is a logical grouping of physical, informational, and application assets sharing common security requirements
- There can be zones within zones, or subzones, that provide layered security, giving defense in depth and addressing multiple levels of security requirements
- A security zone has a border, which is the boundary between included and excluded elements
- Security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone

Security Zones

- Trusted definition
 - Confidence that an operation or data transaction source, network or software process can be relied upon to behave as expected
 - Attribute of an entity that is relied upon to a specified extent to exhibit an expected behavior
- Untrusted definition
 - Not meeting predefined requirements to be trusted
 - Entity that has not met predefined requirements to be trusted
 - Entity may simply be declared as untrusted.
- Zones can be defined
 - Physically (physical zone)
 - Logically (virtual zone)

Security Zone Model



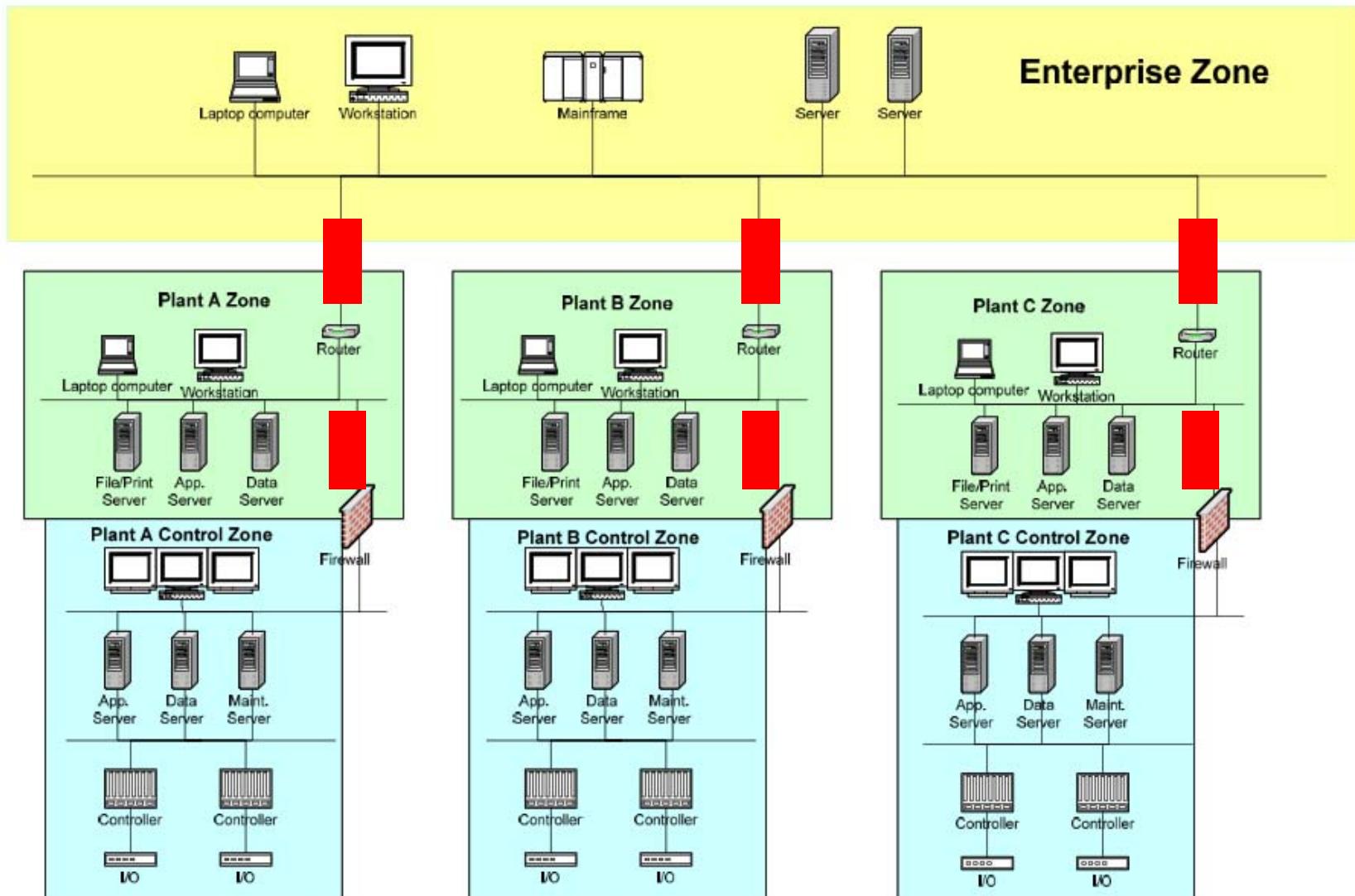
Conduits

- Conduit is a logical grouping of communication assets that protects the security of the channels it contains
 - Similar to how physical conduit protects cables from physical damage
- Stated another way
 - logical grouping of communication channels, connecting two or more zones, that share common security requirements
- Trusted conduits crossing zone boundaries must use an end-to-end secure process
- Physical devices and applications that use the channels contained in a conduit define the conduit end points
- Can be defined physically or logically

Conduits

- Physically a conduit can be cable or wireless that connects zones for communication purposes
- A conduit is a type of zone that cannot have subzones
 - Conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone
 - Can be trusted or untrusted
- Conduits are defined by the list of all zones that share the given communication channels
- It can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carrier
- Conduit is the wiring, patch panels, black boxes, hubs, media converters, routers, switches, and network management devices that make up the communications path under study

Conduit Model



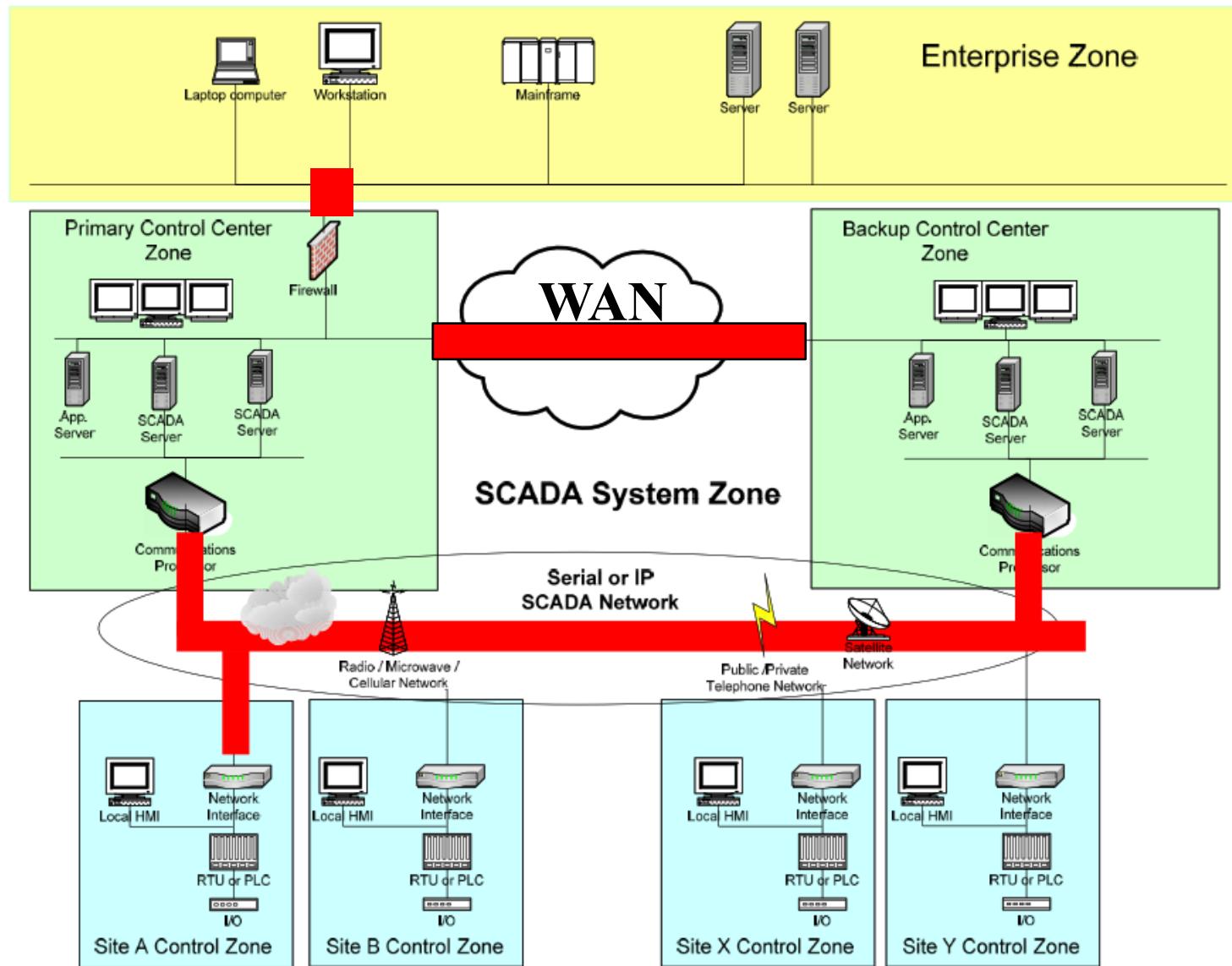
Zone & Conduit Characteristics

- Name and/or Unique Identifier
- Accountable organization(s)
- Definition of logical boundary
- Definition of physical boundary
- Safety designation
- Connected zones or conduits
- SL-T

Zone & Conduit Characteristics – cont'd

- Applicable security requirements
- Applicable security policies
- Assumptions and external dependencies
- List of logical access points
- List of physical access points
- List of data flows
- List of assets

Zone & Conduit Models



Recap

- Differences between IT and IACS
- Defense-in-Depth
- Security Zones & Conduits



Setting the Standard for Automation™

Network Segmentation

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Business/Process Firewall Architectures

- Between plant floor and the rest of the company networks a firewall is a must
- Do not try to use a router to prevent hackers/viruses entering – it isn't good enough.

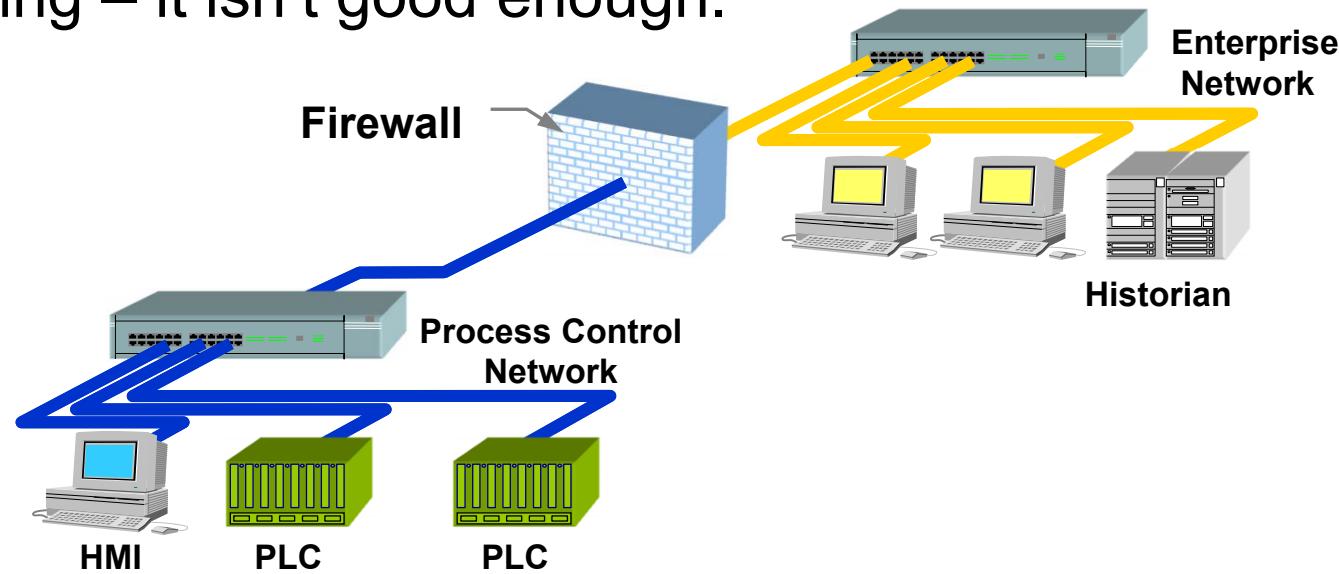
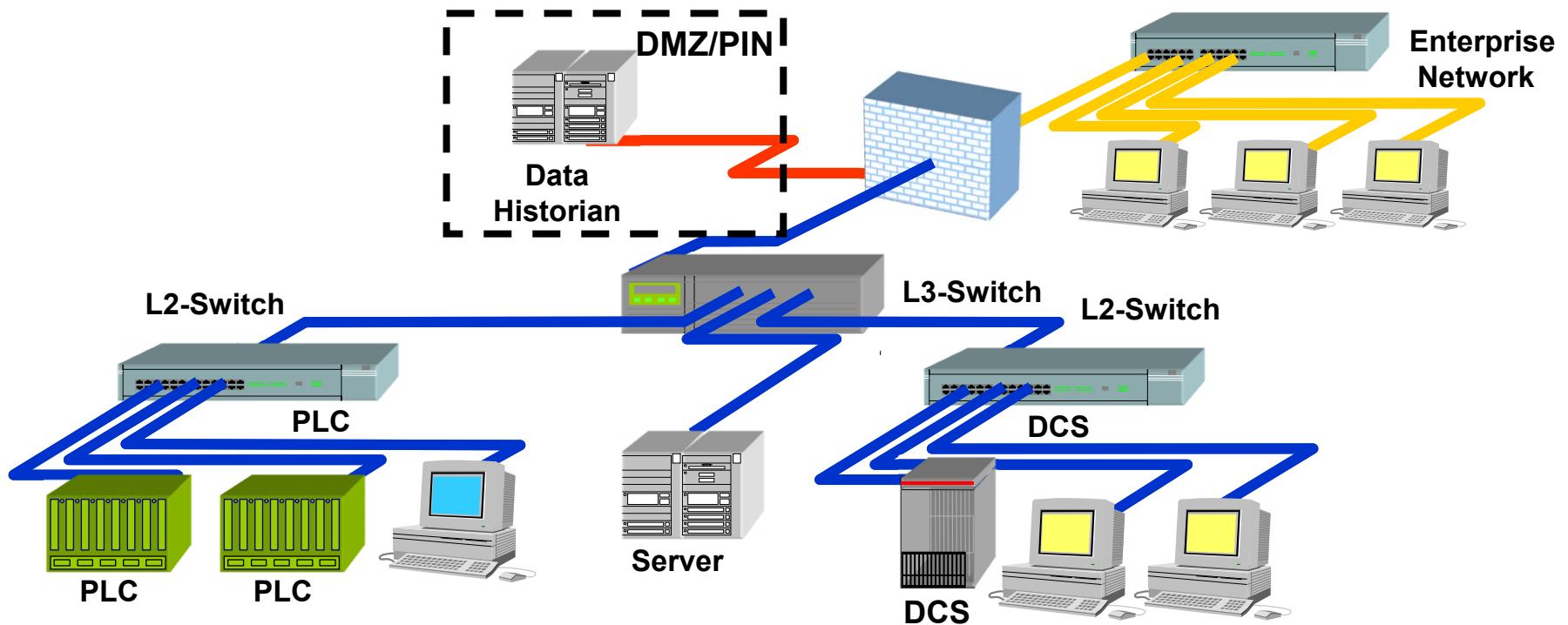


Image Courtesy of CPNI

Business/Process Firewall Architectures

- Much better is the use of a Demilitarized Zones (DMZ) between the enterprise and process control networks.
- This three-tier design allows secure data transfer between systems.



NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control

<https://www.energy.gov/oe/downloads/good-practice-guide-firewall-deployment-scada-and-process-control-networks>

Defense-in-depth firewall architectures

- Distributing security appliances provide defense in depth to key assets like controllers

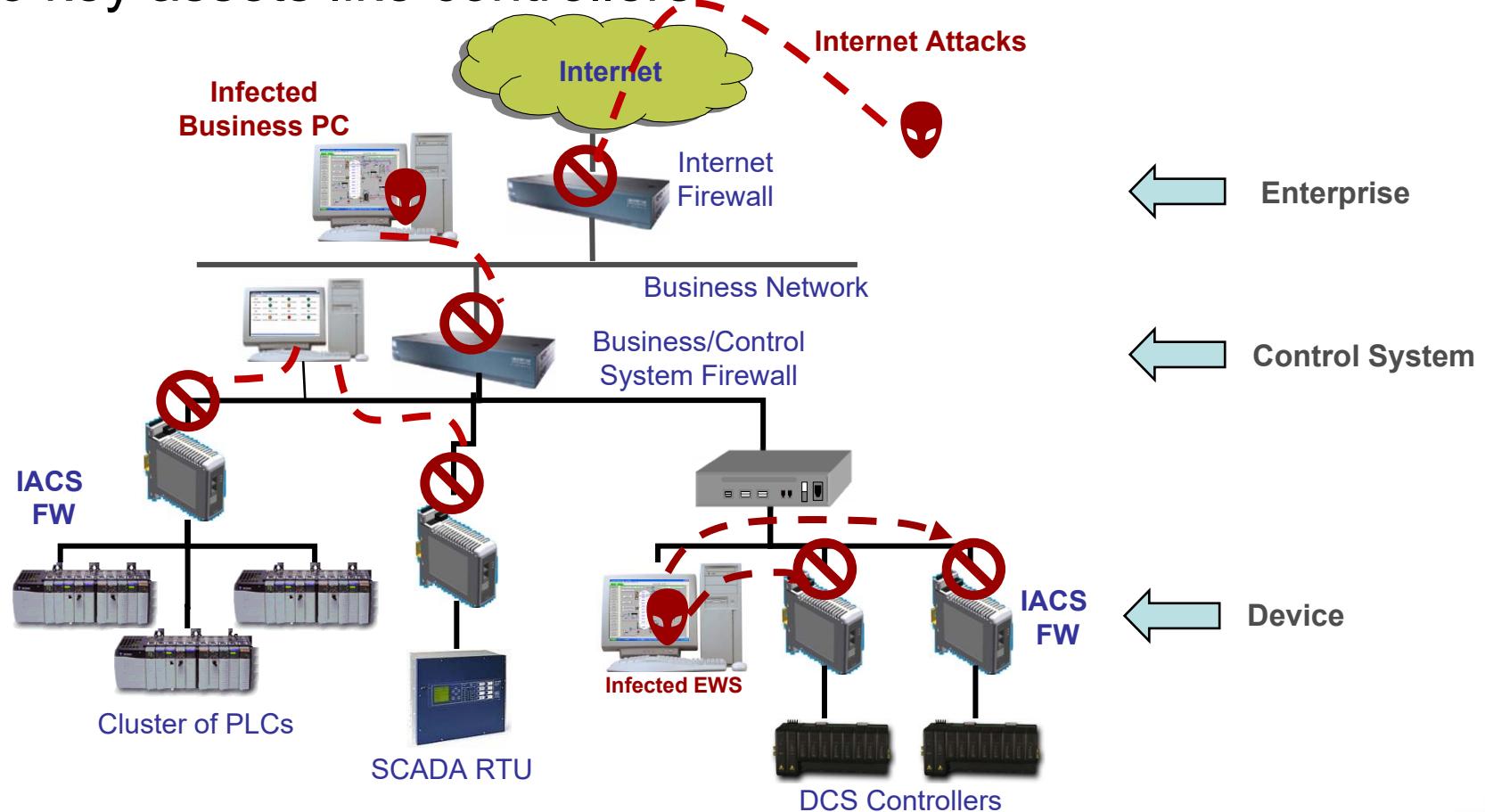
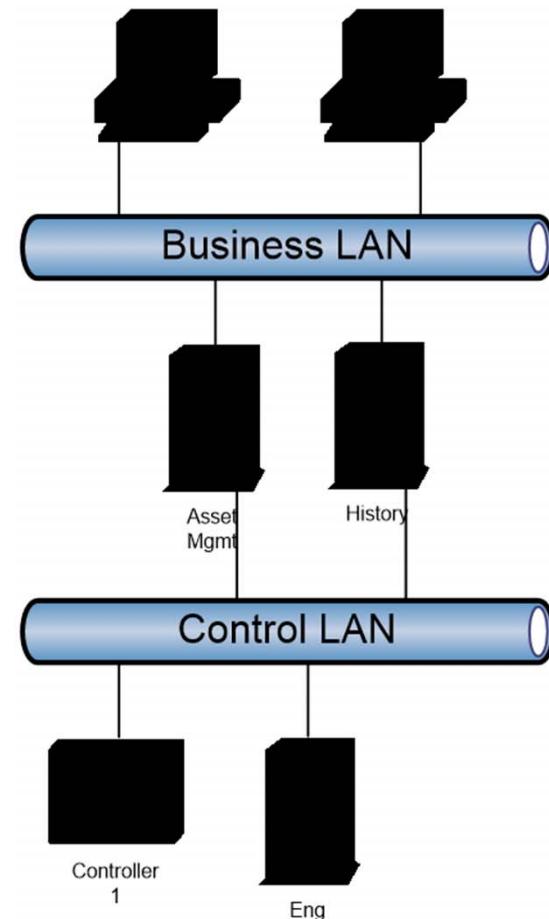


Image Courtesy of MTL Instruments

Comparing Various Architectures

- Dual-homed computers
- Access vulnerabilities -Bridged LANs
- Routers/Firewalls
- Firewall with DMZ

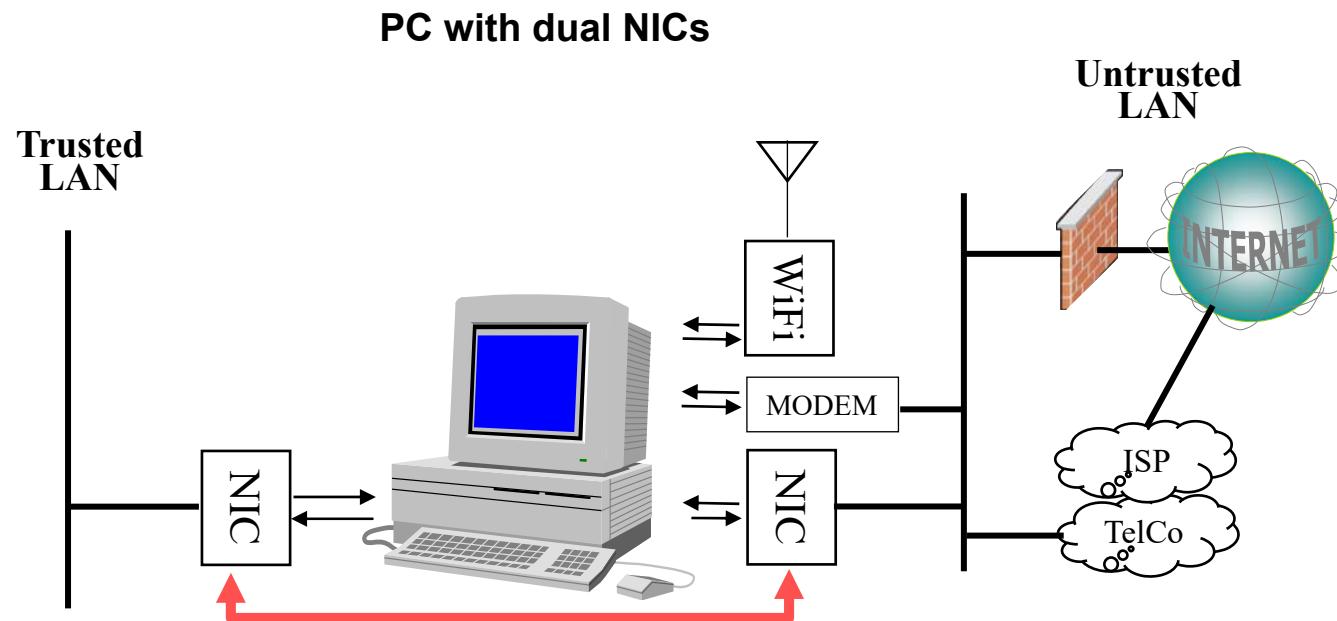
Dual-homed Computers



Dual-Homed Computers

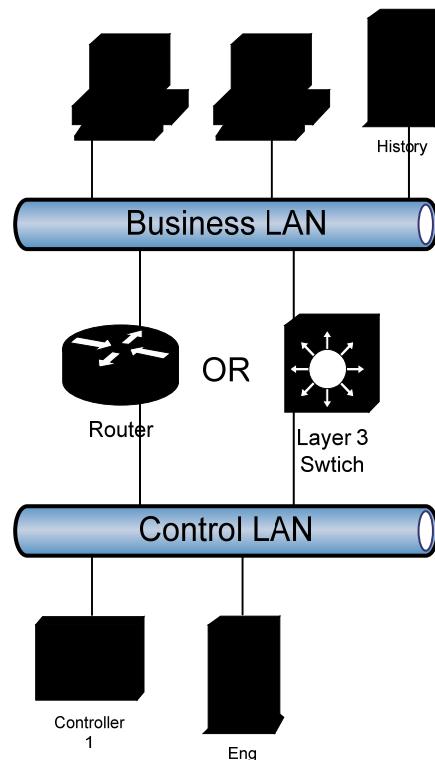
Access Vulnerabilities – Bridged LANs

- A network bridge joins two independent networks



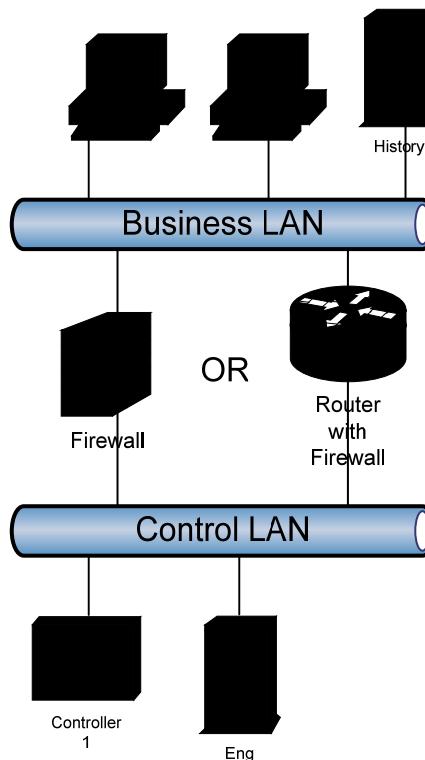
- Layer 1 and Layer 2 route between independent networks

Routers / Firewalls



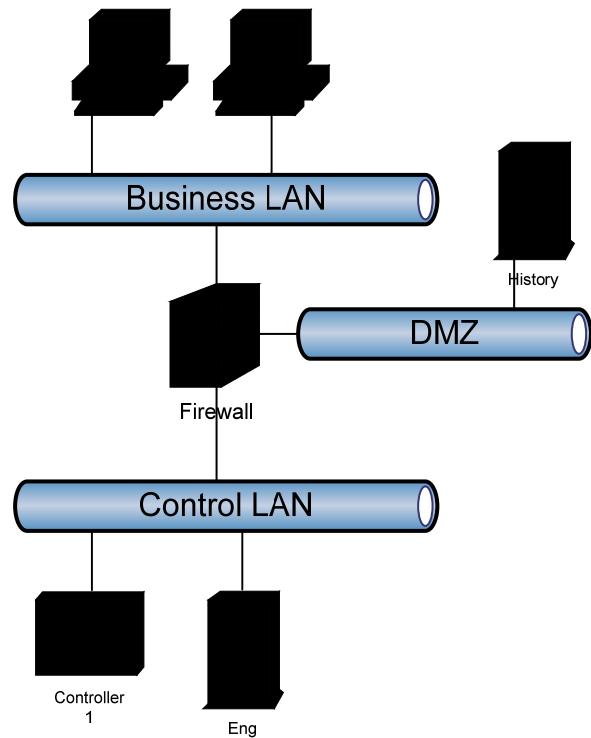
Routers or Layer-3 Switches
with ACL Filters

ACL = Access Control List

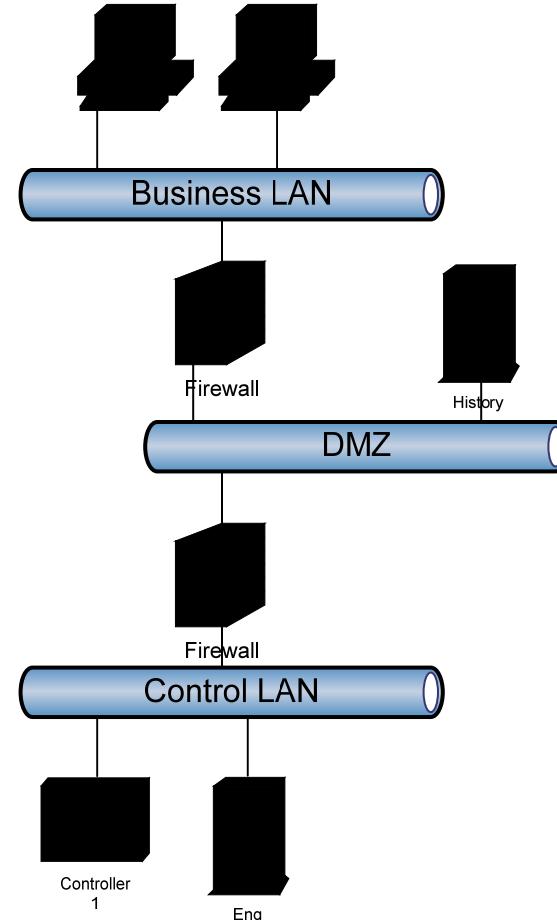


Firewall

Firewalls / DMZs



Firewall with DMZ



Paired Firewalls



Setting the Standard for Automation™

Patch Management in the IACS environment

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Topics

- Malicious Code Protection
- IACS Patching
- Asset Owner Requirements
- Product Supplier/Service Provider Requirements



Malicious Code Protection

- Malware related incidents are among the top cause of cyber-related production losses and upsets in process control systems
- Protection mechanism against malicious code to
 - Prevent
 - Detect
 - Report
 - Mitigate
- How do you verify that your prevention or detection mechanisms are functioning as expected?

Malicious Code Protection

- Use mixed deployment systems:
 - Scanning at the control system firewall
 - Ingress and egress traffic
 - Application whitelisting (AWL)
 - Automatic updating for non-critical systems
 - 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 be located in the DMZ
- Patching an important tool for mitigation

Patch Management in the IACS Environment

- Patching is not a spectator sport
 - It requires all actors to play
 - Asset owners
 - Integrators
 - Maintainers
 - Product suppliers



IACS Patching

- Importance
 - IACS and the software it relies on is highly vulnerable
 - New vulnerabilities are discovered and published almost daily
 - Malware authors take advantage of these vulnerabilities to exploit systems
 - Old malware still works on unpatched systems
- Challenges
 - **Patches are changes!!!**
 - Changes may impact safety, reliability, certification and performance
 - Must be part of change and configuration management process
 - Patching is very resource intensive
 - Infrequent maintenance outages

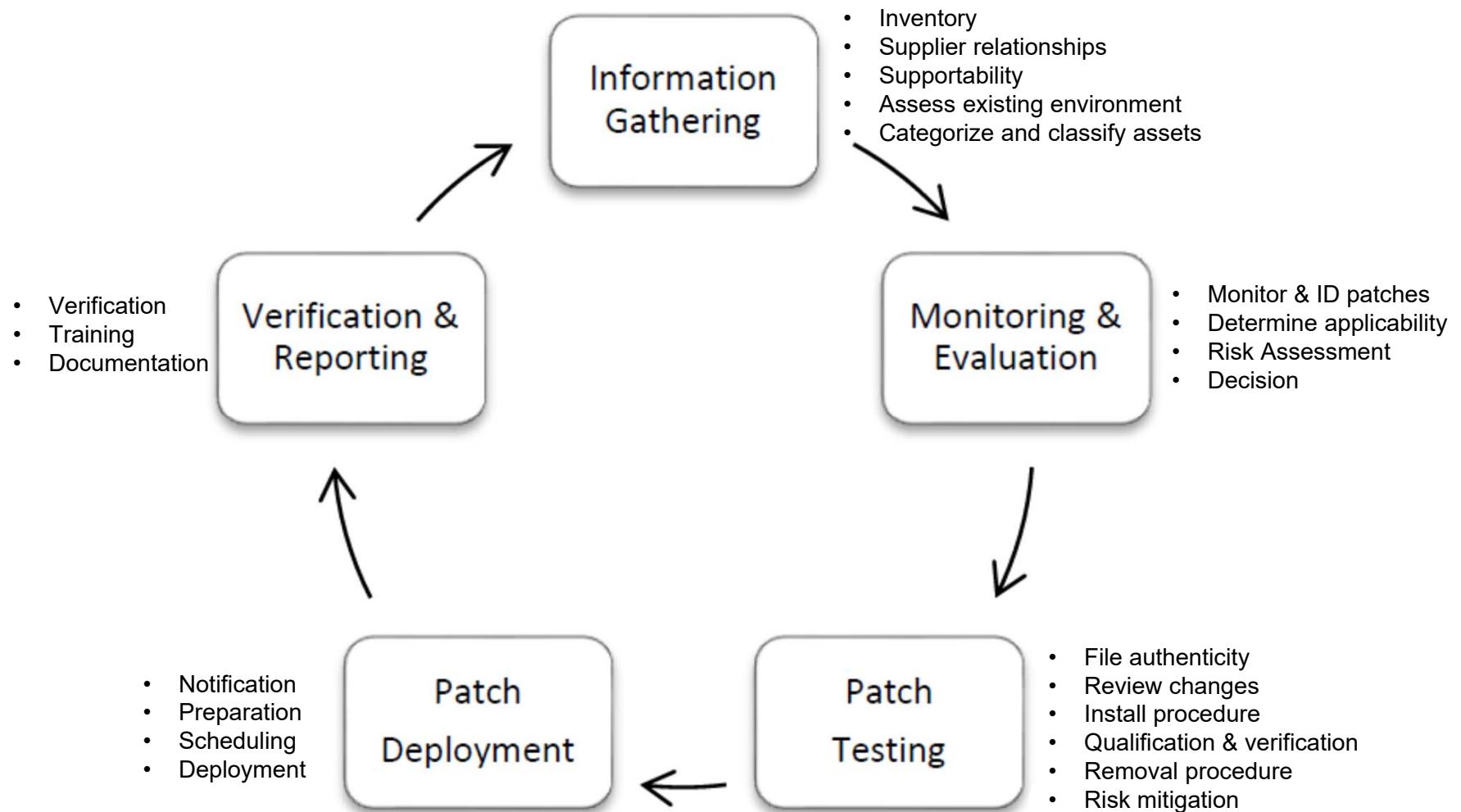
IACS Patching

- Develop the business case
 - Educate critical decision makers on reason for patching



- Patching is a risk management issue
 - Does the benefit of patching outweigh the cost and risks associated with patching?

IACS Patching



Source: ISA-TR62443-2-3 "Patch management in the IACS environment"

Asset Owner Requirements

- Information gathering
 - Inventory of existing environment
- Project planning and implementation
 - Develop patch management process
- Monitoring and evaluation
 - Security related patches applicability
- Patch testing
 - Test and qualify in a lab environment
- Patch deployment and installation
 - Notification of affected parties
 - Roll-back plan
- Operating patch management program
 - Sustained and optimized

Asset Owner Requirements

Priority Level	Target installation timeframe after approval of the patch by the IACS vendor
High	Within 1 week
Medium (default)	Within 3 months
Low	Within 2 years or next available outage
None	Never

Sample
severity based patch management timeframes

Product Supplier/Service Provider Requirements



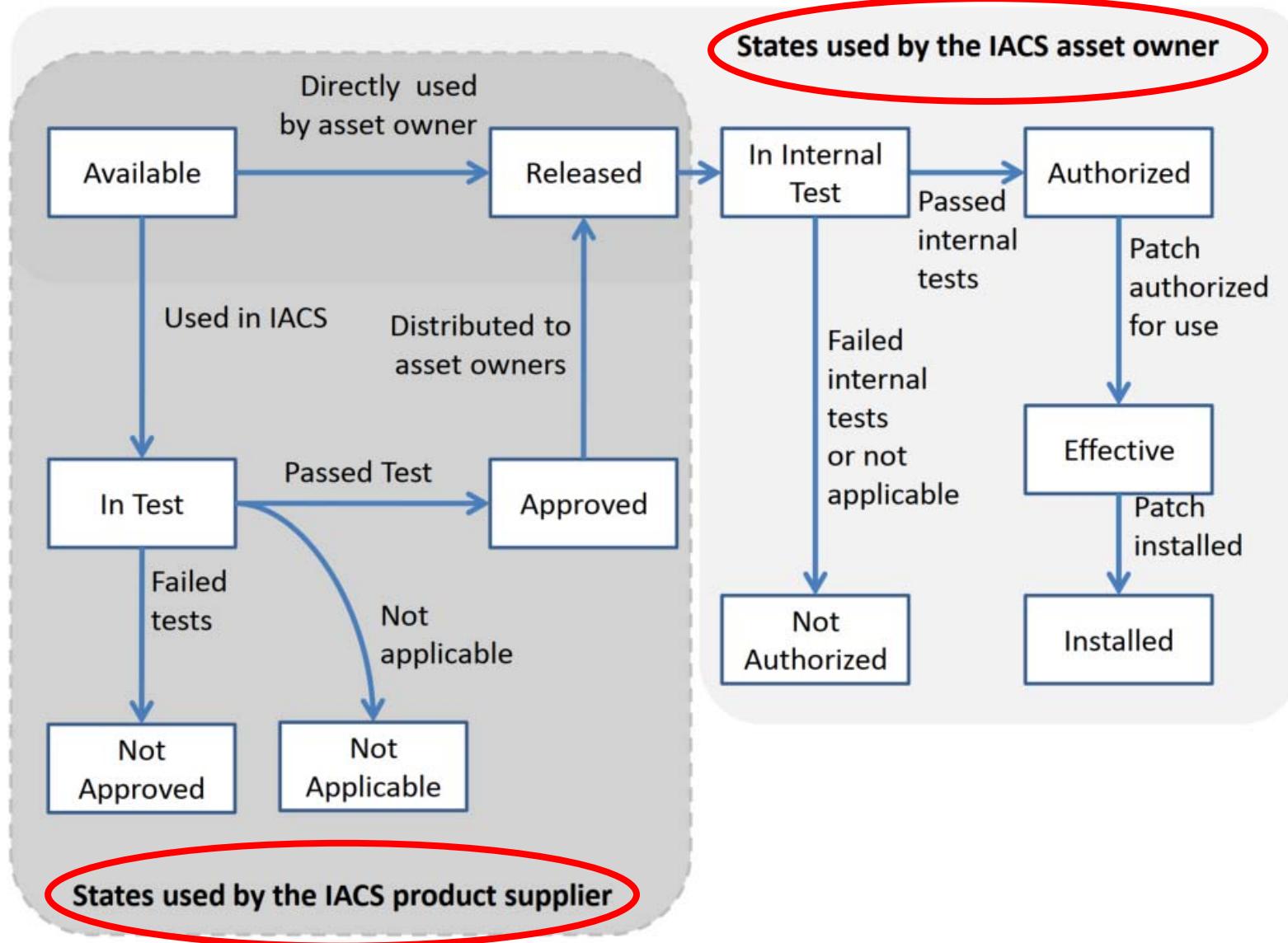
- Discovery of vulnerabilities
 - Procedures in place
 - Frequency defined
- Development, verification and validation
 - Validate mitigation
 - Compensating controls to reduce attack surface

Product Supplier/Service Provider Requirements



- Distribution of cyber security updates
 - Available via a secure channel
 - Provide patch sources for third-party software used in product
 - Windows Server Update Services (WSUS)
 - Traditional Microsoft second Tuesday of the month release day
 - Microsoft patch release process is evolving
 - Out of band patching
- Communication and outreach
 - Address asset owner communications
 - Where and how to report a suspected attack or vulnerability
 - Communicate to asset owners and system integrators
 - Life cycle support

Patch Lifecycle State Model



Recap

- Malicious Code Protection
- IACS Patching
- Asset Owner Requirements
- Product Supply Chain Elements





Setting the Standard for Automation™

Intrusion Detection

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Intrusion Detection Systems (IDS)

- Tools to detect attempts to break into or misuse a computer system
- Security service monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner
- Allow system admins to respond to potential security issues
- If firewalls and access control systems are the door
– IDS is the burglar alarm



Intrusion Prevention Systems (IPS)

- Intrusion Prevention Systems (IPS) add the ability to act on intrusion detection by automatically blocking malicious activity
 - IPS generally not used within IACS zones
- As attacks become more sophisticated, tools and techniques will need to become more sophisticated as well
 - Behavior-based IPS



Types of IDS

- Network Intrusion Detection (NIDS)
 - Monitor network traffic
 - Pre-defined rules (signature-based)
 - Behaviors (heuristics-based)
 - Passive Sniffing
 - Inline Deployment (bump in the wire)
- Host Intrusion Detection (HIDS)
 - Monitor host
 - Pre-defined rules (signature-based)
 - Behaviors (heuristics-based)
 - Passive Sniffing

IDS Issues

- False positives
- Deployment and operational costs
- Only effective against known vulnerabilities
- Limited signatures for control system protocols
- Requires continuous care and feeding

IDS/IPS Best Practices

- Distributed deployment – install NIDS at zone entry points
- Enhance IT IDS signatures with SCADA IDS signatures
 - Industrial protocols such as Modbus, DNP3
- Rules written in Snort syntax cover
 - Unauthorized requests
 - Malformed protocol requests and responses
 - Dangerous commands
 - Malicious network behavior
- Intrusion Prevention System (IPS) should be implemented with extreme care to avoid inadvertently blocking necessary traffic

Unified Threat Management (UTM)

- Unified Threat Management (UT)
 - Single appliance, multiple features
 - Network firewalling
 - Network intrusion prevention
 - Gateway antivirus (AV)
 - Gateway anti-spam
 - VPN
 - Content filtering
 - Load balancing
 - Data leak prevention





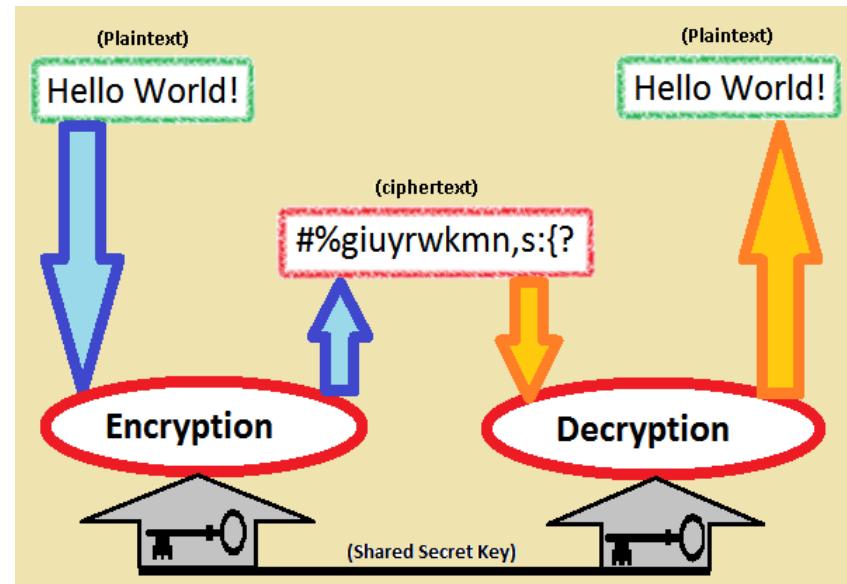
Setting the Standard for Automation™

Encryption

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Cryptography

- Classes of Ciphers
 - Block Ciphers
 - Fixed size e.g 64 bits
 - Stream Ciphers
 - Continuous stream
 - Bit by bit
- Types of Ciphers
 - Symmetric key
 - Same shared key
 - Lower network overhead
 - Faster than asymmetric
 - Asymmetric key
 - Different keys
 - Higher network overhead



Cryptographic Algorithms

- Symmetric (private) key examples
 - Data Encryption Standard (DES), 56-bit key
 - Triple DES (3DES), 192-bit key
 - Advanced Encryption Standard (AES), up to 256-bit key
- Asymmetric (public) key examples
 - RSA, 2048-bit key
 - Diffie-Hellman, 4096-bit key
 - Elliptic Curve, 256-bit key (comparable to 3027-bit RSA)



Caesar cipher rotating disks

File Hashing

- What is hashing?
 - Creating a unique identifier of some chunk of data
- What are cryptographic hashing algorithms?
 - One-way directional math formula used to generate a unique hex signature
- What are some common algorithms?
 - Message Digest (MD5)
 - Secure Hash Algorithm (SHA-1, SHA-256, SHA-512)
- Why should I care about hashing?
 - Verify that data is legitimate and has not been tampered with
- Where can I learn how to hash my data?
 - Browser search on “NCCIC ICS_Factsheet_File_Hashing_S508C.pdf”
 - https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_Factsheet_File_Hashing_S508C.pdf
 - Retrieved (31 March 2021)



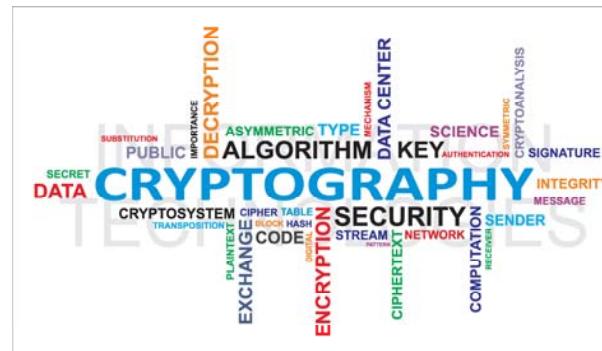
Setting the Standard for Automation™

Making Wise Choices

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Secure Protocols

- Internet Security protocols
 - SSL (Secure Sockets Layer)
 - TLS (Transport Layer Security)
 - HTTPS (Hypertext Transfer Protocol Secure)
 - Encrypts the communications layer over SSL and TLS
 - IPSec (Internet Protocol Security)
 - MPLS (Multiprotocol Label Switching)
 - SSH-2 (secure Shell)
 - WTLS (Wireless Transport Layer Security)

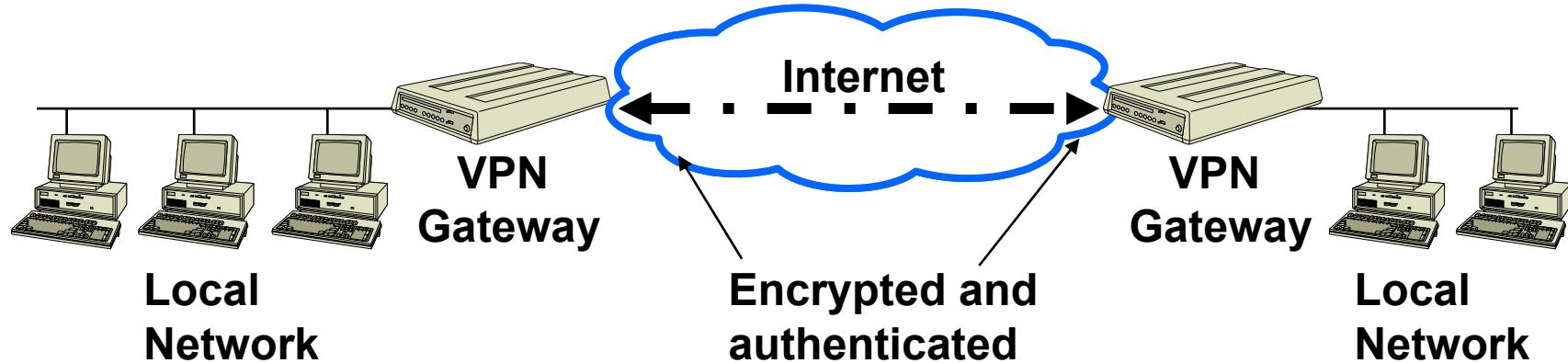


Virtual Private Network (VPN) Appliances

- Network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their proprietary data
- Ideal VPN appliance offers central management and multi-platform functionality and is compatible with all essential network applications and legacy platforms
- SSL VPN is a commonly-used protocol for managing the security of message transmission on the Internet via the web browser

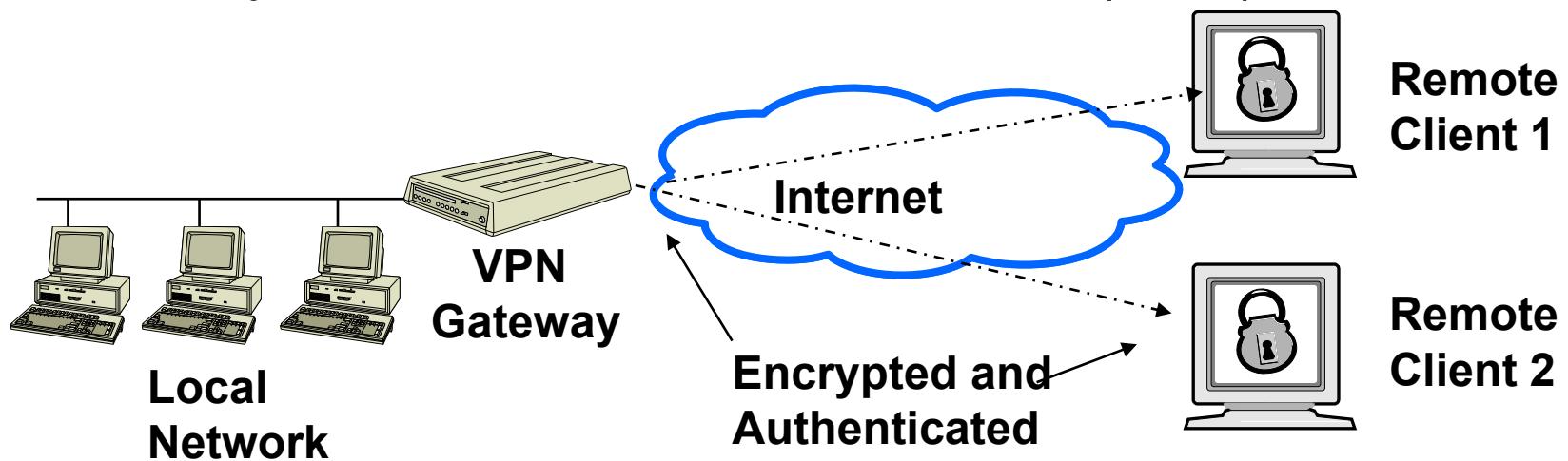
Site-to-Site VPNs

- The two endpoints of the VPN are intermediary devices that pass traffic from a trusted network to another trusted network while relying on the VPN technology to secure the traffic on the untrusted transport network.
- Commonly called site-to-site or LAN-to-LAN VPNs.



Remote Access VPNs

- One endpoint is a host computing device, and the other endpoint is an intermediate device that passes traffic from the host to the trusted network behind the security gateway while relying on the VPN technology to secure the traffic on the untrusted network
- Commonly called remote access service (RAS) VPNs.





Setting the Standard for Automation™

Section

Security Risk Assessment for System Design Intro

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Security Levels (SL)
- Foundational Requirements (FR)



Security Level (SL) Definitions

- Security Level is the measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner
- ISA/IEC 62443 series define SLs in terms of **five** different levels each with an increasing level of security
 - SL 0: No specific requirements or security protection necessary
 - SL 1: Protection against casual or coincidental violation
 - SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
 - SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
 - SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

ANSI/ISA-62443-3-3, subclause 3.1.40, pg 20

ANSI/ISA-62443-3-3, Annex A, subclause A.3.2, pg 72

Types of Security Levels (SL)

- SLs have been broken down into three different types
 - Target (SL-T)
 - Achieved (SL-A)
 - Capability (SL-C)
- While they all are related, they have to do with different aspects of the security life cycle
- Target SLs (SL-T) are the desired level of security for a particular system
 - This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation

Types of Security Levels (SL)

- Capability SLs (SL-C) are the security levels that components or systems can provide when properly configured
 - These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated
- Achieved SLs (SL-A) are the actual level of security for a particular system.
 - These are measured after a system design is available or when a system is in place
 - They are used to establish that a security system is meeting the goals that were originally set out in the target SLs (SL-T)

Foundational Requirements

- The simple CIA model shown earlier is not adequate for a full understanding of the requirements for security in IACS
- Seven basic or Foundational Requirements (FR) have been identified for IACS that includes CIA model
- All FRs are within the scope of all standards
 - We will use FR terms/acronyms located in Part 3-3
 - In some cases more detailed normative information is provided by other standards



ANSI/ISA-62443-1-1, subclause 5.2.1, pg 37

ANSI/ISA-62443-3-3, Annex A, subclause A.3.1, pg 72

Foundational Requirements

- FR 1 - Identification and Authentication Control (IAC)
 - Control access to selected devices, information or both
 - Protect against unauthorized interrogation of the device or information
- FR 2 - Use Control (UC)
 - Control use of selected devices, information or both
 - Protect against unauthorized operation of the device or use of information
- FR 3 - System Integrity (SI)
 - Ensure the integrity of data on selected communication channels
 - Protect against unauthorized changes
- FR 4 - Data Confidentiality (DC)
 - Ensure the confidentiality of data on selected communication channels
 - Protect against eavesdropping

Foundational Requirements

- FR 5 - Restrict Data Flow (RDF)
 - Restrict the flow of data on communication channels
 - Protect against the publication of information to unauthorized sources
- FR 6 - Timely Response to Events (TRE)
 - Respond to security violations
 - Notify the proper authority
 - Report needed forensic evidence of the violation
 - Automatically taking timely corrective action in mission critical or safety critical situations
- FR 7 - Resource Availability (RA)
 - Ensure the availability of all network resources
 - Protect against denial-of-service attacks

FR and SL Vector

- Instead of compressing SLs down to a single number, it is possible to use a vector of SLs that uses the seven FRs instead of a single protection factor
 - $\text{SL-?}([\text{FR},]\text{domain}) = \{ \text{IAC } \text{ UC } \text{ SI } \text{ DC } \text{ RDF } \text{ TRE } \text{ RA \}$
 - $\text{SL-T(BPCS Zone)} = \{ \text{ 2 } \text{ 2 } \text{ 0 } \text{ 1 } \text{ 3 } \text{ 1 } \text{ 3 \}$
- This vector of SLs allows definable separations between SLs for the different FRs
- The language used in the SL definitions can contain practical explanations of how one system is more secure than another without having to relate everything to HSE consequences

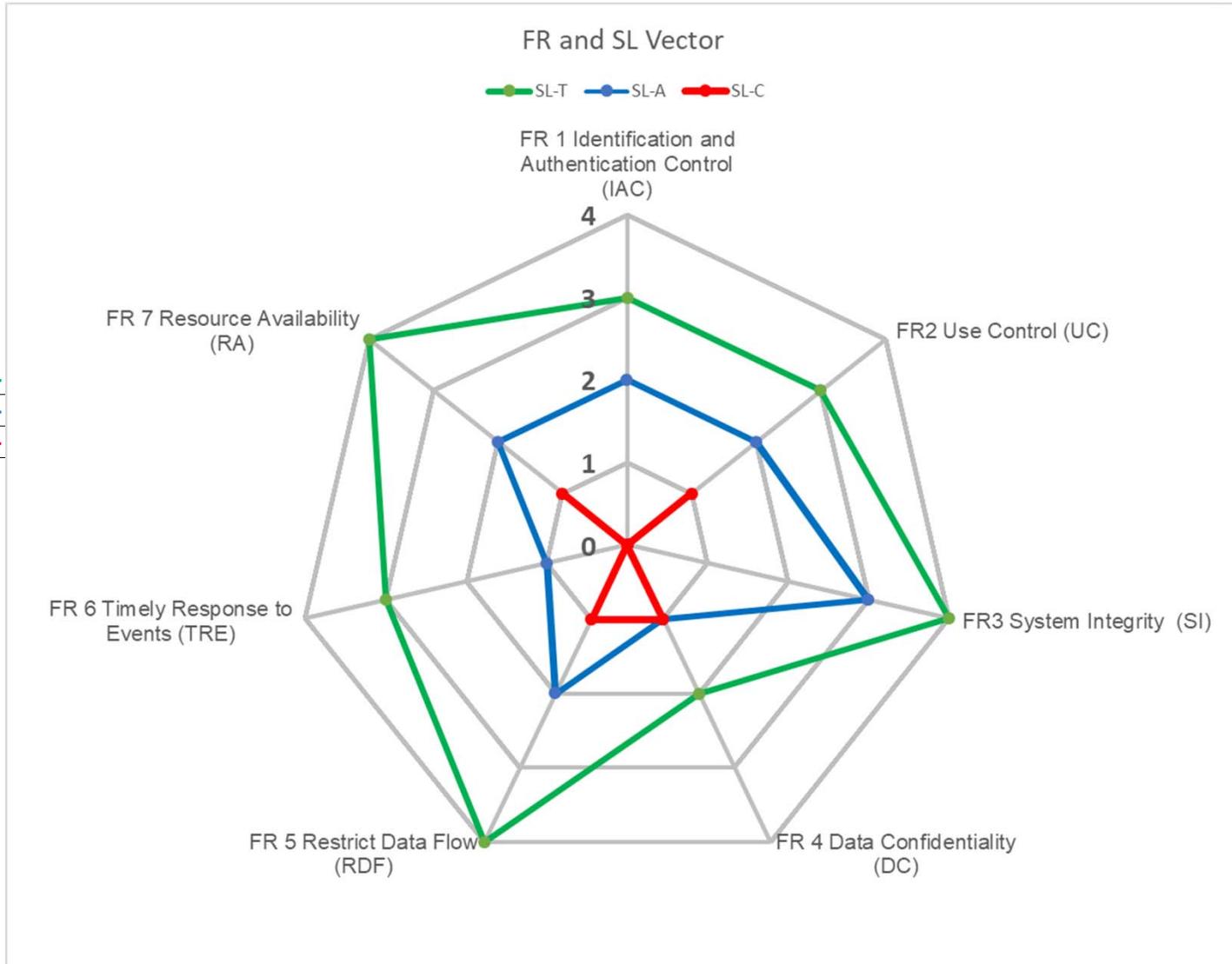
ANSI/ISA-62443-3-3, Annex A, subclause A.3.1, pg 74

FR and SL vector

- A vector can be used to describe the security requirements for a zone, conduit, component or system better than a single number
- Format examples
 - $SL-?([FR,]domain) = \{ IAC \text{ UC } SI \text{ DC } RDF \text{ TRE } RA \}$
 - $SL-T(BPCS \text{ Zone}) = \{ 2 \text{ } 2 \text{ } 0 \text{ } 1 \text{ } 3 \text{ } 1 \text{ } 3 \}$
 - $SL-?([FR,]domain) = \{ IAC \text{ UC } SI \text{ DC } RDF \text{ TRE } RA \}$
 - $SL-C(\text{SIS Engineer Workstation}) = \{ 3 \text{ } 3 \text{ } 2 \text{ } 3 \text{ } 0 \text{ } 0 \text{ } 1 \}$
 - $SL-?([FR,]domain) = \{ IAC \text{ UC } SI \text{ DC } RDF \text{ TRE } \textbf{RA} \}$
 - $SL-C(RA, FS-PL) = \{ - \text{ } 3 \}$
 - $SL-C(RA, FS-PLC) = 3$

FR and SL vector

SL-T(BPCS Zone) = {3 3 4 2 4 3 4}
SL-A(BPCS Zone) = {2 2 3 1 2 1 2}
SL-C(BPCS Zone) = {0 1 0 1 1 0 1}



Recap

- Security Levels (SL)
- Foundational Requirements (FR)



Week 7

Week 7

Week 7

Week 7

Week 7

Week 7



Setting the Standard for Automation™

Risk Assessment ISA-62443-2-1

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Topics

- Risk Assessment Overview
- Security Risk Assessment for System Design
- Zones and Conduits Revisited

Risk Assessment Overview

Risk Equation



- Risk equation
 - Risk = Threat x Vulnerability x Consequence
- Threat
 - Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm
 - Circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service



Risk Equation

- Vulnerability
 - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy
 - Weakness in a system function, procedure, internal control or implementation that could be exploited or triggered by a threat source, either intentionally designed into computer components or accidentally inserted at any time during its lifecycle
 - Sources come from physical and cyber security threats, internal and external threats, consider hardware, software, and information
- Consequence
 - Result that occurs from a particular incident
 - Condition or state that logically or naturally follows from an event

Risk Equation

- Risk = Threat x Vulnerability x Consequence
- Simplify equation
 - Convert “Threat x Vulnerability” = “Likelihood”
 - Likelihood = Quantitative chance that an action, event or incident may occur
- Risk = Likelihood x Consequence
 - Easier to work with 2 factors

Use Case—Financial Impact

- What is the likelihood for a virus to cripple the IACS?
 - First it needs to be a viable virus that can affect the IACS
 - Windows virus on a Unix system not a big concern
 - Windows virus on unpatched Windows operating system a big concern
 - What do you mean we still have an XP SP2 machine running!!!
 - Second it needs to reach the IACS
 - Many vectors available for that, including sneaker net
 - Third it needs to defeat antivirus controls on the IACS
 - The virus signatures are up to date, aren't they?
 - What does the Reasonable Person On the Street say?
 - Chances are good IACS could get hit by virus in the next year



Likelihood Scale

- We have determined that the likelihood of a virus to cripple the IACS is possible
 - Establish a category of high, medium, low
 - Use existing Scale matrix
 - In the case of the virus
 - Chances are good network could get hit by one in the next year

Likelihood	
Category	Description
High	A threat/vulnerability whose occurrence is likely in the next year.
Medium	A threat/vulnerability whose occurrence is likely in the next 10 years.
Low	A threat/vulnerability for which there is no history of occurrence and for which the likelihood of occurrence is deemed unlikely.

Consequence Scale

- Next determine consequence for each risk area
 - Use financial COST (million USD) impact for this walk through
 - Virus resulting in operations upset
 - 8 days of off-specification product that cannot be sold
 - Financial loss is 41 million USD = Cost >5 = Consequence Category = B (medium)

Consequence									
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	> 5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community
C (low)	< 1 day	< 1 hour	< 5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits	Little to no impact to business sectors beyond the individual company. Little to no impact on community services

Risk Level Matrix

- Matrix is tool for establishing first go around on assessing risk
 - Provides starting point for financial COST example
- Risk = Likelihood x Consequence
- Proceed using organization's matrix to determine Risk Response

Likelihood of virus = High

Consequence Category = B

		Consequence category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

Risk = High-risk

- Risk assessment covered in more detail in Assessing Cybersecurity of New or Existing IACS Systems (IC33)
- Discuss risk assessment and risk response next

Risk Assessment

- A good risk assessment should provide the following information for the entire system as well as for each zone and conduit
- Risk profile
- Highest severity consequences
- Threats & vulnerabilities leading to the highest risks
- Target Security Levels
- Recommendations

Risk Assessment

- Risk Response
 - Design the risk out
 - Reduce the risk
 - Accept the risk
 - Transfer or share the risk
 - Eliminate or redesign redundant or ineffective controls
- Risk Tolerance
 - It is management's responsibility to determine the level of risk the organization is willing to tolerate



Setting the Standard for Automation™

Security Risk Assessment for System Design

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Security risk assessment for system design

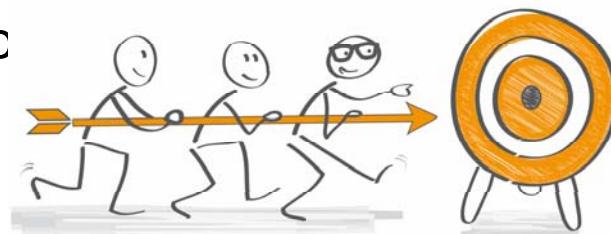
- Security risk assessment for system design
 - ISA-62443-3-2 high level overview
 - Approved and published August-October 2020
- Purpose is to align risk ranked vulnerabilities
 - ISA-62443-3-3 system security requirements and security levels
 - Uses a risk reduction factor approach like Safety Integrated Levels of ISA-84
- Scope
 - Define System under Consideration (SuC)
 - Partition SuC into zones and conduits
 - Assess risk
 - Establish Target Security Level (SL-Ts)
 - Document requirements



Security Risk Assessment for System Design



- System under Consideration (SuC)
 - Defined collection of IACS and related assets for the purpose of security risk analysis
 - Consists of one or more zones and related conduits
 - All assets belong to either a zone or conduit
- Target Security Level (SL-T)
 - Measure of confidence based on security policy and consequence analysis
 - This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its c



Security Risk Assessment for System Design

- Achieved Security Level (SL-A)
 - Actual level of security
 - Measured after a system design is available
 - Additional compensating countermeasures in place
 - Used to measure that the Target Security Level (SL-T) goal is met
- Capability Security Level (SL-C)
 - Built into a device or system when properly configured
 - Capable of meeting a Target Security Level (SL-T) without additional compensating countermeasures



Security Risk Assessment for System Design

- Any documented detailed risk assessment methodology may be followed
 - Provided the risk assessment requirements are satisfied by the methodology selected
- The initial and detailed risk assessment methodologies should be derived from the same
 - Framework
 - Standard
 - Source
- Must use a consistent risk ranking scale
 - Produce consistent and coherent results

Security Risk Assessment for System Design

- One approach to measure the degree of risk reduction required to achieve tolerable risk is by using
 - Cyber Risk Reduction Factor (CRRF)
 - Process Hazard Analysis (PHA)
 - Safety instrumented system design (ISA84/IEC61511)
- In any method
 - Relationship between risk reduction factor and SL-T will need to be established
 - Based upon the organization's
 - risk matrix
 - risk tolerance

Security Risk Assessment for System Design

- CRRF = Unmitigated Risk / Tolerable Risk
- Unmitigated risk is determined for each identified threat
- Threat intelligence
 - Vendor
 - Government sources
 - Sector specific intel
 - Other relevant sources

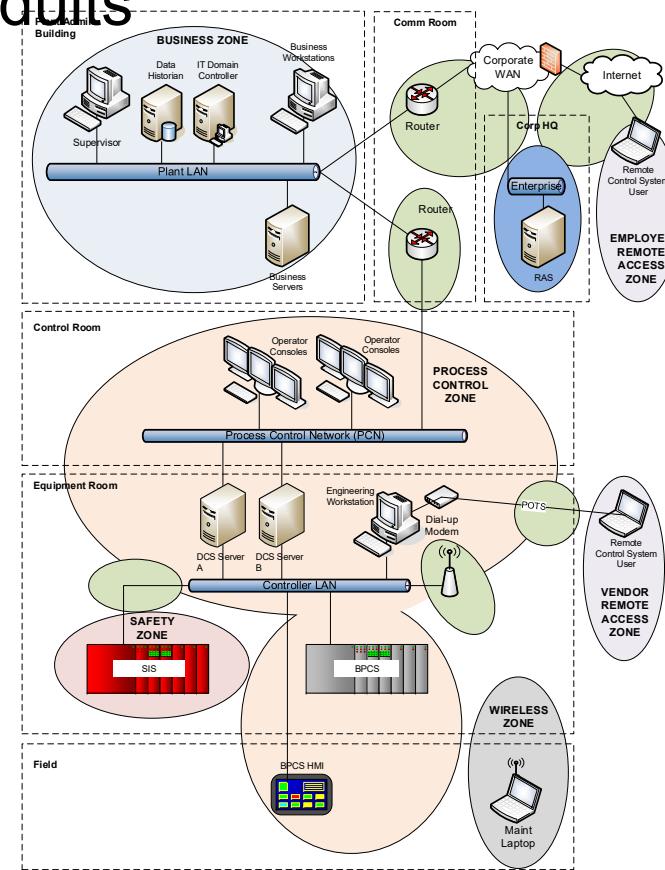
Security Risk Assessment for System Design

- Unmitigated cyber security risk is compared to the organization's tolerable risk
- If the unmitigated risk exceeds the tolerable risk, the organization determines whether to accept, transfer or mitigate the risk
- IC33 addresses Cyber Risk Ass detail



Security Risk Assessment for System Design

- Establishment of zones and conduits
 - Group IACS and related assets
 - Criticality of assets
 - Operational function
 - Physical location
 - Logical location



Zone & Conduit Characteristics

- Name and/or Unique Identifier
- Accountable organization(s)
- Definition of logical boundary
- Definition of physical boundary
- Safety designation
- Connected zones or conduits
- SL-T

Zone & Conduit Characteristics – cont'd

- Applicable security requirements
- Applicable security policies
- Assumptions and external dependencies
- List of logical access points
- List of physical access points
- List of data flows
- List of assets

Security Risk Assessment for System Design



- Few more considerations
 - Separation of business and control system zones
 - Separation of safety-critical zones
 - Separation of temporarily connected devices
 - Separation of wireless communications
 - Separation of devices connected via untrusted networks
 - Remote access is outside the physical boundary of the SuC
 - Model as a separate zone or zones
 - Separate security requirements identified
- Practical applications
 - Using what we have learned
 - Review sampling of reference architectures in following slides

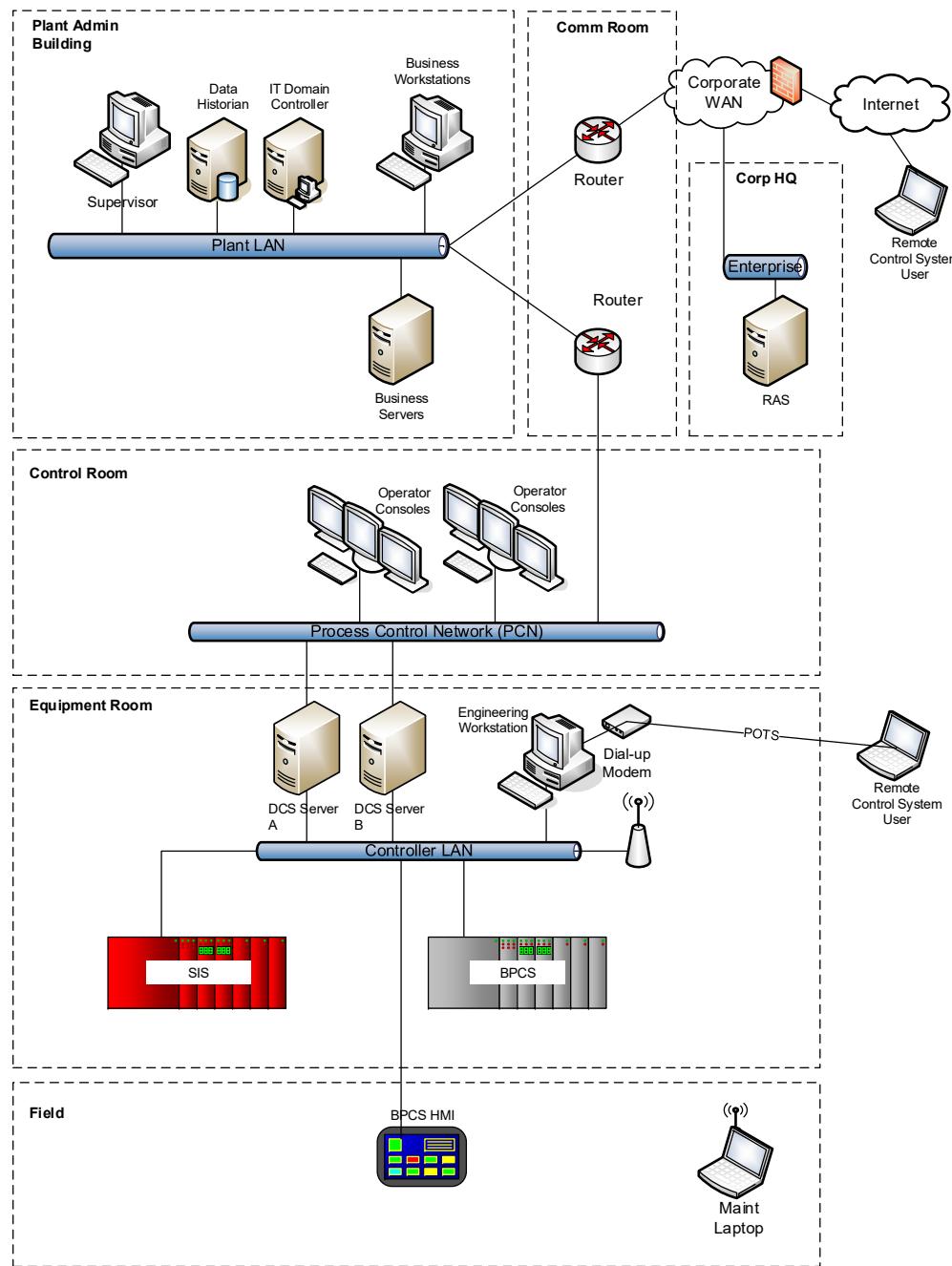


Setting the Standard for Automation™

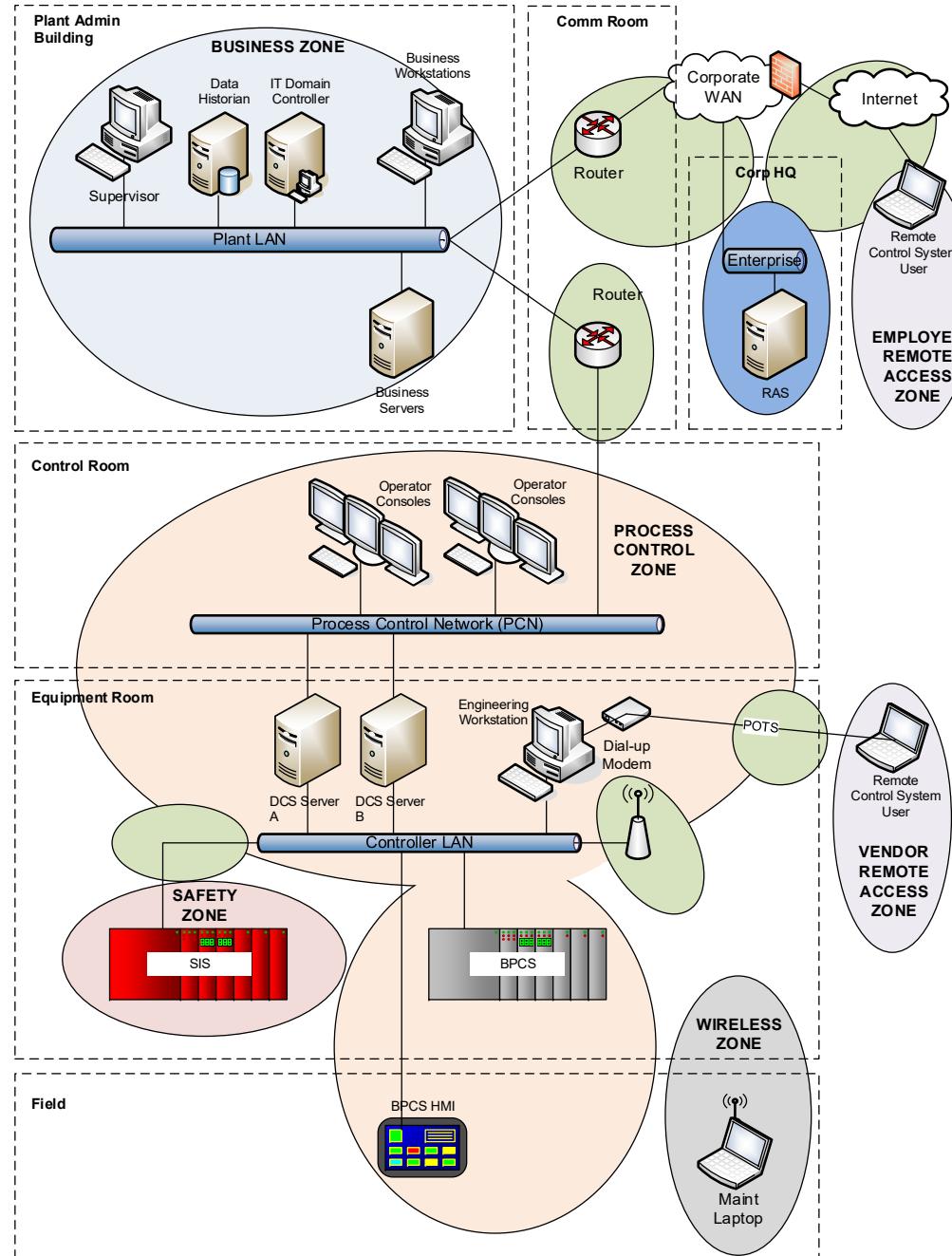
Zones and Conduits Revisited

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Initial Identification of Zones/Conduits



Initial Identification of Zones/Conduits



Recap

- Risk Assessment Overview
- Security Risk Assessment for System Design
- Zones and Conduits Revisited





Week 8

Week 8

Week 8

Week 8

Week 8

Week 8



Setting the Standard for Automation™

Section Security program requirements for IACS service providers

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Introduction

- Requirements for IACS Service Providers
- Providers
 - Integration
 - Maintenance
 - Products



Requirements for IACS Service Providers

- Part 2-4 covers requirements for IACS service providers activities
 - Service providers will have to use technologies considered secure
 - Technologies no longer considered secure e.g., Digital Encryption Standard (DES) or Wireless Equivalent Privacy (WEP) security would be non-conformant



Requirements for IACS Service Providers

- What is a service provider?
 - Individual or organization that provides a specific support service and associated supplies
 - Has an agreement with the asset owner
- Integration Service Provider
- Maintenance Service Provider
- Concept includes Product Suppliers
- Provider & supplier terms used in place of the generic word “vendor” to provide differentiation



IACS Integration Service Provider

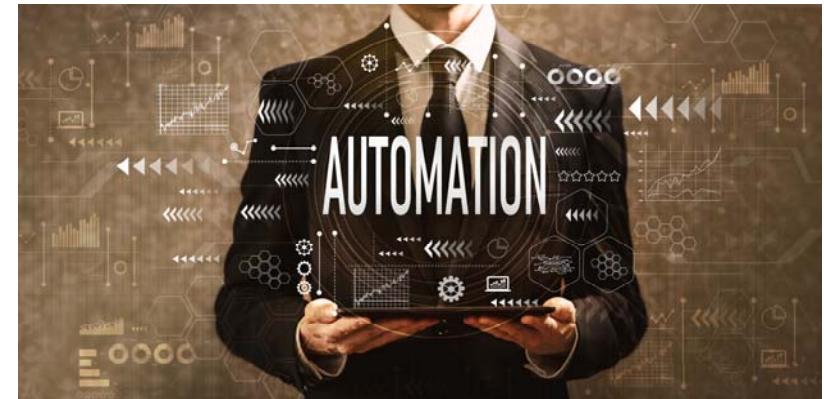
- Provides capabilities to implement/deploy Automation Solutions
 - According to asset owner requirements
- Integration service provider activities generally occur
 - Starting with the design phase
 - Ending in handover of the Automation Solution to the asset owner
- Typical Integration Service Provider Activities
 - Analysis
 - Development
 - Definition
 - Installation, configuration, patching, backup, and testing
 - Gaining approval of the asset owner during the execution of activities

IACS Maintenance Service Provider

- Performs activities that maintain and service Automation Solutions according to asset owner requirements
- Maintenance activities are separate from operation activities
- Maintenance activities generally start after handover of the Solution
 - May continue until the asset owner no longer requires them
- Typical Maintenance Service Provider Activities
 - Patching and anti-virus updates
 - Equipment upgrades and maintenance
 - Component and system migration
 - Change management
 - Contingency plan management

IACS Product Supplier

- Manufacturer of hardware and/or software product
- Develops control system product as a combination of
 - Supporting applications
 - Embedded devices
 - Network components
 - Host devices
- Independent of IACS environment
- Maintenance activities may be shared by
 - Asset Owner
 - Integrator
 - Maintainer
 - Product Supplier



Recap

- Requirements for IACS Service Providers
- Providers
 - Integration
 - Maintenance
 - Products





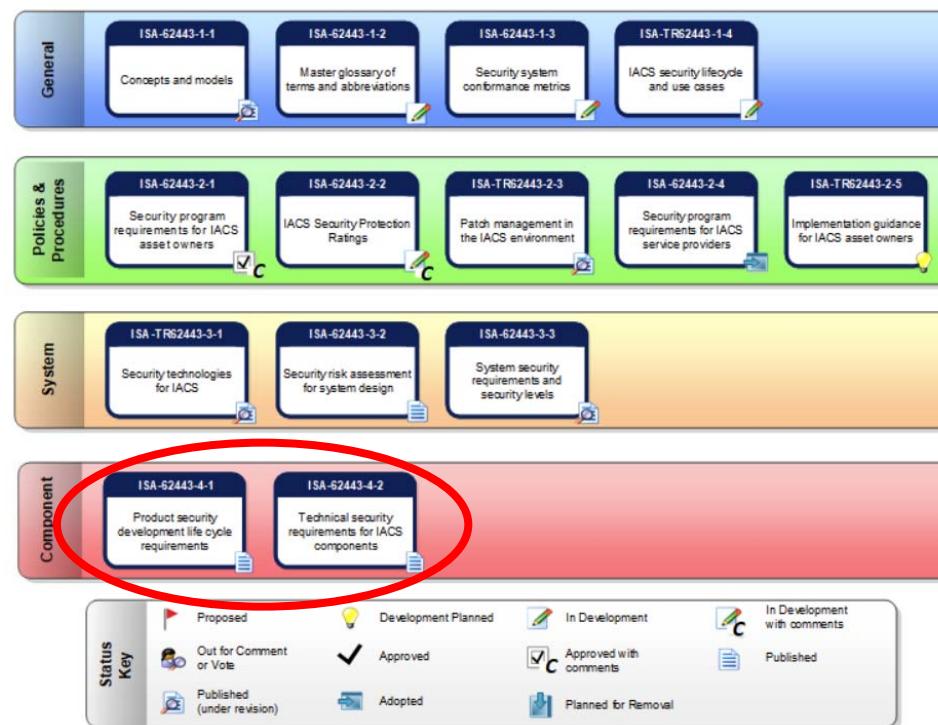
Setting the Standard for Automation™

Section: Developing Secure Products and Systems

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

Topics

- Product security development life-cycle requirements
- Technical security requirements for IACS components



Product security development life-cycle requirements

- Product suppliers are the main audience
- Primary goal to provide a product framework addressing
 - Secure by design
 - Defense in depth approach to designing
 - Building
 - Maintaining
 - Retiring
- Support meeting product overall Capability Security Level (SL-C)
 - What is the product's SL-C?
 - Ensure product security capabilities implemented correctly
 - Know security vulnerabilities are eliminated or mitigated
 - Concept of Target and Achieved Security Levels (SL-T, SL-A) other than Capability (SL-C) not covered in Part 4-1

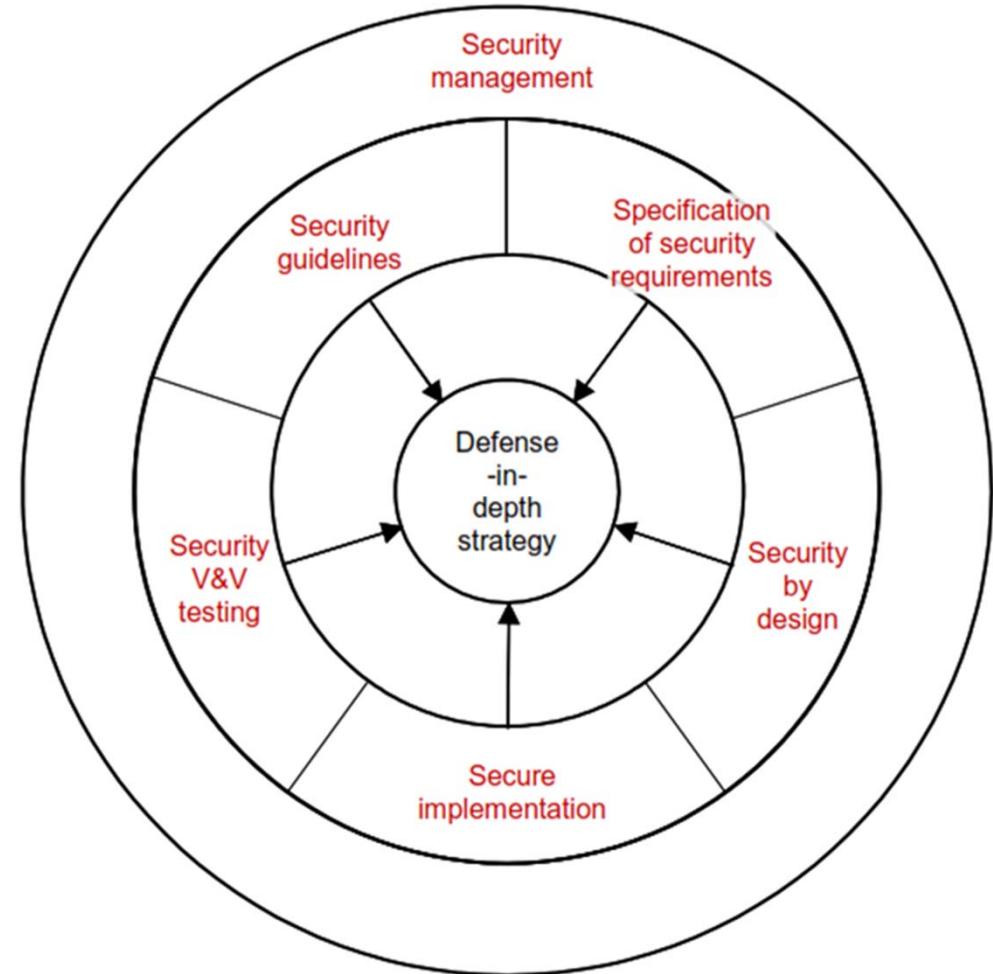


Product security development life-cycle requirements

- Secondary goal is to align
 - Development process
 - Needs of industrial users
 - Asset owners
 - Integrators
 - Maintenance contractors
 - Security configs & patch management polices and procedures
 - Communications about uncovered product security vulnerabilities
- Key concept is use of threat modelling
 - Impact analysis
 - Resolution
- Key philosophy of secure product life-cycle
 - Defense in depth strategy (shown next slide)

Defense in Depth Strategy Practices

- Defense in depth strategy is key philosophy to
 - Secure product life-cycle
 - Security development life-cycle
- Security Management includes
 - Security Defects
 - Security related issues
 - Documentation updates



Product Supplier Maturity Model

- How do we know a product supplier is meeting the practice requirements and benchmarks?
 - Benchmarks have been set for complying with requirements
 - Capability Maturity Model Integration for Development (CMMI-DEV) used
 - Ranging from Level 1 ad hoc processes to Level 5 maturity demonstrating metrics and continuous improvements
 - Using these benchmarks, it is possible that an organization will discover that it is not ready to implement all requirements to the same level of maturity
- 47 practice requirements ranging from the development process, threat modeling to secure operation guidelines
 - Part 4-1, Clause 5 provides details
 - Part 4-1, Annex B, summarizes the requirements in a table format

Technical security requirements for IACS components

- Who is the audience for Part 4-2?
 - System integrators
 - Assist in procuring control system components
 - Specify the appropriate security capability level of the individual components required
 - Choose components that provide necessary security capabilities to achieve SL-T for each zone
 - Product suppliers
 - Understand the requirements placed on control system components for specific security capability level (SL-C)s of those components
 - Provide documentation of how to properly integrate the component into a system to meet a specific SL-T

Technical security requirements for IACS components

- Four types of components
 - Software application
 - Operator workstation
 - Data historian
 - Embedded device
 - PLC
 - IED
 - Host device
 - Operator workstation
 - Data historian
 - Network device
 - Switch (network)
 - VPN terminator

```
208 limit_val = a;
209 $("#limit_val").a(a);
210 update_slider();
211 function(limit_val);
212 $("#word-list-out").a(" ");
213 var b = k();
214 h();
215 var c = 1(), a = "", d = parsing();
216 arseInt($("#slider_shuffle_max"));
217 function("LIMIT_total:" + d);
function("rand:" + f);
function("check_n
e: " + e - d, function("check_n
e: " + e - d);
```



- Series of Component Requirements (CR) and Requirement Enhancements (RE) specifically for components
 - Expands the System Requirements (SR) and Requirement Enhancements (RE) defined in ISA-62443-3-3
 - Built upon the same Foundational Requirements (FR) 1-7 and Security Levels (SL) 0-4

Technical security requirements for IACS components

- Common component security constraints (CCSC)
 - Applies to all components
 - Support of essential functions
 - Compensating countermeasures
 - Least privilege
 - Software development process
- Specific mapping of Component Requirements (CR) and Requirement Enhancements (RE)
 - CR – Component requirement (common to all component types)
 - SAR – Software application requirement
 - EDR – Embedded device requirement
 - HDR – Host device requirement
 - NDR – Network device requirement

ISASecure Conformance

- ISA Security Compliance Institute (ISCI) bridges the gap between standards and their implementation
 - Manages ISASecure conformance certification program
- ISASecure
 - Does not operate an internal testing lab, but instead, partners with qualified labs to perform IACS cybersecurity assessments
 - Independently certifies IACS products and systems to ensure that they are robust against network attacks and free from known vulnerabilities
 - Does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices
 - Certifies off-the-shelf systems



ISASecure Conformance

- Accredited ISASecure Certification Bodies (as of April 2021)



Control System Security Center Certification Laboratory



ISASecure Certified Sample

	Honeywell Process Solutions	PLC	ControlEdge 900 Controller	R160	EDSA 2.0.0 Level 2	12/20/2020
	GE Power Conversion	Power Controller	HPCi Controller	7.1	CSA 1.0.0 Level 1	12/15/2020
	ABB	Controller	SPC 600/700/800 Controller	E_1	EDSA 3.0.0 Level 1	12/15/2020

- Certification includes requirements in
 - Part 3-3: System security requirements and security levels
 - Part 4-1 Product security development life-cycle requirements
- Certifier also performs System Robustness Testing
 - Fuzz testing
 - Network traffic load testing
 - Vulnerability scanning

Recap

- Product security development life-cycle requirements
- Technical security requirements for IACS components



Instructional Surveys

Instructional Surveys

Instructional Surveys

Instructional Surveys

IC32 - Pre-Instructional Survey

1. What is the primary function of a firewall?
 - a. Block all internet traffic
 - b. Detect network intrusions
 - c. Filters network traffic
 - d. Authenticate users
2. Inter-network connection device that restricts data communication traffic between two connected networks is called a(n) _____.
 - a. IDS
 - b. Firewall
 - c. Router
 - d. Anti-virus software
3. The process of securing a system by reducing its attack surface is known as
 - a. Threat Modeling
 - b. System Hardening
 - c. Intrusion Detection
 - d. Whitelisting
4. Policies, procedures and technical controls that govern the use of system resources are known as
 - a. Data Flow Controls
 - b. System Integrity Controls
 - c. Access Controls
 - d. System Hardening Controls
5. Which of the following is an objective of cybersecurity acceptance testing?
 - a. Verification of cybersecurity specifications
 - b. Root cause analysis
 - c. Cyber risk determination
 - d. Verification of system functionality

IC32 - Pre-Instructional Survey

6. What are the three main phases of the IACS Cybersecurity Lifecycle?
 - a. Assess, Develop & Mitigate, Maintain
 - b. Design, Implement, Maintain
 - c. Assess, Develop & Implement, Maintain
 - d. Design, Mitigate, Maintain
7. Which of the following is the correct risk equation?
 - a. Risk = Threat x Asset x Consequence
 - b. Risk = Threat x Vulnerability x Cost
 - c. Risk = Threat Agent x Threat x Vulnerability
 - d. Risk = Threat x Vulnerability x Consequence
8. The desired level of security for a system is known as?
 - a. Target Security Level
 - b. Achieved Security Level
 - c. Capability Security Level
 - d. Protection Level
9. Which of the following is the correct formula for Cyber Risk Reduction Factor (CRRF)?
 - a. CRRF = Unmitigated Risk / Tolerable Risk
 - b. CRRF = Mitigated Risk / Tolerable Risk
 - c. CRRF = Tolerable Risk / Unmitigated Risk
 - d. CRRF = Tolerable Risk / Mitigated Risk
10. An Intrusion Detection System (IDS) is an example of what method of treating risk?
 - a. Detect
 - b. Deter
 - c. Defend
 - d. Defeat

IC32 - Pre-Instructional Survey

11. Security service system that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner is called a(n) _____.
 - a. IDS
 - b. Firewall
 - c. Router
 - d. Anti-virus software
12. What is the name of the firewall feature that analyzes protocols at the application layer to identify malicious or malformed packets?
 - a. Stateful inspection
 - b. Deep packet inspection
 - c. Packet filter
 - d. Layer 3 check
13. A three-tier network segmentation design that prevents direct communication between the enterprise network and the process control network by creating a buffer is also known as a(n) _____.
 - a. Zones and conduits
 - b. Perimeter firewall
 - c. ICS firewall
 - d. DMZ
14. Which of the following represents the recommended process of firewall planning and implementation?
 - a. Plan, Configure, Test, Deploy, Manage
 - b. Plan, Configure, Deploy, Test, Manage
 - c. Plan, Deploy, Manage, Test, Configure
 - d. Design, Configure, Test, Deploy, Document
15. What are the main types of intrusion detection systems?
 - a. Perimeter Intrusion Detection & Network Intrusion Detection
 - b. Host Intrusion Detection & Network Intrusion Detection
 - c. Host Intrusion Detection & Intrusion Prevention Systems
 - d. Intrusion Prevention & Network Intrusion Detection

16. What is the desired outcome of the Initiate a CSMS program activity?
- a. Conceptual diagrams that show how an AD forest can be attacked
 - b. Obtain leadership commitment, support, and funding
 - c. Identify software agents used by threat agents to propagate attacks
 - d. Conduct periodic IACS conformance audits
17. Which of the following is NOT a network device hardening best practice?
- a. Install latest firmware updates
 - b. Shut down unused physical interfaces
 - c. Enable logging, collect logs (e.g. Syslog) and review regularly
 - d. Use Telnet for remote management
18. Which of the following is an example of dual-factor authentication?
- a. Username and password
 - b. Digital certificate and smart card
 - c. Fingerprint and retinal signature
 - d. Fingerprint and smart card
19. A network that uses a public telecommunication infrastructure such as the Internet to provide remote networks or computers with secure access to another network is known as a _____.
- a. VLAN
 - b. VSAT
 - c. VPN
 - d. VNC
20. If a virus shuts down an industrial network by overloading the Ethernet switches which basic information security property is affected?
- a. Integrity
 - b. Confidentiality
 - c. Availability
 - d. Reliability

IC32 - Post-Instructional Survey

- 1) Which three basic properties are the building blocks of cyber security?
 - a) Authorization, Identification, and Integrity (AII)
 - b) Confidentiality, Integrity and Availability (CIA)
 - c) Authorization, Reliability and Integrity (ARI)
 - d) Confidentiality, Integrity and Authorization (CIA)
- 2) What is the biggest security problem if business networks connect directly to industrial control systems?
 - a) Too many business users requesting data will slow control system operation to a crawl, endangering the security of processes.
 - b) Unauthorized business users, outsiders and malware can penetrate critical industrial control systems and upset critical processes.
 - c) Production workers will change data in business systems given the opportunity
 - d) Cybersecurity insurance will increase in cost
- 3) “Countermeasures” in cyber security are measures taken to:
 - a) Eliminate system penetration by outsiders
 - b) Confuse perimeter intrusion detectors
 - c) Reduce the system’s risk of loss from vulnerabilities and threats
 - d) Eliminate the risk of an inside attacker taking over a computer network
- 4) Why would a company issue security policies for industrial networks?
 - a) To let outside intruders know the consequences of their actions.
 - b) To clearly establish which department “owns” the network
 - c) To guide a company’s cybersecurity department on how to catch security violations.
 - d) To communicate the responsibilities of users, management, IT staff for company security.
- 5) A key factor for the success of a cyber security program is:
 - a) Security policy, objectives and activities that reflect business rationale and objectives.
 - b) Strict rules that forbid interconnection of control system to business systems.
 - c) The latest in security technologies.
 - d) The latest in hardware technologies.

IC32 - Post-Instructional Survey

- 6) One-way safety is different from security in industrial plants is that:
- a) Safety considers the effects of malicious actions, not just the causes.
 - b) The field of safety encompasses the field of security.
 - c) Safety concerns itself with human error and the natural causes of accidents, while security may involve malicious behavior.
 - d) Safety concerns itself with malicious behavior, while security may involve human error and the natural causes of accidents.
- 7) Which of the following documents are IT Security standards?
- a) IEC 61850
 - b) ISO 27001:2013
 - c) ISA 95
 - d) ISA 84
- 8) Which of the following are control system security standards?
- a) COBIT 5
 - b) ISO/IEC 15408:2009
 - c) ISA/IEC 62443
 - d) ISO 27001:2013
- 9) The standard ISA 62443-2-1 belongs in which tier/group of the ISA 99 committee work products?
- a) Component
 - b) System
 - c) General
 - d) Policies & Procedures
- 10) Which of the following is NOT generally considered to be a requirement of industrial control systems?
- a) Real-time performance
 - b) High availability
 - c) Frequent updates
 - d) HSE considerations

IC32 - Post-Instructional Survey

11) Which formula is correct?

- a) Risk = Threat x Asset x Consequence
- b) Risk = Threat x Vulnerability x Cost
- c) Risk = Threat x Likelihood x Vulnerability
- d) Risk = Threat x Vulnerability x Consequence

12) Which of the following would NOT be considered a countermeasure?

- a) Replay
- b) Access Controls
- c) Encryption
- d) Intrusion Detection

13) A logical grouping of physical, informational, and application assets sharing common security requirements is called a(n) _____

- a) Security model
- b) Asset model
- c) Conduit
- d) Zone

14) Which of the following is Layer 4 in the ISO OSI/Reference Model?

- a) Session
- b) Network
- c) Transport
- d) Data

15) Which one of the following can best perform a network subnet routing function?

- a) Layer 1 hub
- b) Layer 2 network interface card
- c) Layer 3 switch
- d) Layer 4 user datagram protocol

IC32 - Post-Instructional Survey

- 16) TCP is a _____ protocol
- a) Connection based
 - b) Layer 3
 - c) Send and forget
 - d) Layer 7
- 17) In IPv4 which protocol resolves IP addresses into MAC addresses?
- a) ICMP
 - b) TCP
 - c) IP
 - d) ARP
- 18) What is Microsoft's normal scheduled release day for security patches?
- a) When critical patches available
 - b) The first Monday of the month
 - c) The first Friday of the month
 - d) The second Tuesday of the month
- 19) What is the purpose of Windows Server Update Services (WSUS)?
- a) Deploy the latest Microsoft Hyper-V product updates
 - b) Distribution of Microsoft Software Update Services
 - c) Deploy the latest Microsoft product updates and hotfixes
 - d) Distribution of Windows Software Unified Server
- 20) What is the primary function of a firewall?
- a) Block all internet traffic
 - b) Detect network intrusions
 - c) Filters network traffic
 - d) Authenticate users

IC32 - Post-Instructional Survey

- 21) What is the first step in the High-Level Risk Assessment?
- a) Identify Threats
 - b) Identify Critical Assets and Consequences
 - c) Define Methodology for Identifying Risks
 - d) Analyze Threats
- 22) What is the desired outcome of the Initiate a CSMS program activity?
- a) Conceptual diagrams that show how an AD forest can be attacked
 - b) Obtain leadership commitment, support, and funding
 - c) Identify software agents used by threat agents to propagate attacks
 - d) Select and implement countermeasures
- 23) Which organization bridges the gap between 62443 standards and their implementation?
- a) National Institute of Standards and Technology (NIST)
 - b) International Electrotechnical Commission (IEC)
 - c) European Union Agency for Network and Information Security (ENISA)
 - d) ISA Security Compliance Institute (ISCI)
- 24) System Robustness Testing includes which of the following?
- a) Fuzz testing
 - b) Network traffic load testing
 - c) Vulnerability scanning
 - d) All the above
- 25) What are the three main phases of the ISA/IEC 62443 Cybersecurity Lifecycle?
- a) Assess, Develop and Implement, Maintain
 - b) Assess, Integrate, Maintain
 - c) Analyze, Develop and Implement, Maintain
 - d) Analyze, Integrate, Maintain



Answer Sheets

Answer Sheets

Answer Sheets

Answer Sheets

Answer Sheets

Answer Sheets

IC32 - Pre-Instructional Survey

Answer Key

1. c

2. b

3. b

4. c

5. a

6. c

7. d

8. a

9. a

10. a

11. a

12. b

13. d

14. a

15. b

16. b

17. d

18. d

19. c

20. c

IC32 Post-Instructional Survey Answer Key

1) b
2) b
3) c
4) d
5) a

6) c
7) b
8) c
9) d
10) c

11) d
12) a
13) d
14) c
15) c

16) a
17) d
18) d
19) c
20) c

21) c
22) b
23) d
24) d
25) a



Additional Resources

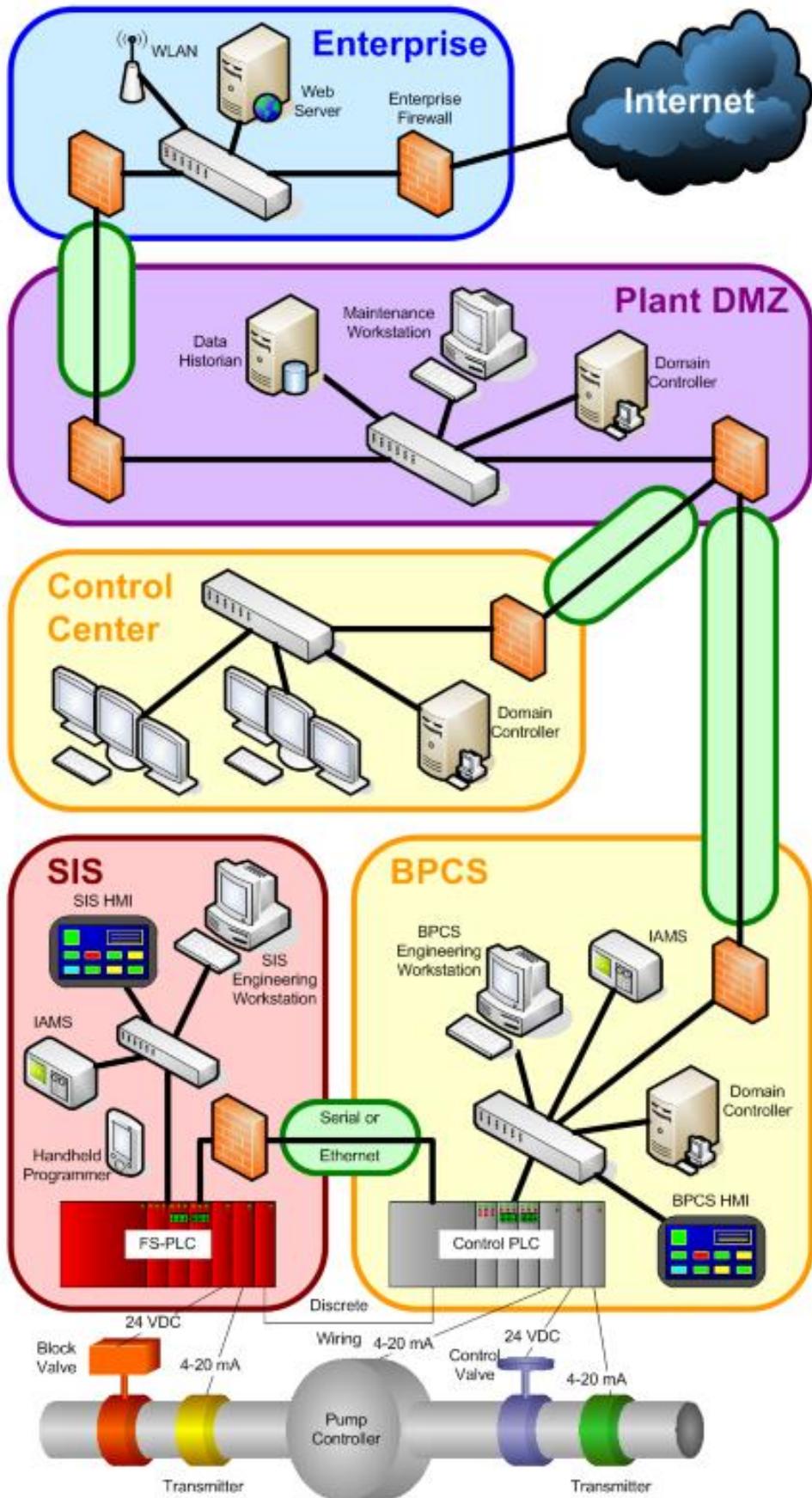
Additional Resources

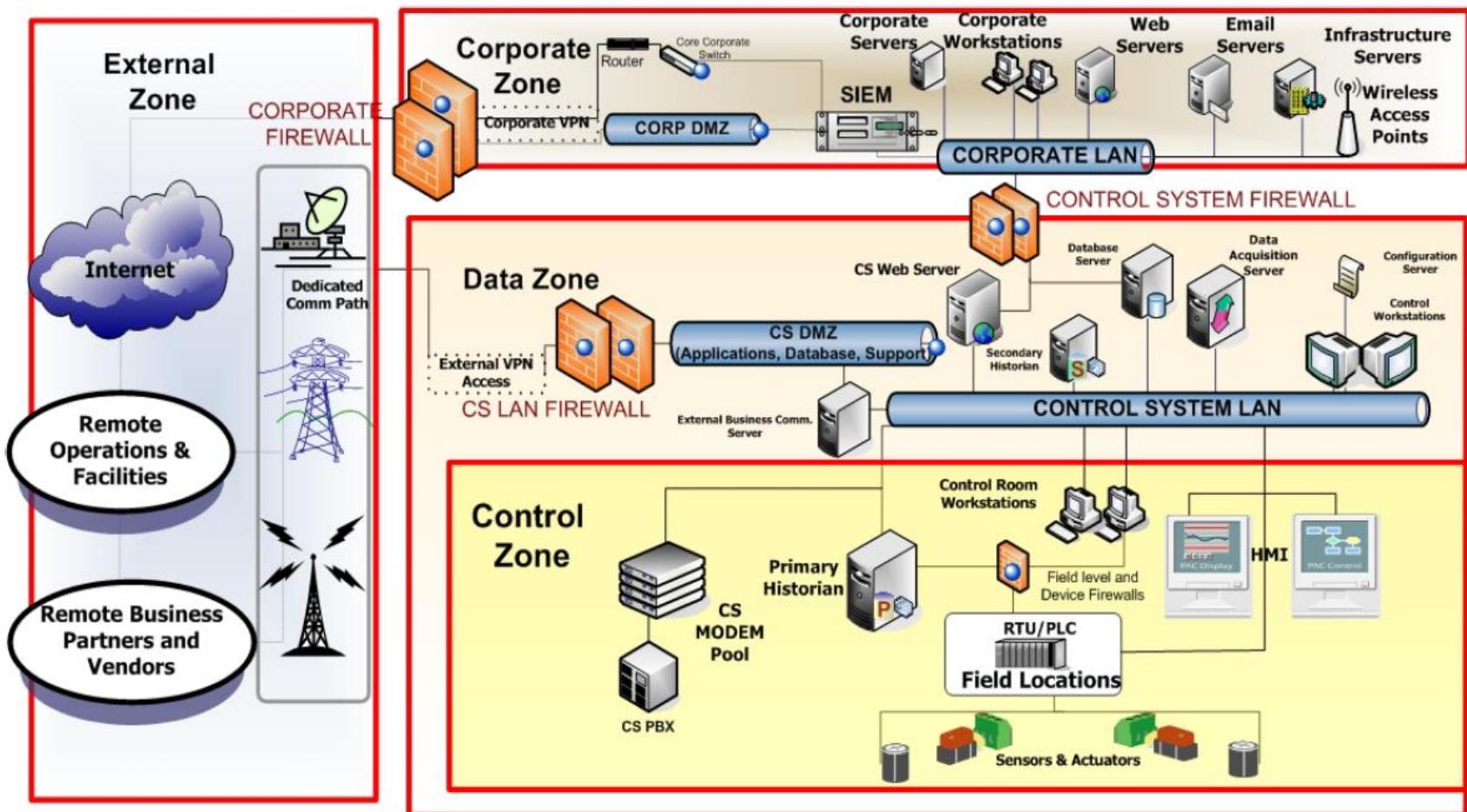
Additional Resources

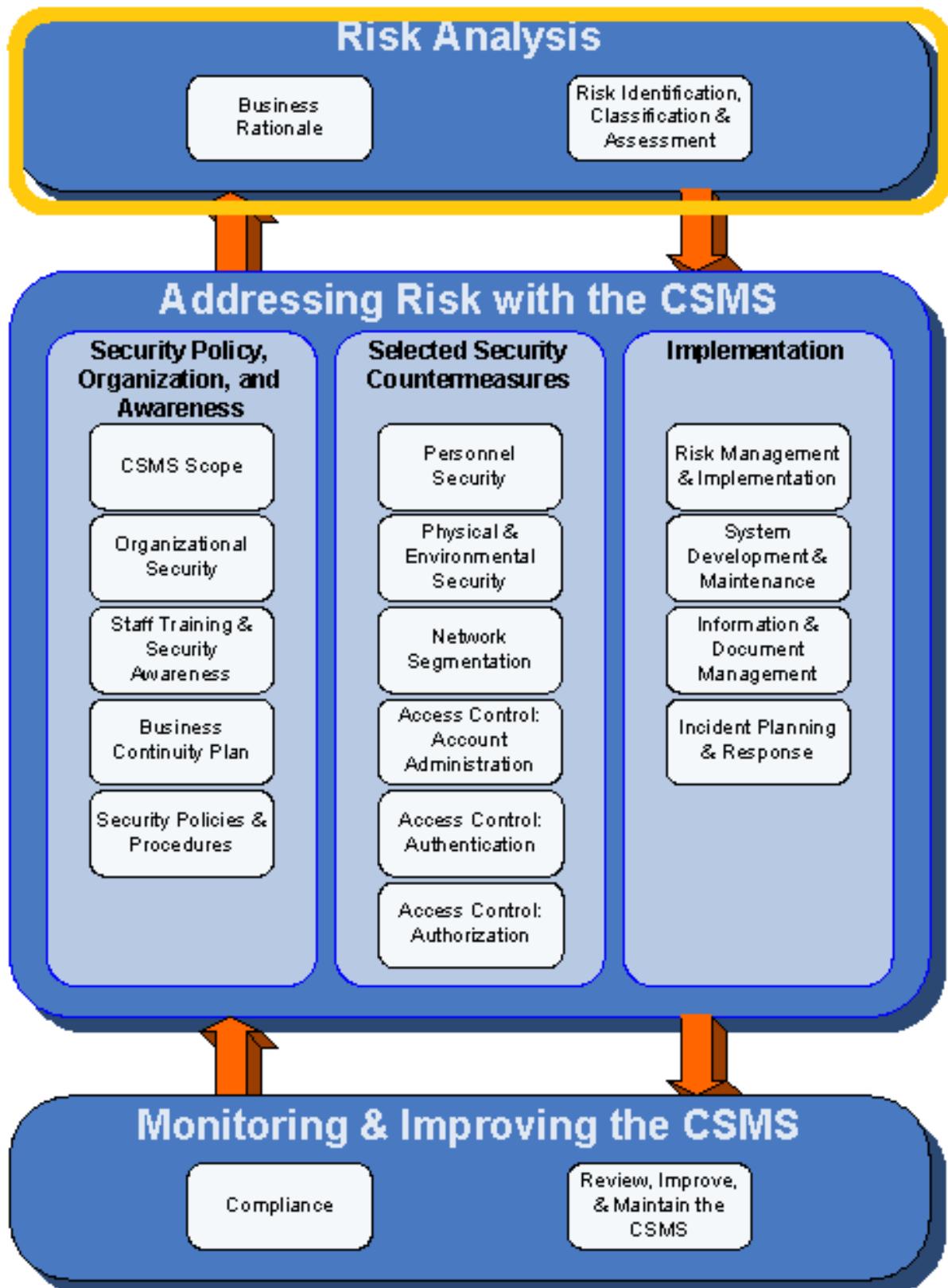
Additional Resources

Additional Resources

Additional Resources







S=Safety E=Environmental F=Financial R=Reputation

Risk Colors/Numbers from Stakeholder Risk Matric Chart. Typical Green (little or no risk) to Yellow, Orange, Red (High Risk)

UTL=Unmitigated Threat Likelihood SL-T=Security Level Target MTL=Mitigated Threat Likelihood ATL=Adjusted Threat Likelihood

Zone	Threat Source	Threat Action	Vulnerabilities	Consequence Description	Consequence					SL-T	Countermeasures	MTL	Risk	Recommendations	ATL	Risk							
					Impact																		
					S	E	F	R	Max														
Process Control Zone	Authorized personnel	Inserts USB into Operator Station with general malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No antivirus	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24 - 72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	5	15	2	* Policies and procedures	5	15	* Disable unused USB ports (e.g. GPO, registry, SEP, etc.) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	2	6					
		Inserts USB into Operator Station with targeted malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No antivirus	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Policies and procedures	2	10	* Disable unused USB ports (e.g. GPO, registry, SEP, etc.) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	1	5					
		Plugs laptop infected with general malware into the Control LAN	* Unused ports on Control LAN switch are enabled * No policy governing use of laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propagation	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24 - 72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	4	12	2	* Laptops are running a supported OS, are patched and running antivirus	4	12	* Develop policies to prohibit use of laptops on Control LAN * Block unused ports on Control LAN switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus	1	3					
		Plugs laptop infected with targeted malware into the Control LAN	* Unused ports on Control LAN switch are enabled * No policy governing use of laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propagation	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Laptops are running a supported OS, are patched and running antivirus	2	10	* Develop policies to prohibit use of laptops on Control LAN * Block unused ports on Control LAN switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus	1	5					
		Engineer remotes into the EWS from the Plant Business Zone using VNC and makes changes without knowledge of current process conditions	* By default VNC credentials are in "clear text" * VNC file transfer capabilities * EWS is dual-homed	* Possible process upset or modification leading to loss of batch	1	1	2	1	2	4	8	1		4	8	* Develop and enforce MoC process * Eliminate VNC	2						
		Unauthorized person uses the VNC credentials to gain access to EWS	* No lock-out on VNC	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	3	15	2		3	15	* Develop and enforce MoC process * Eliminate VNC	1	5					

MEMBERSHIP	TRAINING & CERTIFICATIONS	STANDARDS & PUBLICATIONS	CONFERENCES & EVENTS	NEWS & PRESS RELEASES	RESOURCES	TECHNICAL TOPICS	PROFESSIONAL DEVELOPMENT	STORE
------------	---------------------------	--------------------------	----------------------	-----------------------	-----------	------------------	--------------------------	-------

Home > Training and Certifications > ISA Certification > Certificate Programs > ISA/IEC 62443 Cybersecurity Certificate Programs Frequently Asked Questions

A A A

ISA/IEC 62443 Cybersecurity Certificate Programs Frequently Asked Questions

- Program Definition
- Training Course Requirements
- Documentation
- Fees
- Testing
- Examination Process
- Renewal
- General

Program Definition

Why did ISA develop the ISA/IEC 62443 Cybersecurity Certificate Programs?

ISA has developed this program to increase knowledge and awareness of the ISA/IEC 62442 standards. The first certificate in the program is the ISA/IEC 62443 Cybersecurity Fundamentals Specialist. Other specialization certificates are also available in the areas of risk assessment, system design, and operations/maintenance.

The new ISA/IEC 62443 Cybersecurity Fundamentals Specialist certificate program is designed for professionals involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology and understanding of the material embedded in the ISA/IEC 62443 standards.

Who can say they hold a certificate?

The ISA/IEC 62443 Cybersecurity certificates are awarded to those who successfully complete a designated training course and pass a 75-100 question multiple choice exam.

How does the ISA/IEC 62443 Cybersecurity Certificate Program compare to other security programs?

Review the [comparison chart](#) here.

- top -

Training Course Requirements

Why are courses required for the ISA/IEC 62443 certificate program exam candidates?

Certificate programs are typically associated with mastery of specific course content and may or may not require work experience. The ISA/IEC 62443 certificate program was developed by ISA working with industry experts. The program(s) increase knowledge/awareness and application of the ISA/IEC 62443 standard through mastery of the course material and examination.

What training courses can I take to qualify to take the ISA/IEC 62443 Cybersecurity Fundamentals certificate exam?

ISA's two-day classroom course, Using the ISA/IEC 62443 Standards to Secure Your Industrial Control System ([IC32](#)), must be successfully completed in order to be eligible to take the ISA/IEC 62443 Cybersecurity Fundamentals certificate exam. Or, ISA's multi-week, online course: Cyber Security for Automation, Control and SCADA Systems ([IC32E](#)) is also an eligible option to complete and sit for the exam.

For other exam specialization areas, there are specific related coursework for same.

What if I already took the IC32 or IC32E courses?

If you took either course LESS THAN one year from the date you wish to take the exam, you do not have to retake the course and can register for the certificate exam. If you took either course MORE THAN one year from the date you wish to take the exam, you must retake the course in order to be eligible to sit for the certificate exam.

Will course participants receive CEUs for the courses taken?

Yes. The number of CEUs is determined by the number of instructional hours, and awarded upon successful completion of the course. Completing course post-tests and receiving CEUs for course completion are not connected to passing scores on one of the certificate exams.

What if a course is rescheduled by a candidate or ISA?

A candidate is not eligible to sit for the exam until he or she successfully completes the prerequisite course. [Click here](#) for information regarding course cancellations/rescheduling.

- top -

Documentation

What paperwork must be completed to take one of the exams?

No application is required for the ISA/IEC 62443 Cybersecurity certificate exams.

What are the pre-requisites for the certificate program?

There are no required prerequisites for this program; however, it is highly recommended that applicants have:

Apply for the ISA/IEC 62443

Requirements

FAQs

Take the Exam

Renew

Directory

Onsite ISA Training at Your Plant

Search for ISA Cybersecurity Training

ISA's Cybersecurity Resources Brochure

White Paper on Cybersecurity

Certifications and Certificates

- Three to five years of experience in the IT cybersecurity field with some experience in an industrial setting-with at least two years specifically in a process control engineering setting
- Some level of knowledge or exposure to the ISA/IEC 62443 standards
- **More advanced courses have recommended coursework, in addition to experience, but it is not required.**
- **Certificate 1 attainment is required to go onto all other certificate levels.**

- top -

Fees

What are the fees for the certificate program?

Fees for required courses can be found on the course registration page. The exam fee for an ISA/IEC 62443 certificate exam is \$200. There are no group discounts for certificate exam fees. This fee includes one electronic exam.

Can an exam be rescheduled without incurring fees?

Applicants may reschedule an exam appointment during the six (6) month eligibility period by contacting Prometric at least 2 days (48 hours) prior to the scheduled exam time for Prometric locations in the United States/Canada and at least 5 days (120 hours) prior to the scheduled exam time for all other Prometric locations. No reschedule fee will apply.

Prometric Location	Advance Notice Required to Reschedule with no fee
--------------------	---------------------------------------------------

United States/Canada	At least 2 days (48 Hours) Prior to Scheduled Exam Date
----------------------	---------------------------------------------------------

All other locations	At least 5 Days (120 hours) Prior to Scheduled Exam Date
---------------------	----------------------------------------------------------

What are the reschedule fees?

Candidates who do not appear for their scheduled exam appointment and do not give proper advance notice of intent to reschedule their exam will incur a fee of \$150.

Can a candidate retest and what is the retest fee?

Applicants may retest within the six (6) month eligibility period for a fee of \$150. If you are outside the six (6) month eligibility period, you must register again for the required course and exam and re-take both.

What if a candidate cannot make the scheduled appointment or is late for the appointment?

For candidates who fail to appear for a scheduled exam, or arrive more than 15 minutes after the scheduled start time, the \$150 reschedule fee will apply. The exam must be rescheduled within the candidate's six (6) month eligibility period.

What forms of payment does ISA accept for the certificate program fees?

ISA will accept check, certified check, money order, or wire transfer (in U.S. Dollars), credit card and purchase orders. Make checks payable to ISA. For wire transfer account information, please contact ISA Customer Service at info@isa.org or +1 919-549-8411. ISA accepts AMEX, Discover Card, Master Card, and VISA credit cards.

Payment should be received with the course registration.

Is the certificate program exam fee refundable?

ISA/IEC 62443 certificate program fees are refundable, less a \$50 processing fee, if you decide not to take the exam after completing the course and within the six-month eligibility window.

- top -

Testing

The ISA/IEC 62443 Cybersecurity Certificate Program exams are offered electronically through the Prometric global network of testing centers in early 2014. For testing center locations, visit www.prometric.com/isa. The exams are not offered the day after completing the required course.

How does one become eligible to take an ISA/IEC 62443 certificate exam?

Certificate program applicants must register for the required course and the exam, and successfully complete the required course. [Click here](#) to review the certificate program requirements.

When will applicants find out if they are eligible to take an ISA/IEC 62443 certificate program exam?

Within 5 business days of completion of the required course, an eligibility email that contains the information needed to schedule a paper/pencil exam (or a computer-based exam at Prometric, when available) will be sent to the exam candidate.

How long is an applicant eligible to take an ISA/IEC 62443 certificate program exam?

The certificate exam and any retests must be taken within six (6) months of the last day of the certificate program course.

What if the required course is not completed?

If the applicant is still interested in pursuing the certificate, he/she must register for the course and exam again and re-take the course. Once the course is successfully completed, the candidate is eligible to sit for the exam.

What is a passing score for an ISA/IEC 62443 certificate program exam?

Passing scores vary for all level exams based upon different number of questions at each level.

What if a candidate does not pass the certificate exam?

If a candidate fails the exam, he/she may retest one time within the initial six (6) month eligibility window for a fee of \$150. If an applicant does not pass the exam within the six (6) month window after the course and would like to receive the certificate, the

applicant must register for the course and exam again and re-take both.

An ISA99/IEC 62443 certificate program exam must be taken within six (6) months of the last day of the certificate program required course. If a candidate fails the exam, he/she may retest one (1) time within the six (6) month eligibility period. If a candidate does not pass the exam within the six (6) month window after the course and would like to receive the certificate, the applicant must register for the course and exam again and re-take both.

Once the computer-based exam is available, applicants who successfully complete the program requirements will receive an email with an eligibility code to use to schedule their exam through Prometric. In this case, you would go to www.prometric.com/isa to review locations and schedule an appointment.

Once scheduled, how is an exam confirmed?

Exam appointments are confirmed by Prometric via email. ISA does not provide candidate email addresses to Prometric—the candidate provides the email address they wish to receive the exam confirmation.

What if an exam confirmation is not received from Prometric?

Contact Prometric Candidate Care at 800-853-6769 and ask that it be emailed to you again. ISA cannot provide the confirmation for you.

Who should be contacted to reschedule an exam appointment?

Candidates must contact ISA if an exam appointment needs to be rescheduled. If the appointment is not cancelled at least 2 days in advance at Prometric locations in the United States/Canada or at least 5 days in advance at other Prometric locations, a reschedule form must be completed and sent to ISA with payment before the candidate eligibility can be re-set.

- top -

Examination Process

Once a candidate is eligible, how much time is available for testing?

The eligibility period to take a certificate exam is six (6) months from the date the course is completed. You must complete all testing within the six (6) month eligibility period, including any reschedules or retests. Candidates have two hours to complete the exam.

Are there testing windows for taking certificate exams?

There are no testing windows for taking any of the certificate exams. Testing center availability is set by each Prometric testing center in the Prometric network. Some Prometric testing centers offer evening and Saturday appointments. Paper/Pencil exams can be schedule through ISA customer service: +1 919-549-8411.

When should a candidate arrive at the testing center?

Candidates should arrive at the testing center no later than 30 minutes prior to the scheduled exam time to sign-in and receive instruction. All examinations are given in a two hour time period.

What if the testing center cannot accommodate an exam appointment?

If technical difficulties or inclement weather cause the cancellation of an appointment or the closure of a Prometric testing center, Prometric will attempt to contact the candidate using the phone numbers provided to them by ISA. Last minute cancellation situations will be handled on a case-by-case basis, and ISA and Prometric will work together to reschedule the candidate as quickly as possible.

What should be brought to the testing center?

The Confirmation Letter from Prometric and a valid government issued photo ID with signature.

Are there any materials that are not allowed at the testing center?

All exams are closed book. No reference material will be allowed in the testing center. A location for personal items such as a pocket book, palmtop, mobile phone, or pager will be made available to you. Please note that storage space will be limited.

Will anything be provided to candidates at the testing center?

A whiteboard with marker will be provided when candidates check-in at the testing center, and a scientific calculator will be available as a hot button on the computer screen.

When are candidates notified of their certificate status?

Results are reported immediately at the testing center. If a candidate passes, a certificate will be mailed within thirty (30) days of the exam date. Failing candidates receive a diagnostic report of how they performed on the exam at the testing center.

What if the testing center does not provide the testing results?

If the testing center is unable to provide testing results, have the test center administrator complete a candidate incident report and then let ISA know by calling Customer Service at +1 919-549-8411.

- top -

Renewal

Because the ISA/IEC 62443 Cybersecurity Certificate Programs are *certificates* and not *certifications*, you are not required to renew your ISA/IEC 62443 certificate(s); however, once obtained your certificate(s) will only be considered **current** for three (3) years. After your three-year expiration date, your certificate's status will no longer be considered active and you will not be able to claim that you hold a current/active ISA/IEC 62443 certificate. [Click here](#) to learn more about extending the current status of your certificate(s).

- top -

Displaying Your ISA/IEC 62443 Certificate

Program Credentials

How do I get a copy of my ISA/IEC 62443 certificate in case I lose it or if my supervisor wants one?

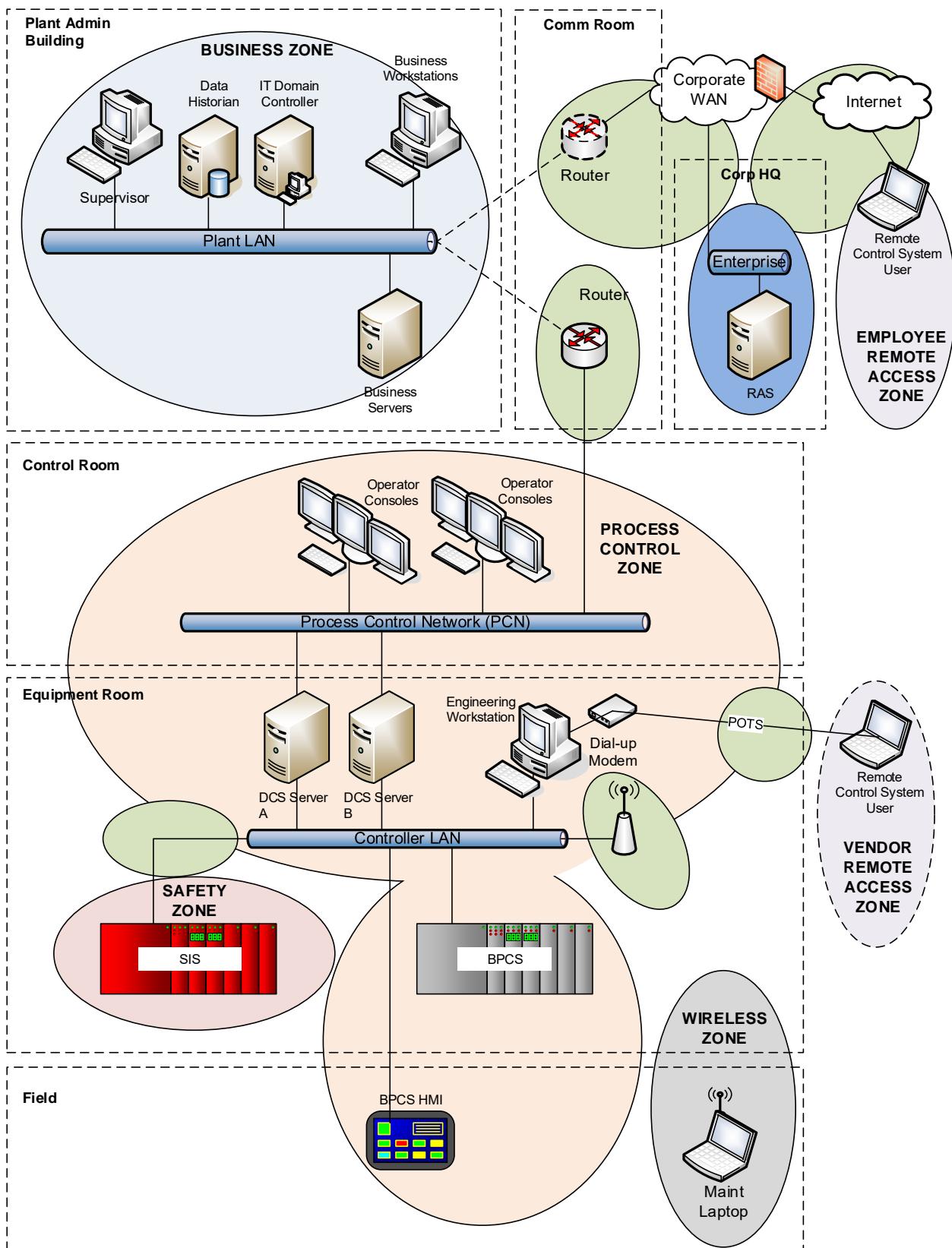
To receive a duplicate copy of your certificate, send a written request to ISA with your mailing address and payment of \$15 for a duplicate certificate. Once your payment is received, a certificate will be mailed to you.

How should I display my ISA/IEC 62443 certificate designation(s) on business cards, in signature blocks, etc.?

ISA recommends the following for displaying or noting your credentials:

- If you have achieved ISA/IEC 62443 Certificate 1: **ISA/IEC 62443 Cybersecurity Fundamentals Specialist** (ISA/CFS)
- If you have achieved ISA/IEC 62443 Certificate 2: **ISA/IEC 62443 Cybersecurity Risk Assessment Specialist** (ISA/CRS)
- If you have achieved ISA/IEC 62443 Certificate 3: **ISA/IEC 62443 Cybersecurity Design Specialist** (ISA/CDS)
- If you have achieved ISA/IEC 62443 Certificate 4: **ISA/IEC 62443 Cybersecurity Maintenance Specialist** (ISA/CMS)

Because these are certificate programs and not certification programs, you should not list your ISA/IEC 62443 certificate designations directly after your name. On your business card (signature block, resume, etc.), you should display/include your ISA/IEC 62443 certificate designation in an area distinctly separate from your name and certificate/licensure/degree designations (e.g. CAP, PE, MBA, etc.). When possible, include "Certificate" or "Certificate Holder" after your ISA/IEC 62443 designation listing (e.g. ISA/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Holder).



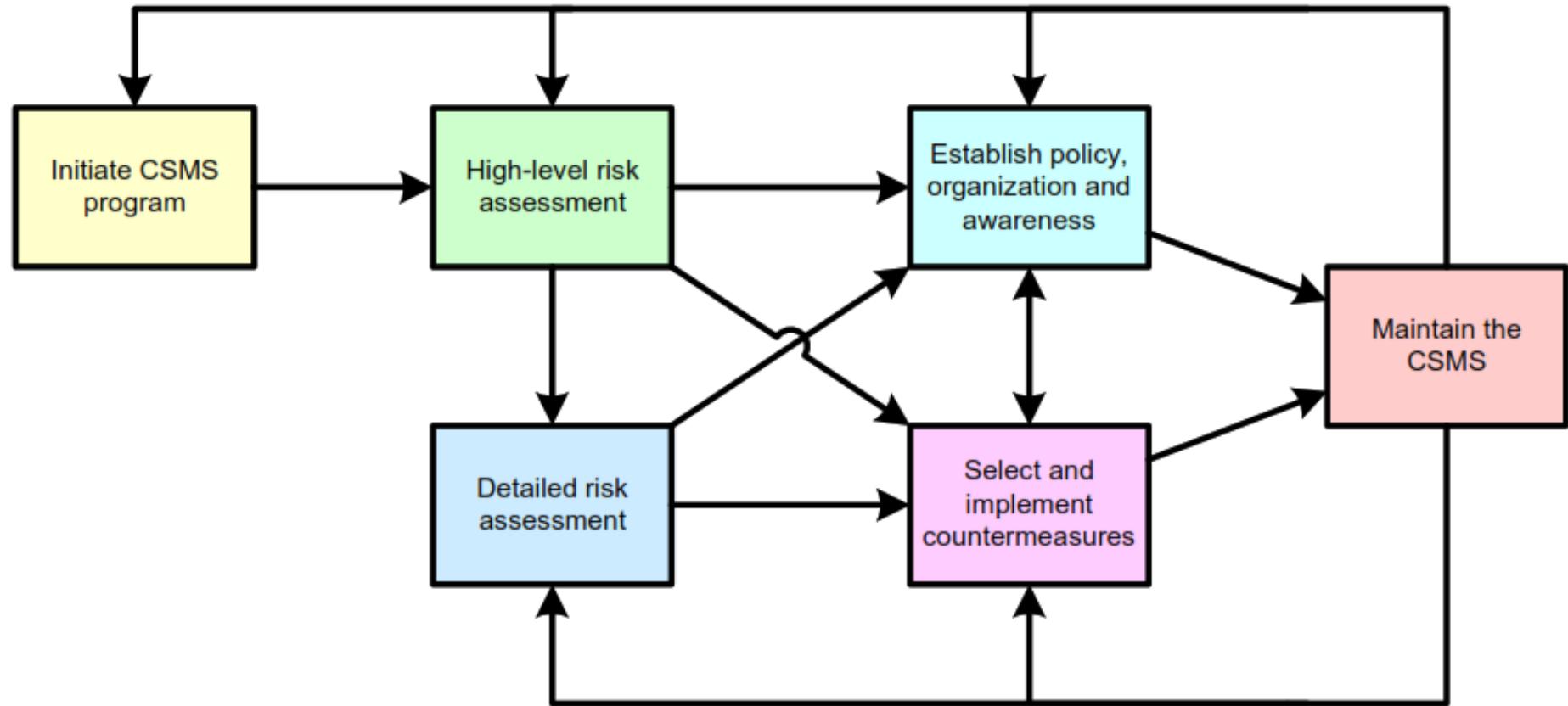


Setting the Standard for Automation™

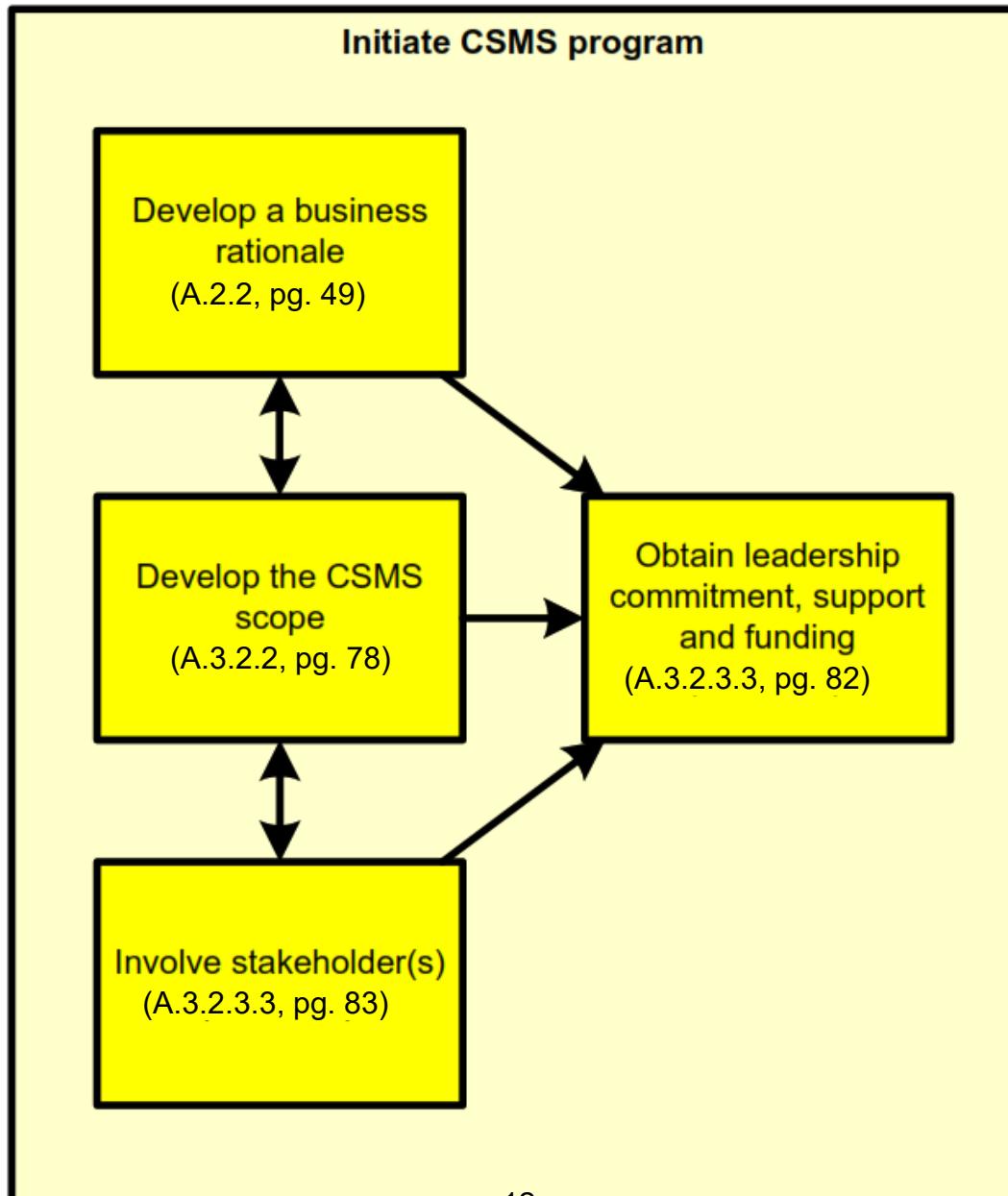
CSMS Boils Down to Six Top Level Activities

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits
©ISA, IC32E

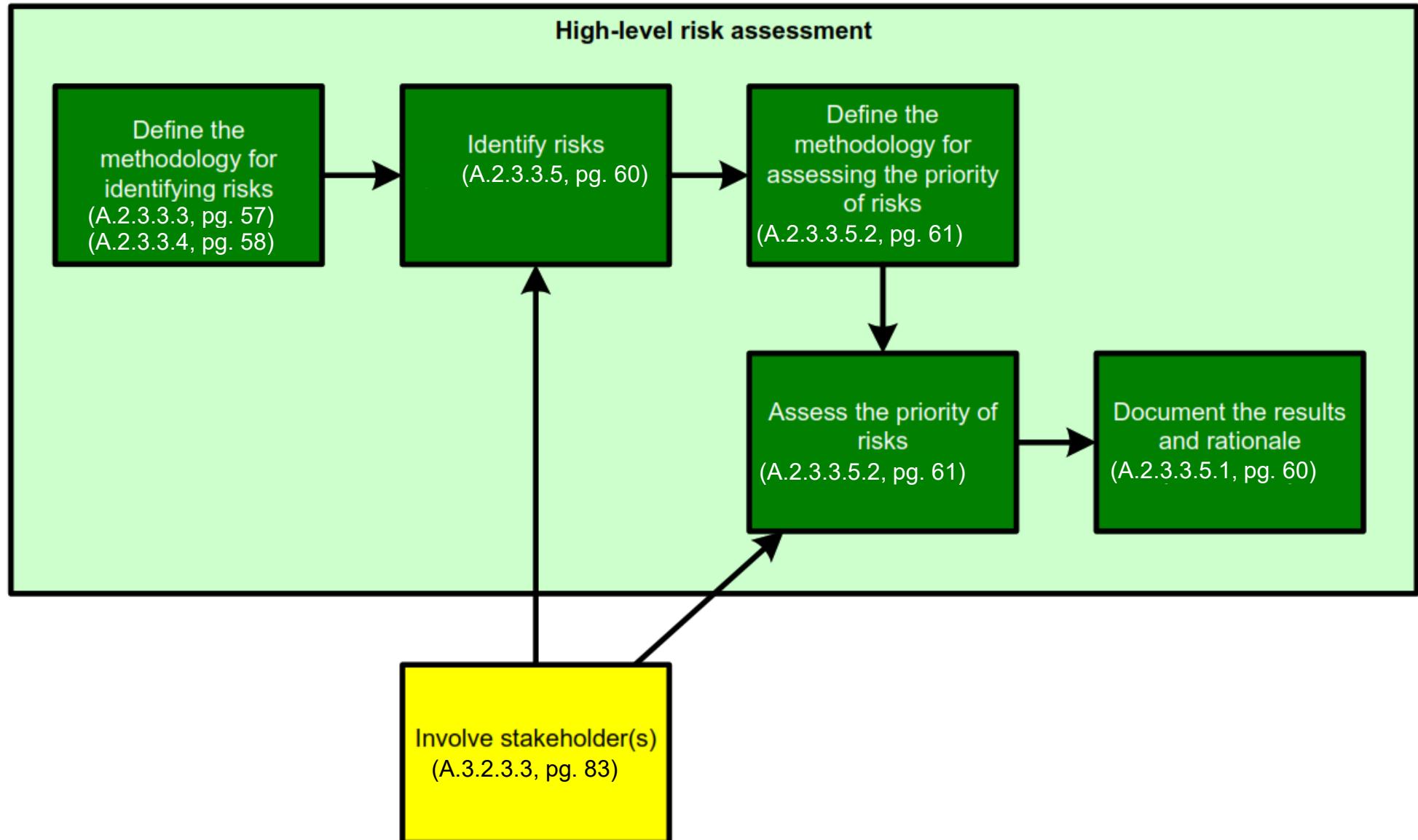
Description of the Process



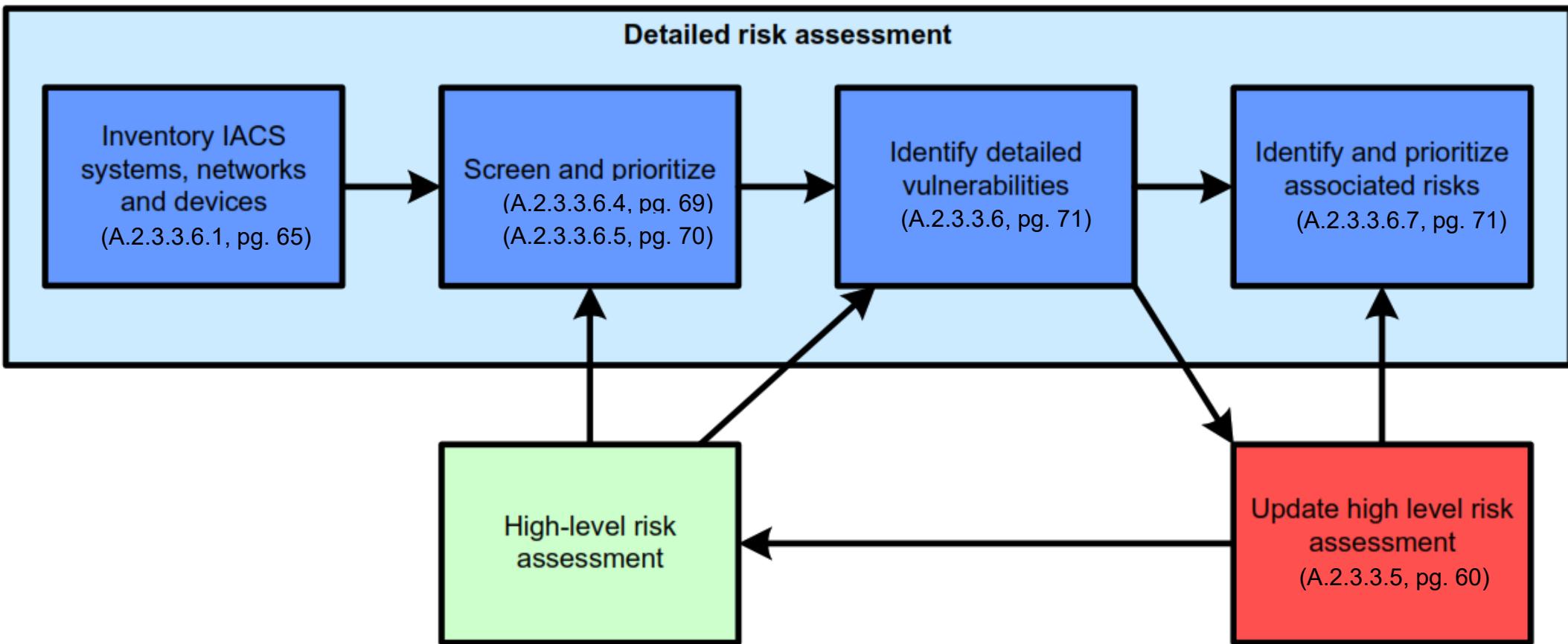
Initiate the CSMS Program



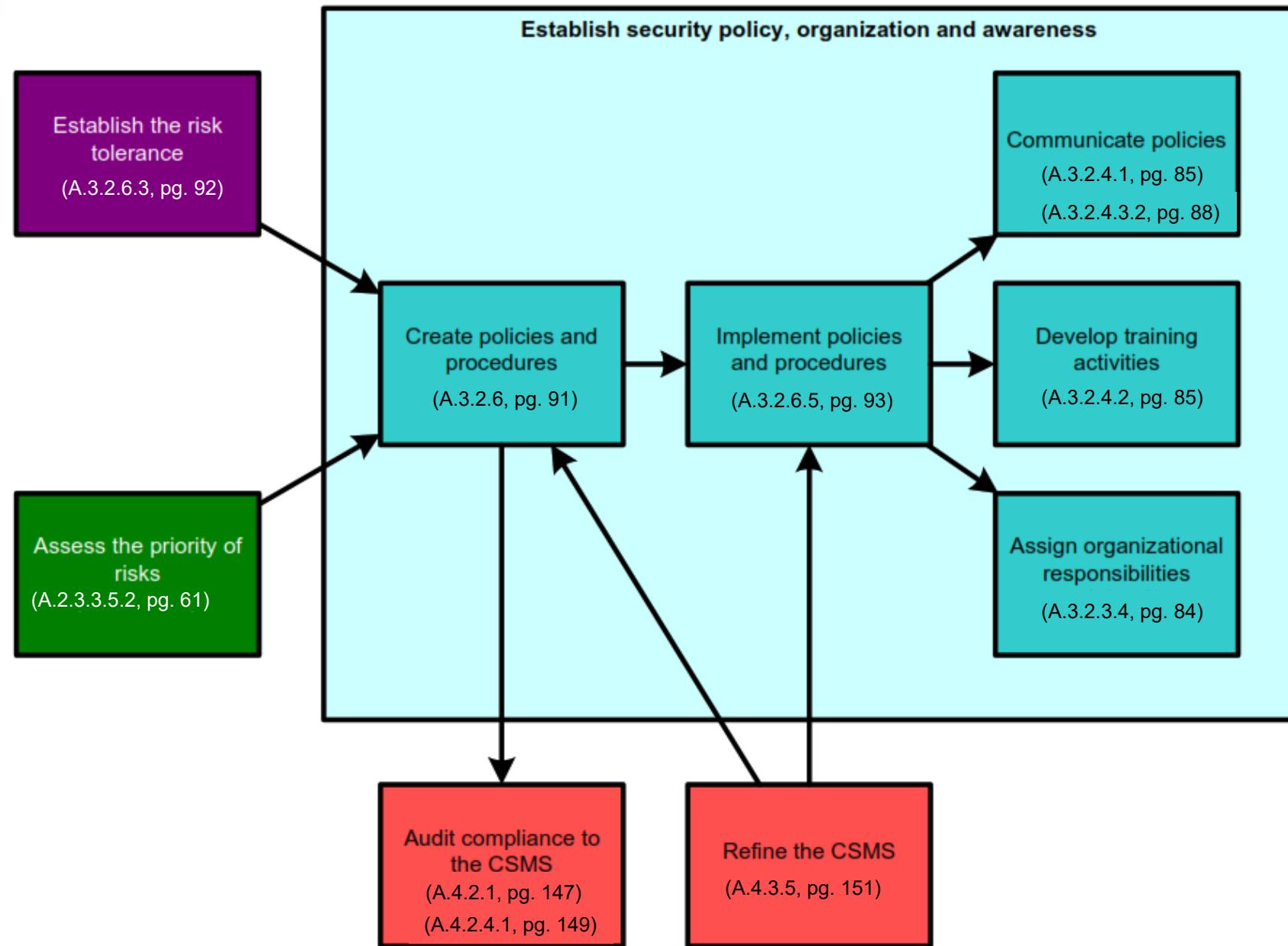
High-level Risk Assessment



Detailed Risk Assessment

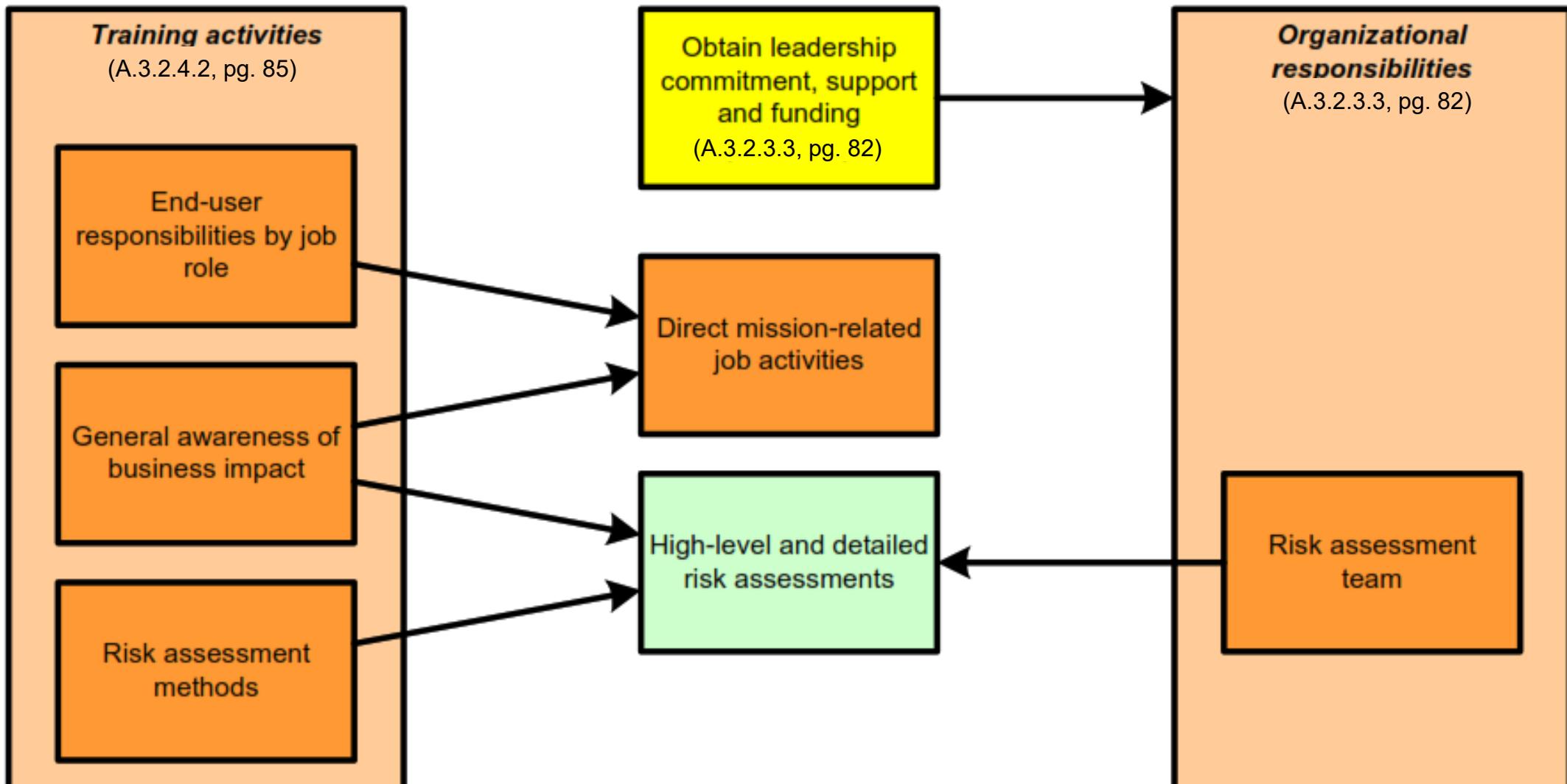


Establish Policy, Organization & Awareness



Training and Assignment of Responsibilities (Cont'd)

CSMS program

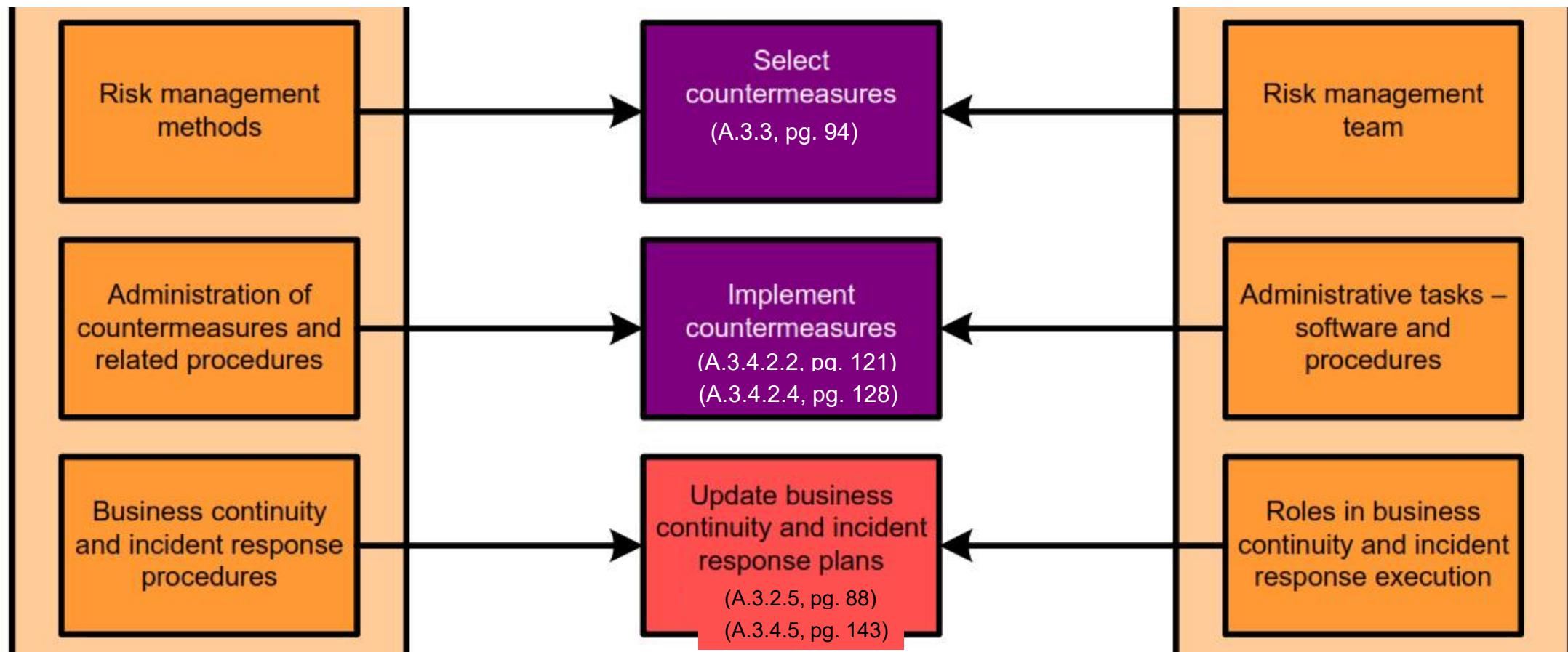


Training and Assignment of Responsibilities (Cont'd)

Training activities (Cont'd)

CSMS program (Cont'd)

Organizational responsibilities (Cont'd)

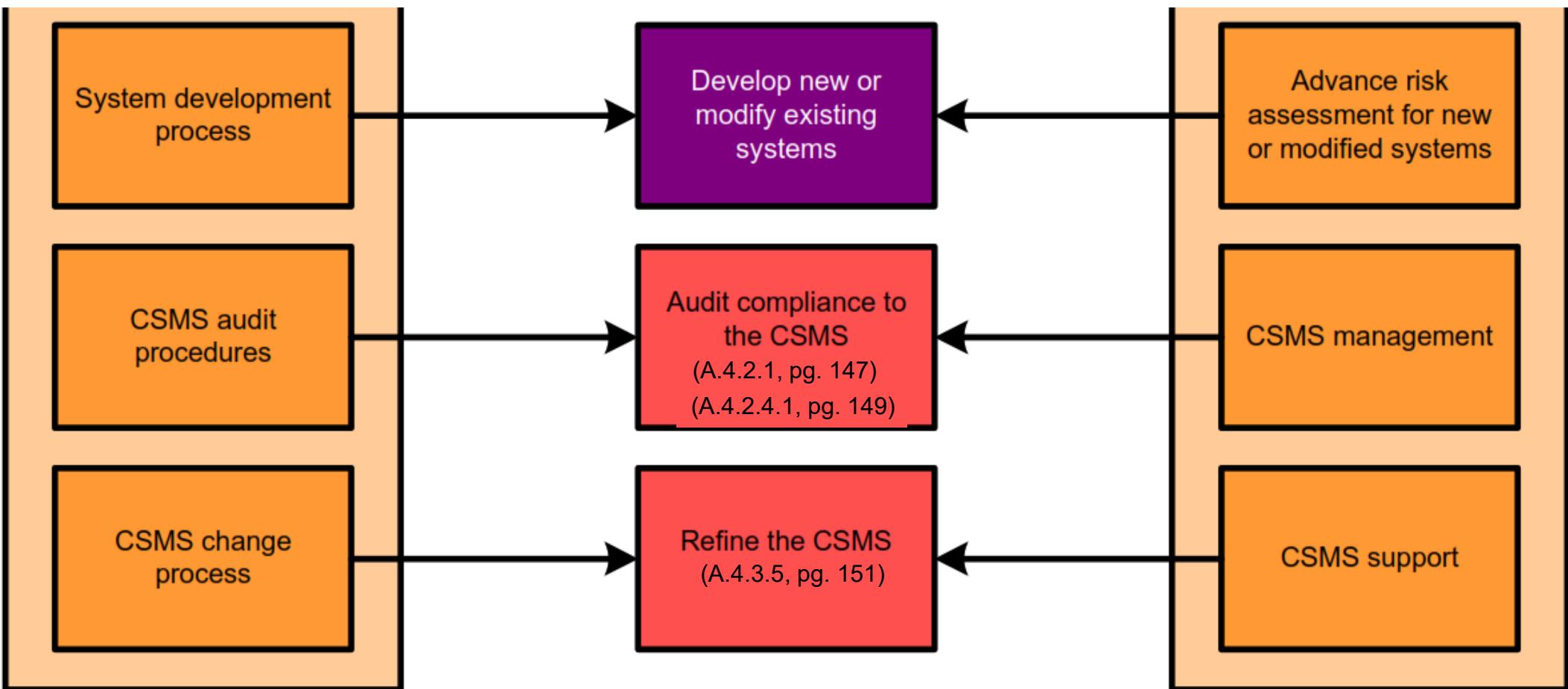


Training and Assignment of Responsibilities (Cont'd)

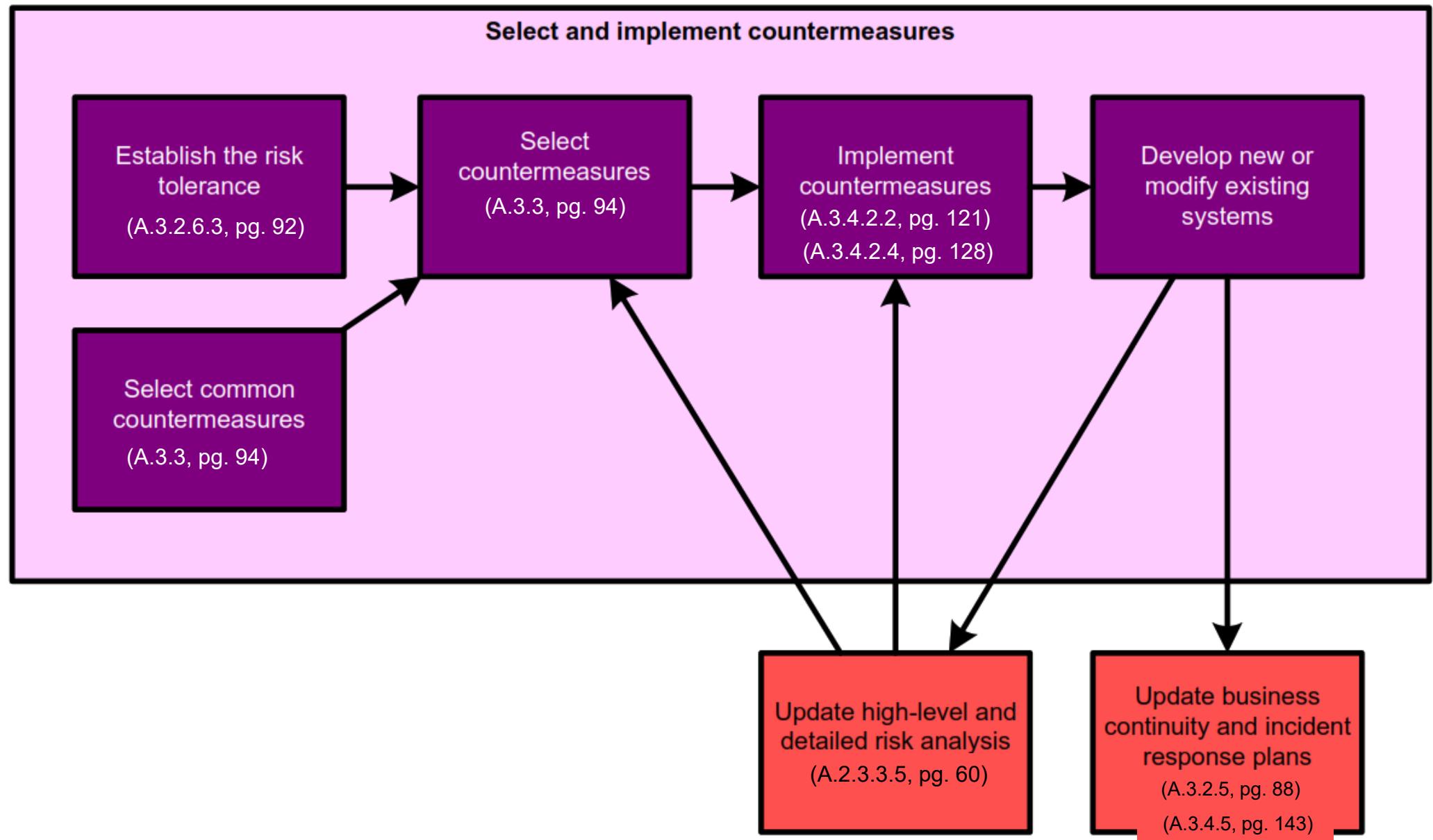
Training activities (Cont'd)

CSMS program (Cont'd)

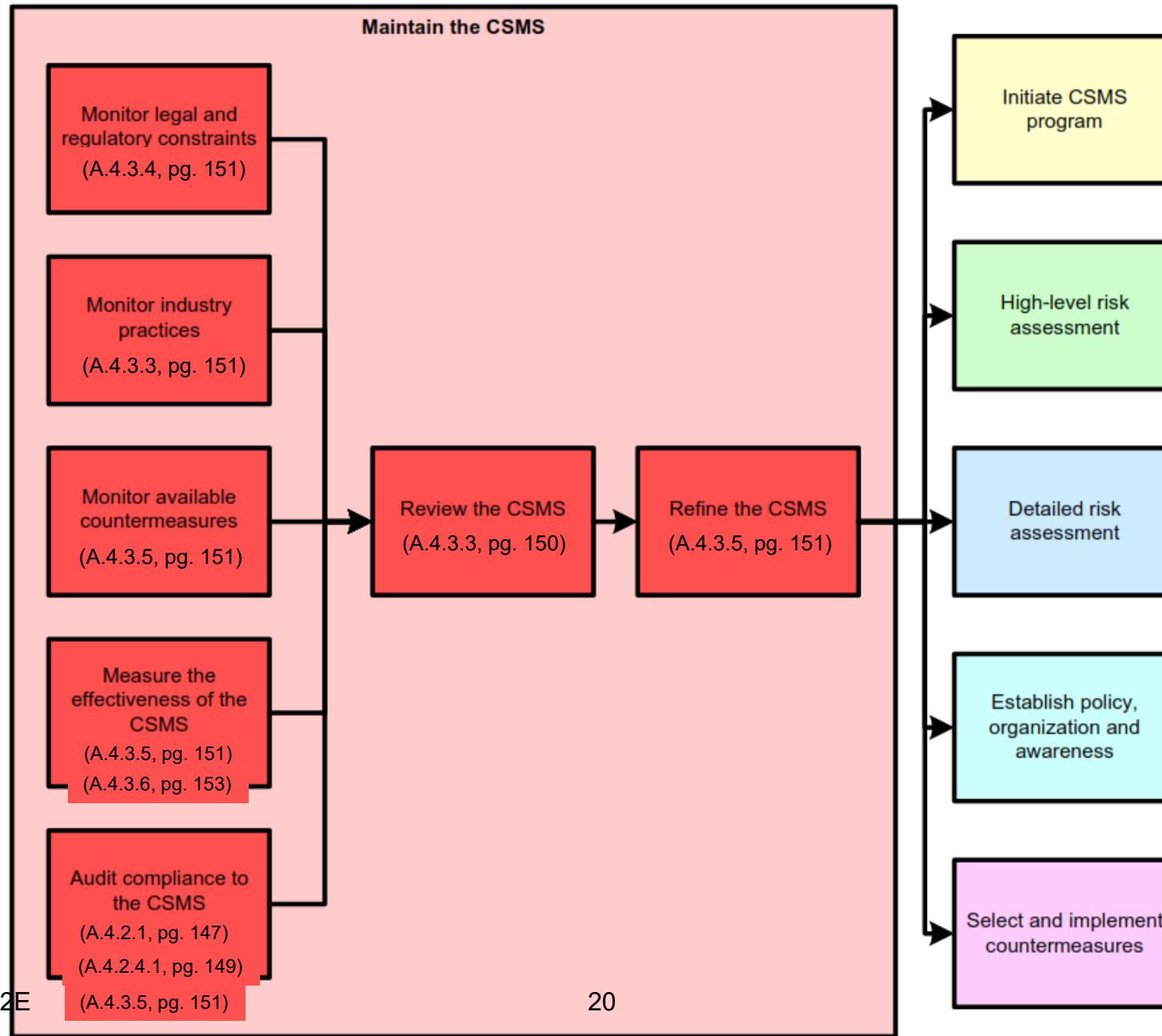
Organizational responsibilities (Cont'd)



Select and Implement Countermeasures



Maintain the CSMS



General

ISA-62443-1-1

Concepts and models



ISA-TR62443-1-2

Master glossary of terms and abbreviations



(TR) ISA-62443-1-3

System security conformance metrics



ISA-TR62443-1-4

IACS security life-cycle and use-cases



Policies & Procedures

ISA-62443-2-1

Requirements for an IACS security management system



ISA-TR62443-2-2

Implementation guidance for an IACS security management system



ISA-TR62443-2-3

Patch management in the IACS environment



ISA-62443-2-4

Requirements for IACS solution suppliers



System

ISA-TR62443-3-1

Security technologies for IACS



ISA-62443-3-2

Security risk assessment and system design



ISA-62443-3-3

System security requirements and security levels



Component

ISA-62443-4-1

Product development requirements



ISA-62443-4-2

Technical security requirements for IACS components



Status Key



Published



In development



Planned



Published (under review)



Out for comment/vote

Retrieved 16 Dec 2016



The ISO Open System Interconnection Reference Model (OSI/RM) defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

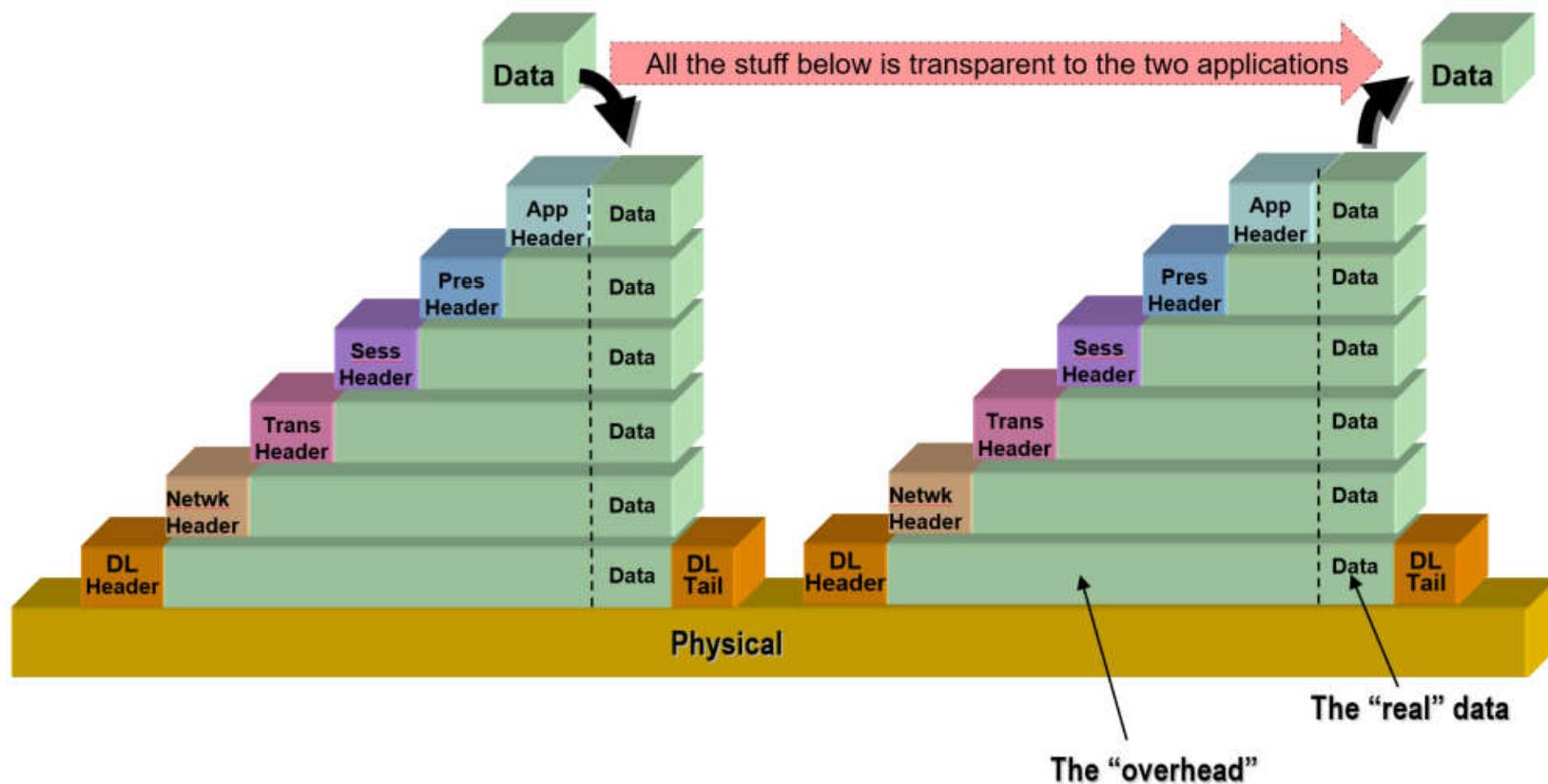
- **Application (Layer 7)** This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
- **Presentation (Layer 6)** This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.
- **Session (Layer 5)** This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
- **Transport (Layer 4)** This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
- **Network (Layer 3)** This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
- **Data Link (Layer 2)** At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
- **Physical (Layer 1)** This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

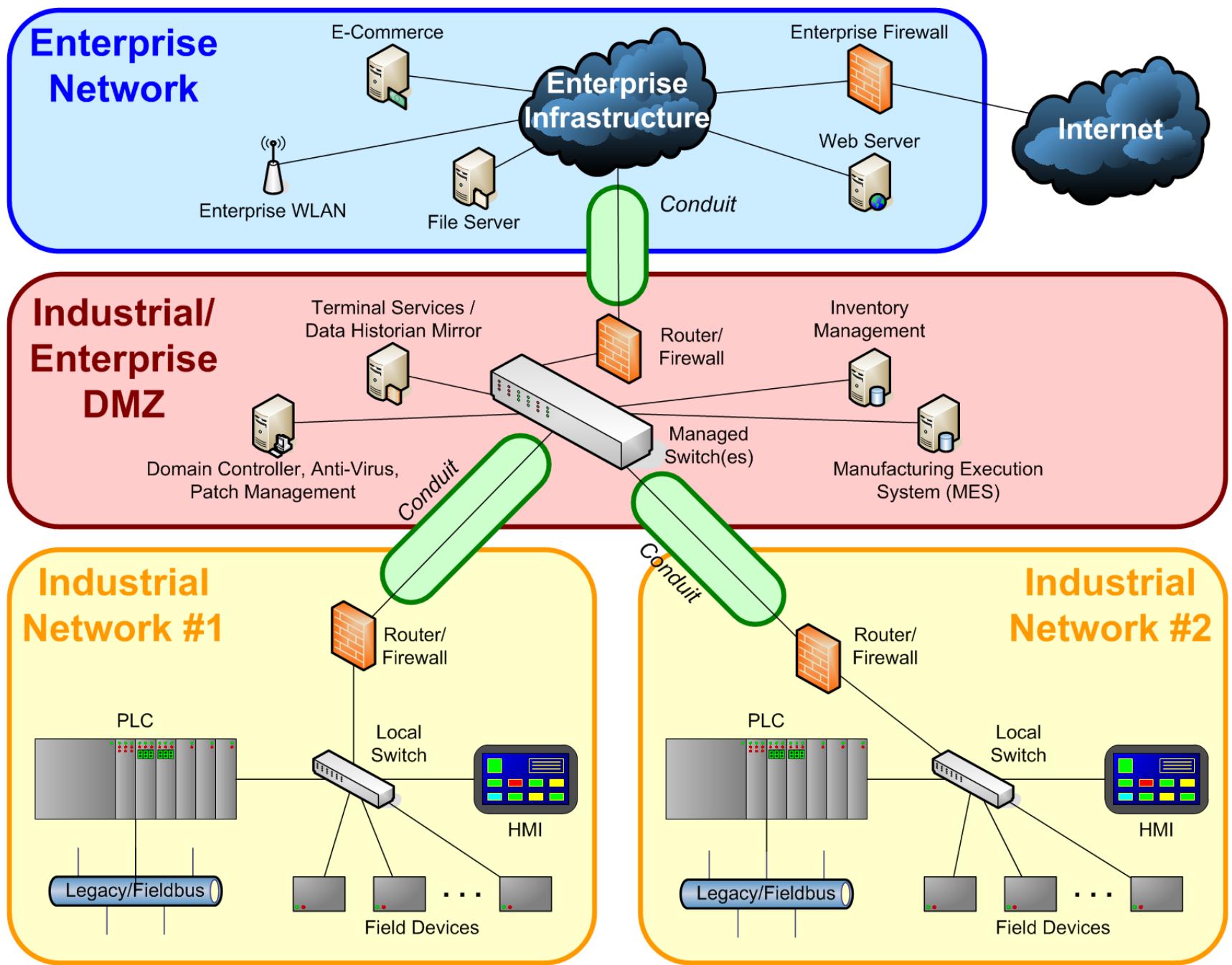
Encapsulating the Data

- **Data** passes down and up through the layers
 - Each layer adds or removes instructions (a header)

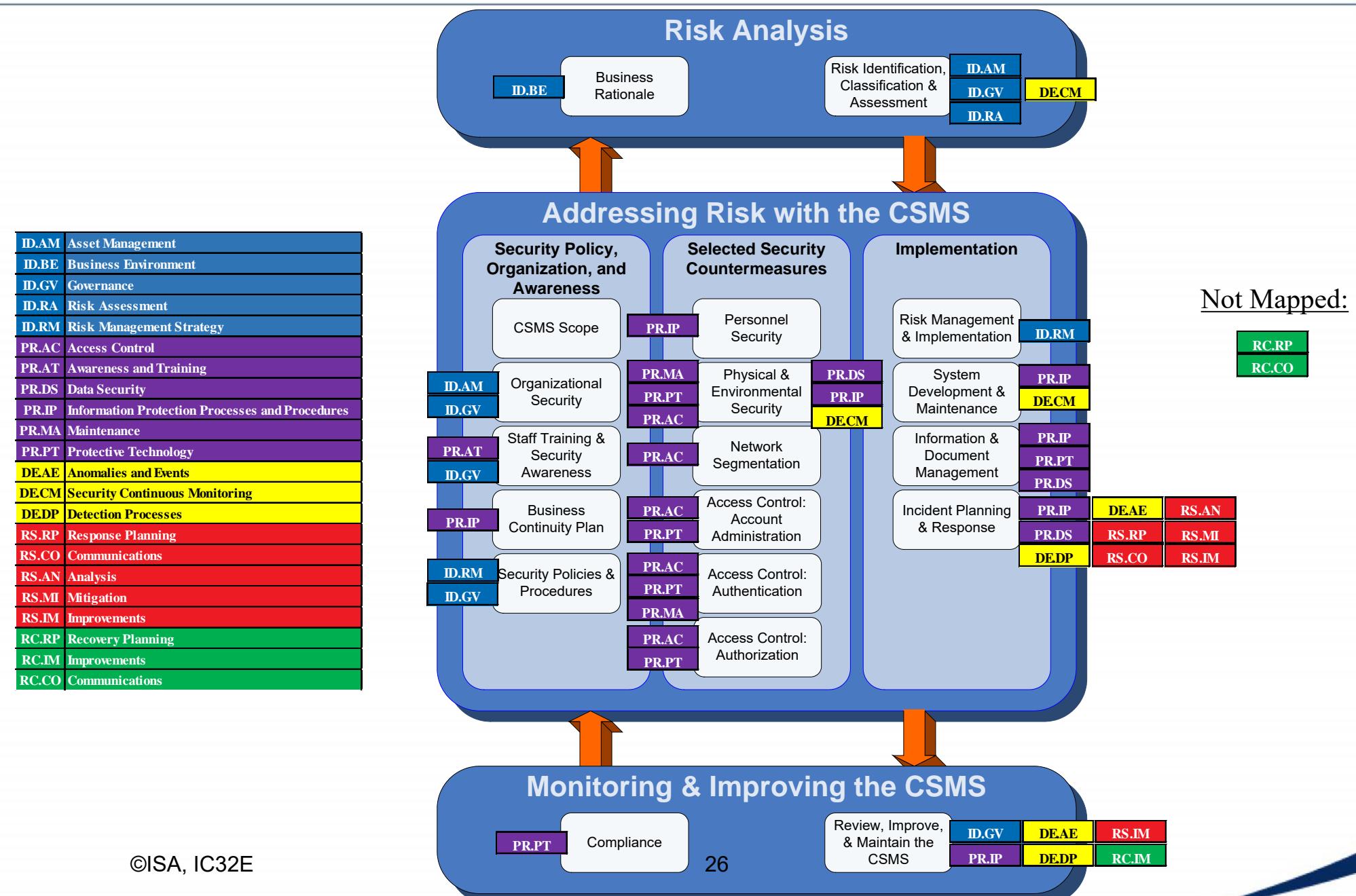
User program sending data (payload)
Down the stack

User program receiving data (payload)
Up the stack





Mapping the NIST Framework Categories to ISA 62443-2-1





Notes

Notes

Notes

Notes

Notes

Notes