ISA™

Setting the Standard for Automation™

How can I use ISA/IEC-62443 (Formally ISA 99) to minimize risk?

^
real

Standards

Certification

Education & Training

Publishing

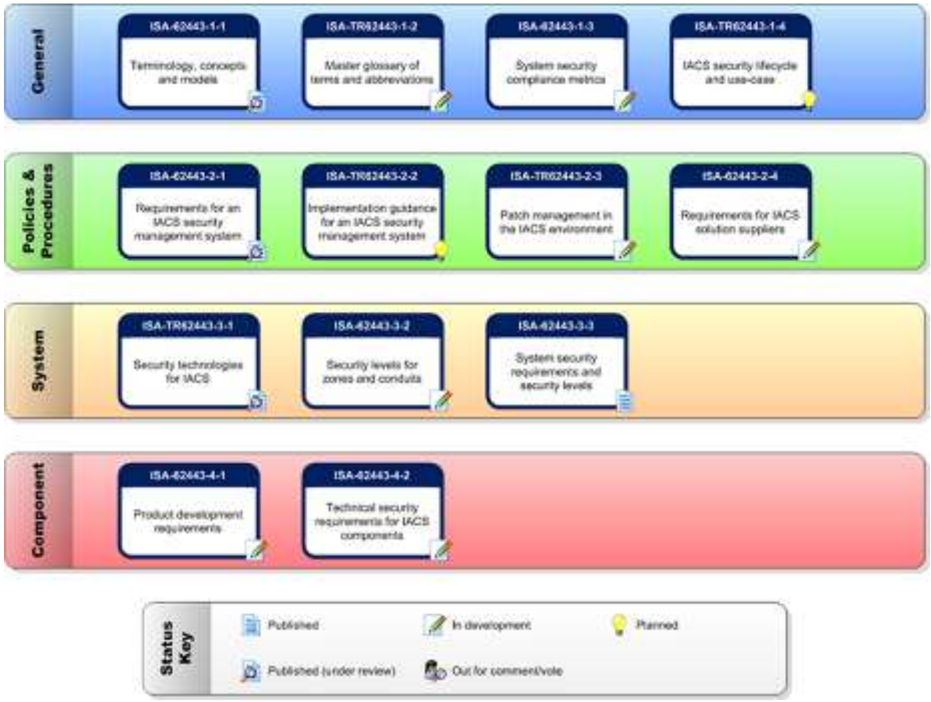
Conferences & Exhibits

Presenter

- Senior consultant in Maverick's Operation Consulting Team. Twenty five year field systems engineer with a California Professional Engineer license, and BA in Economics from California State University Fullerton. Proudly served twenty years as a Marine Safety Officer in the United States Coast Guard Reserve.

What is ISA 62443?

A series of ISA standards that addresses the subject of security for industrial automation and control systems. The focus is on the electronic security of these systems, commonly referred to as cyber security.



General

ISA-62443-1-1 Terminology, concepts and models

ISA-TR62443-1-2 Master glossary of terms and abbreviations

ISA-62443-1-3 System security compliance metrics

ISA-TR62443-1-4 IACS security lifecycle and use-case

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 levels for zones and conduits

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

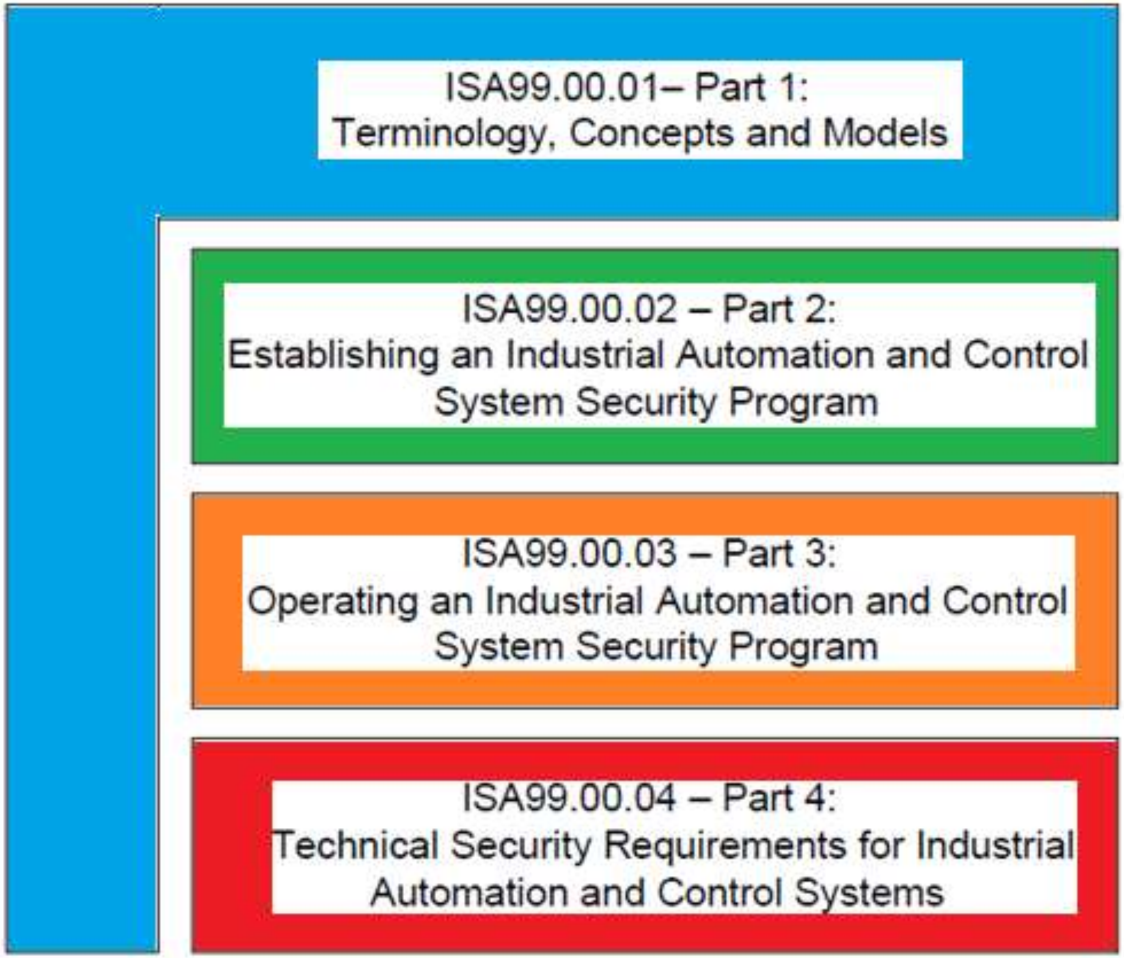
In development

Planned

Published (under review)

Out for comment/vote

What is ISA 62443?



ISA99.00.01– Part 1:
Terminology, Concepts and Models

ISA99.00.02 – Part 2:
Establishing an Industrial Automation and Control System Security Program

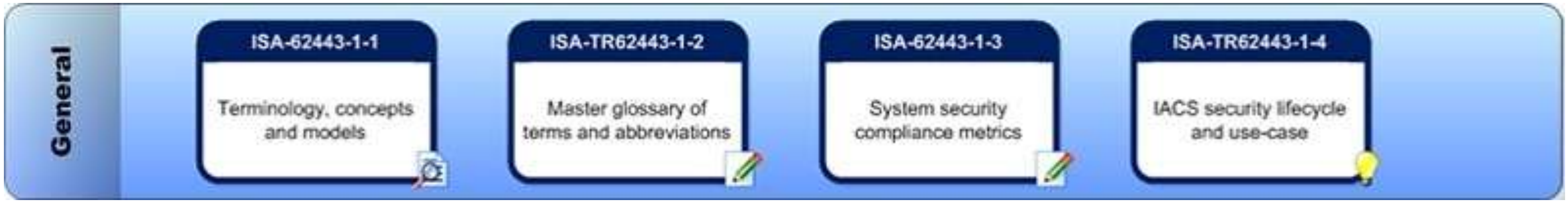
ISA99.00.03 – Part 3:
Operating an Industrial Automation and Control System Security Program

ISA99.00.04 – Part 4:
Technical Security Requirements for Industrial Automation and Control Systems

What is ISA 62443?

Part 1: Terminology, Concepts and Models

Establishes the context for all of the remaining standards in the series by defining a common set of terminology, concepts and models for electronic security in the industrial automation and control systems environment.



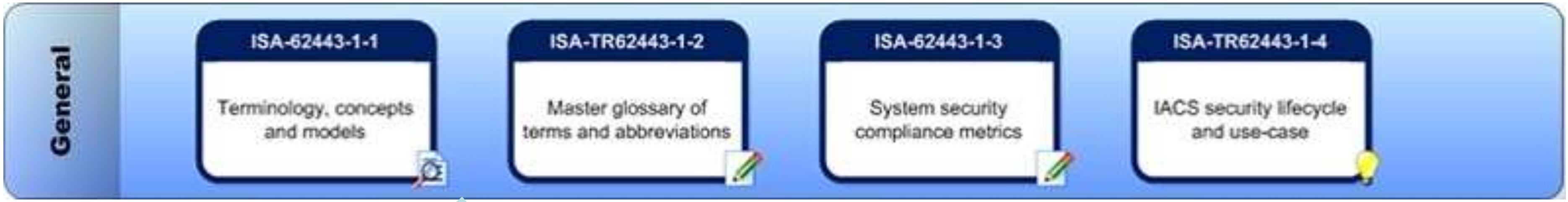
General

ISA-62443-1-1
Terminology, concepts and models

ISA-TR62443-1-2
Master glossary of terms and abbreviations

ISA-62443-1-3
System security compliance metrics

ISA-TR62443-1-4
IACS security lifecycle and use-case



General

ISA-62443-1-1

Terminology, concepts and models

ISA-TR62443-1-2

Master glossary of terms and abbreviations

ISA-62443-1-3

System security compliance metrics

ISA-TR62443-1-4

IACS security lifecycle and use-case

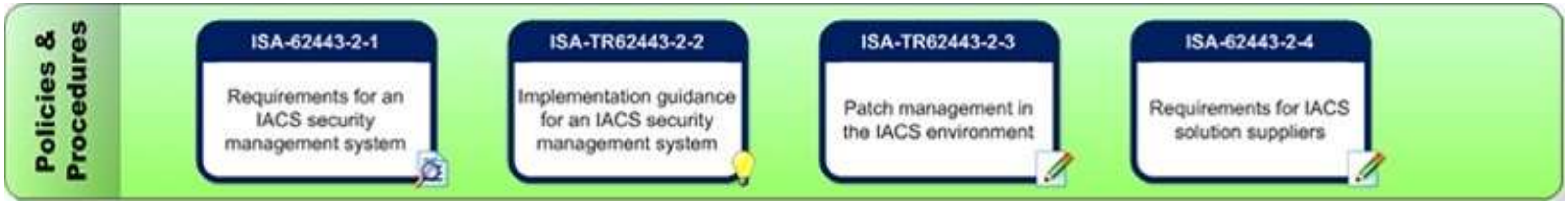
ISA/IEC 62443-1-1

Terminology, Concepts and Models

What is ISA 62443?

Part 2: Establishing an Industrial Automation and Control System Security Program

Describes the elements of a cyber security management system and provide guidance for their application to industrial automation and control systems.



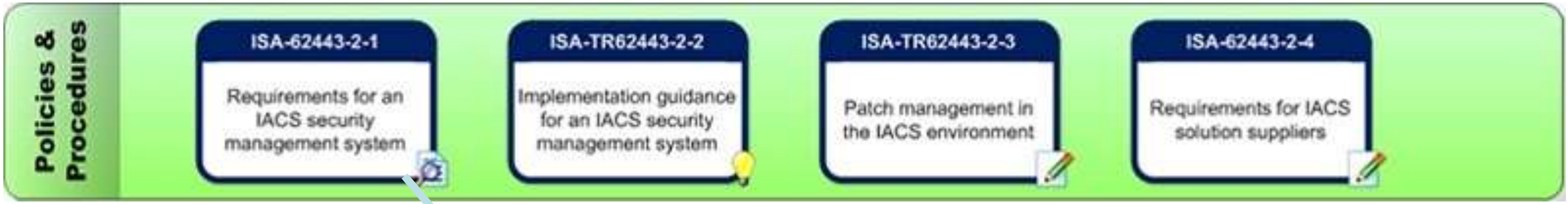
Policies & Procedures

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



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

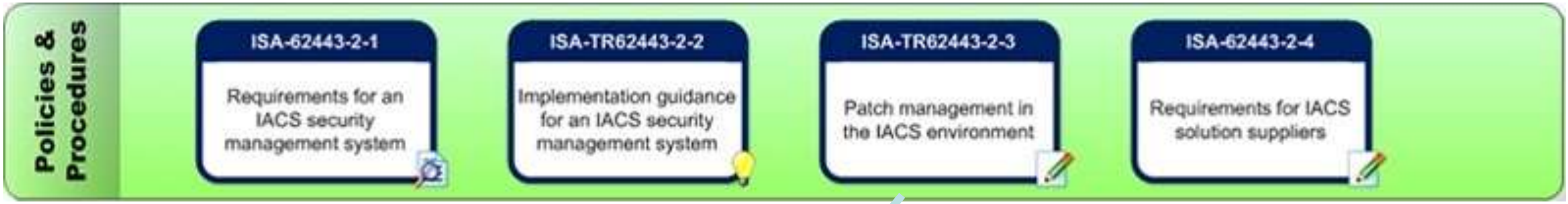
ISA/IEC 62443-2-1

Establishing an Industrial Automation and Control Systems Security

ISA/IEC 62443-2-1

Requirements for an IACS Security Management System

New Name!



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

ISA/IEC 62443-2-3

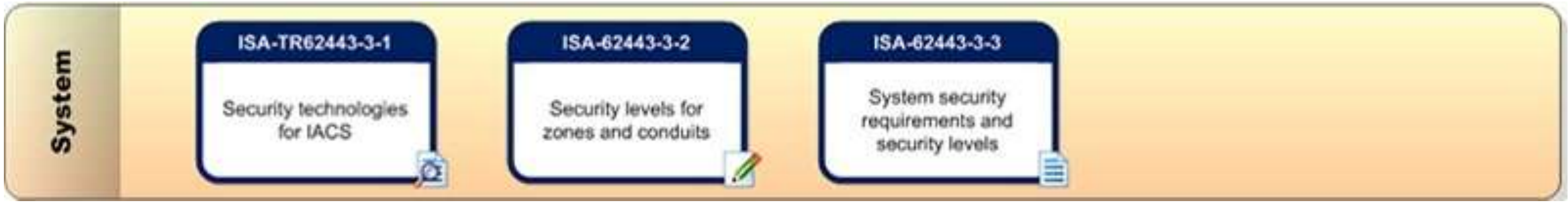
Patch management in the IACS environment

Just approved!

What is ISA 62443?

Part 3: Operating an Industrial Automation and Control System Security Program

Addresses how to operate a security program after it is designed and implemented. This includes definition and application of metrics to measure program effectiveness.



System

ISA-TR62443-3-1

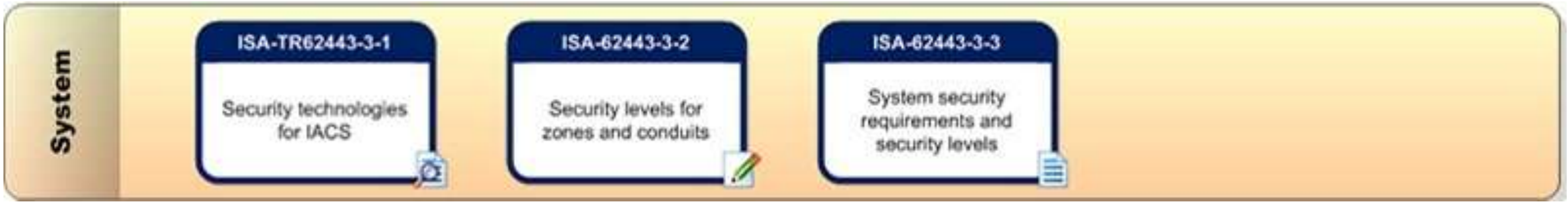
Security technologies for IACS

ISA-62443-3-2

Security levels for zones and conduits

ISA-62443-3-3

System security requirements and security levels

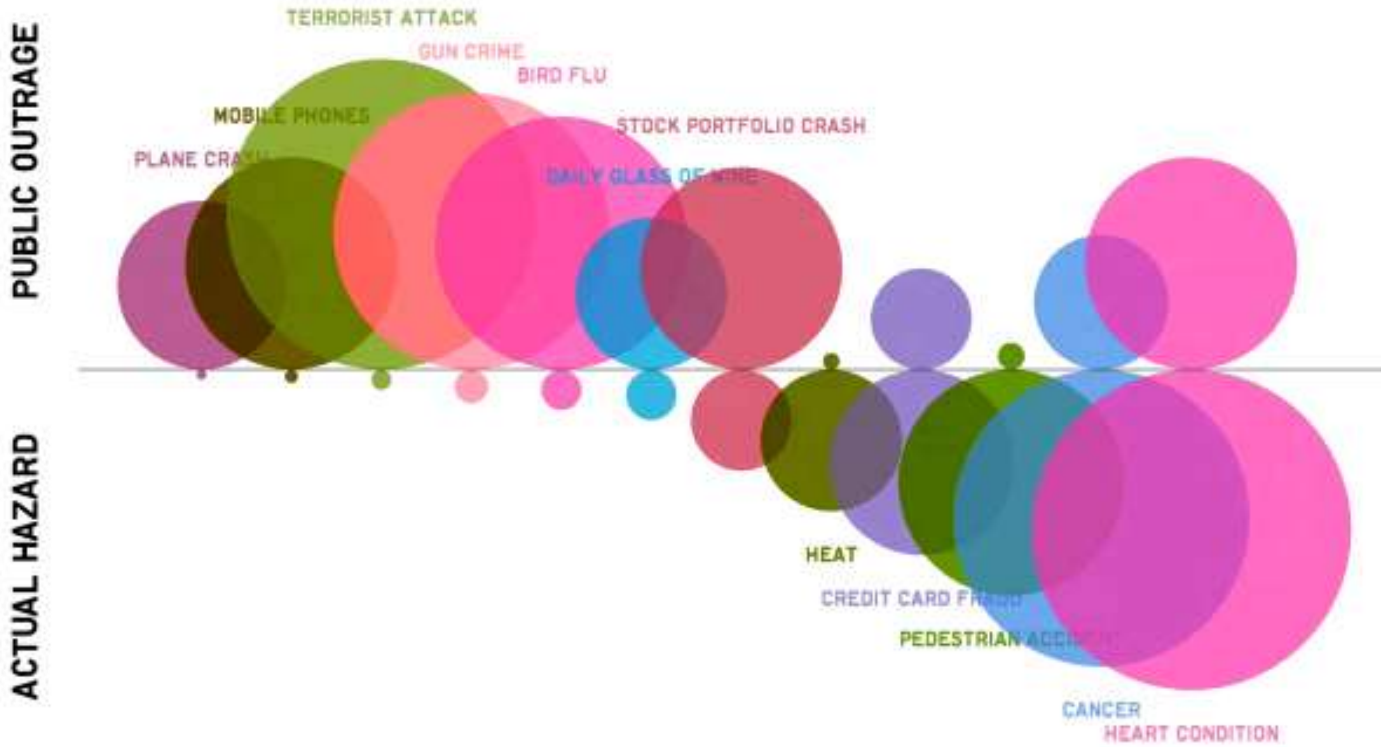

System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels

ISA/IEC 62443-2-3

System security requirements and security levels

Just approved!

Real threats vs. Perceived threats



Potential cyber threats (What management hears on the news or from IT)

- Database Injection
- Replay
- Spoofing
- Social Engineering
- Phishing
- Malicious Code
- Denial of Service
- Escalation of Privileges

ISA/IEC 62443-1-1 5.5.4

FACTS

Targeted attack on a steel plant in Germany 2010.

METHOD

Using sophisticated *spear phishing* and *social engineering* an attacker gained initial access on the office network of the steelworks. From there, they worked successively to the production networks.

DAMAGE

More frequent failures of individual control components or entire plants became evident. The failures resulted in a unregulated blast furnace in a controlled condition that could not be shut down. The result was massive damage to the furnace.

Technical skills

The technical capabilities of the attacker were very advanced. Compromise extended to a variety of internal systems of industrial components. The know-how of the attacker was very pronounced in the field of conventional IT security and extended to applied industrial control and production processes.

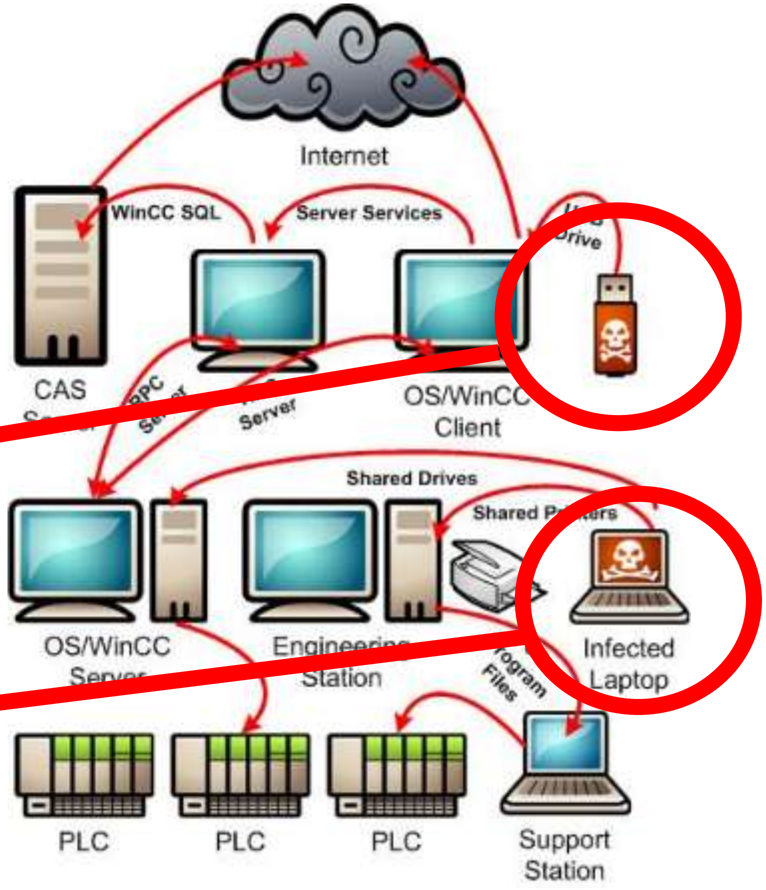
“sophisticated spear phishing and social engineering”

This is only the second confirmed case in which a wholly digital attack caused physical destruction of equipment.

Suxtnet is not your problem

It’s the USB

Or the contractors laptop



Your current likely cyber threats

- Missing or undocumented DCS/PLC programs
- Missing drivers or configuration software
- Loading old program versions
- Loss of passwords
- Inadvertent virus infections
- Disruptive polling of automation system from business network
- Curious employees
- Power failure

ISA/IEC 62443-1-1 5.5.4

Your current likely cyber threats

In a report released today, Unisys recommended that critical infrastructure organizations take on cost effective security strategies by aligning them with other business strategies and goals, and through managing identities and entitlements to improve identity assurance and reduce "critical employee errors," – as 47 percent of respondents said an "accident or mistake" was the root cause of their security breaches in the past year.

What if you could mitigate your current cyber threats (what you are interested in)

while also preventing potential cyber threats? (what management is concerned about)

The first step to implementing a cyber security program for IACS is to develop a **compelling business rationale** for the unique needs of the organization to address **cyber risk**

- Prioritized business consequences
- Prioritized threats
- Estimated annual business impact
- Cost

In a report released today, Unisys recommended that critical infrastructure organizations take on cost effective security strategies by aligning them with other business strategies and goals, and through managing identities and entitlements to improve identity assurance and reduce "critical employee errors," – as 47 percent of respondents said an "accident or mistake" was the root cause of their security breaches in the past year.

Business risks from current and potential threats

- Personnel safety risks: death or injury
- Process safety risks: equipment damage or business interruption
- Information security risk: cost, legal violation, or loss of brand image
- Environmental risk: notice of violation, legal violations, or major impact
- Business continuity risk: business interruption

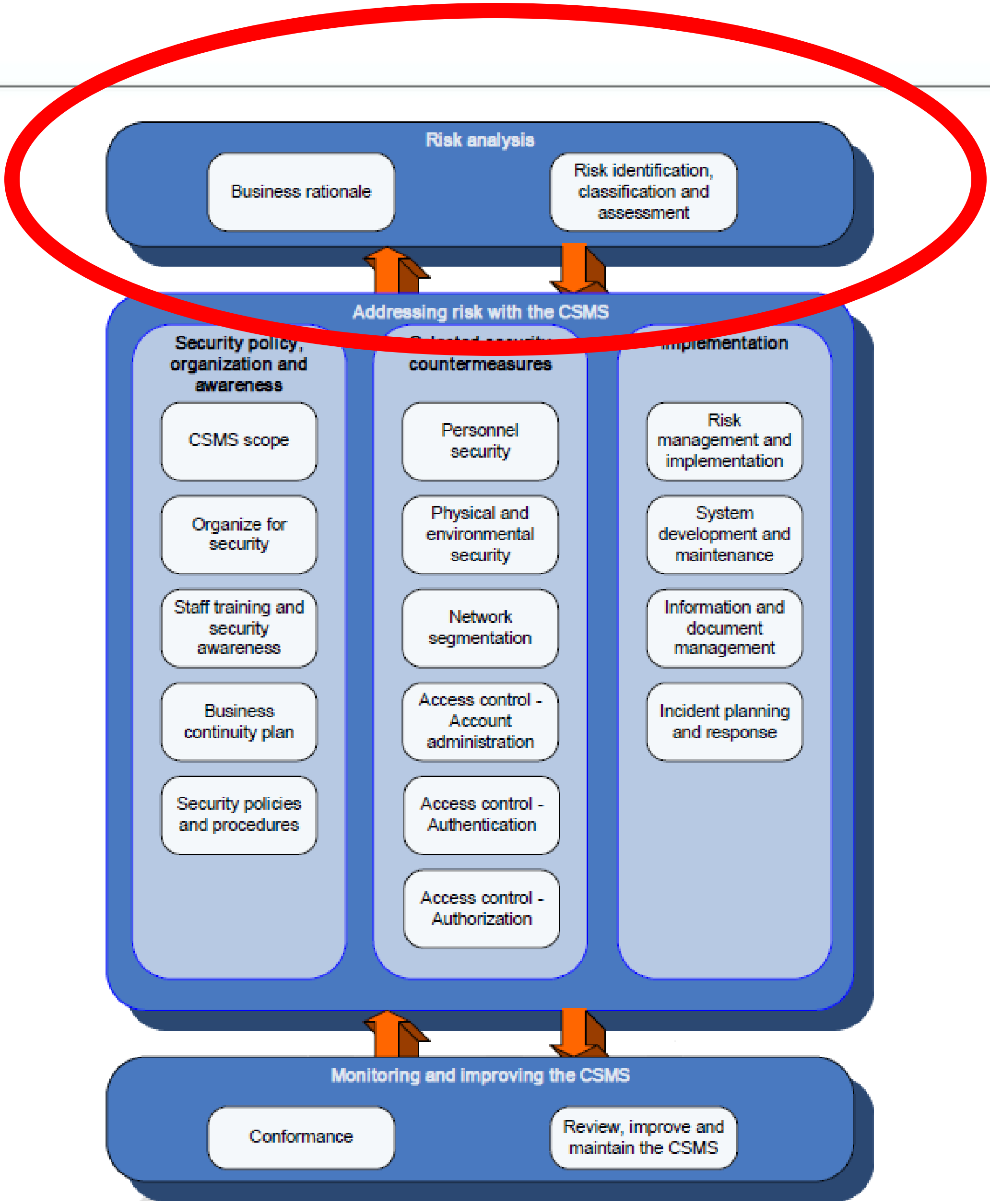
Let’s save some time!

“High-level assessment is required because experience has shown that if organizations start out by looking at detailed vulnerabilities, they miss the big picture of cyber risk and find it difficult to determine where to focus their cyber security efforts. Examination of risks at a high level can help to focus effort in detailed vulnerability assessments.”

ISA/IEC 62443-2-1 Annex C Proposed

© MARK ANDERSON
WWW.ANDERTOONS.COM
FOREST
TREES
ANDERSON

"Hold on, where's the forest again?"



Risk analysis

Business rationale

Risk identification, classification and assessment

Addressing risk with the CSMS

Security policy, organization and awareness

CSMS scope

Organize for security

Staff training and security awareness

Business continuity plan

Security policies and procedures

Selected security countermeasures

Personnel security

Physical and environmental security

Network segmentation

Access control - Account administration

Access control - Authentication

Access control - Authorization

Implementation

Risk management and implementation

System development and maintenance

Information and document management

Incident planning and response

Monitoring and improving the CSMS

Conformance

Review, improve and maintain the CSMS

ISA/IEC 62443-2-1 4.1

So where do I start?

ISA/IEC 62443-2-1 Annex A

Annex A soon to be Annex C

- **Developing a network diagram of the IACS (see C.3.3.3.8.4).**

- Understanding that risks, risk tolerance and acceptability of countermeasures may vary by geographic region or business organization.

- Maintaining an up-to-date record of all devices comprising the IACS for future assessments.

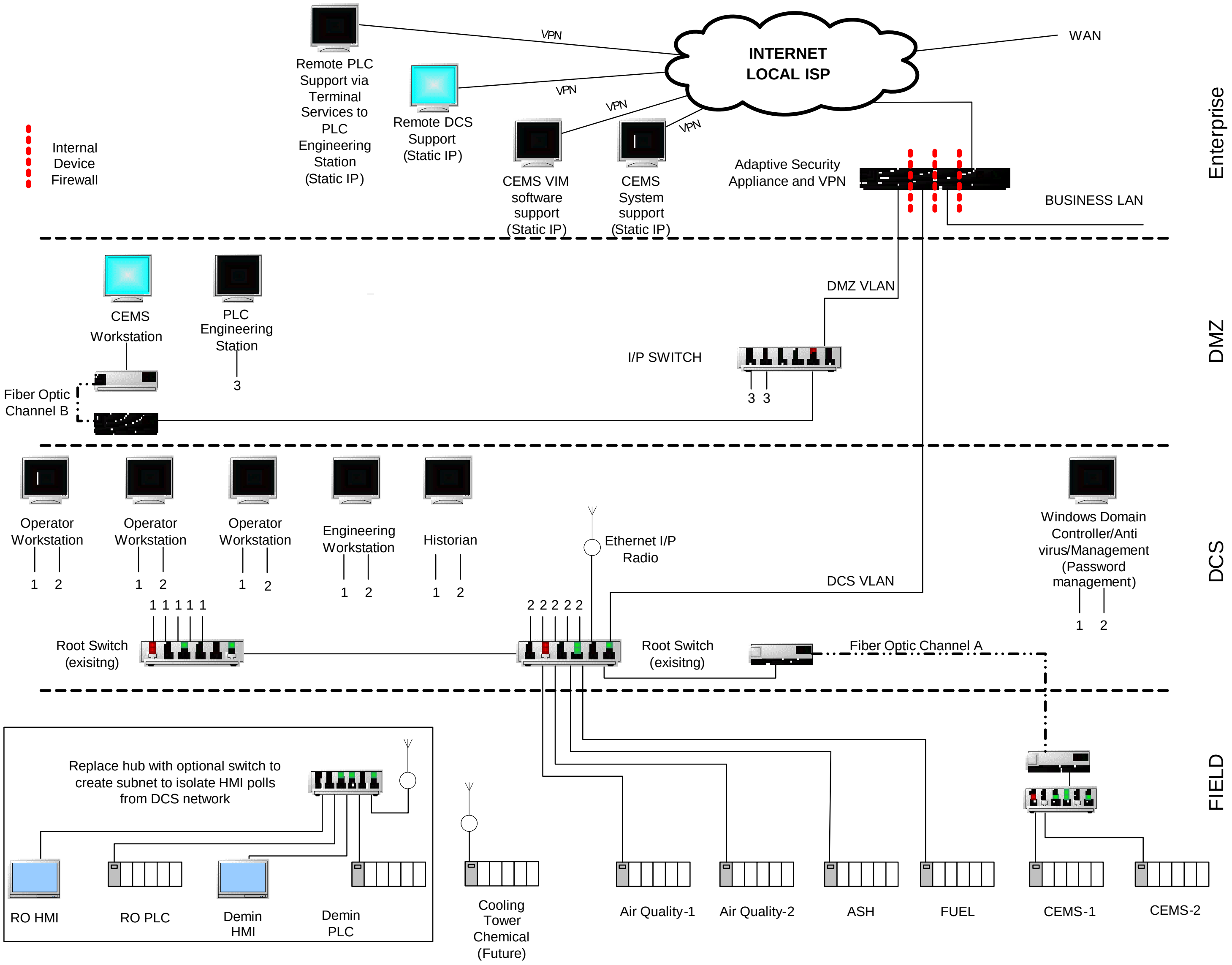
Annex A soon to be Annex C

- Establishing the criteria for identifying which devices comprise the IACS.

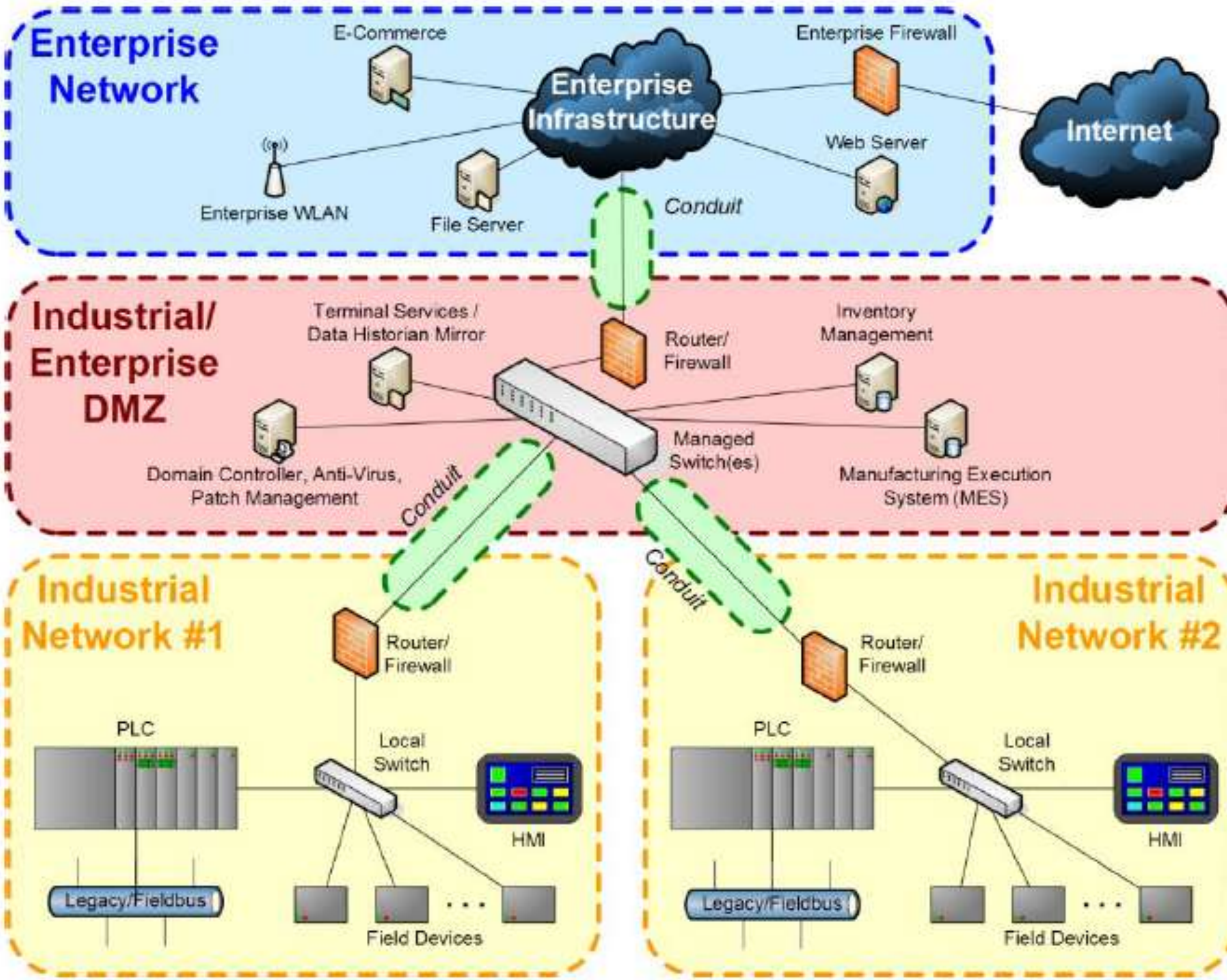
- Identifying devices that support critical business processes and IACS operations including the IT systems that support these business processes and IACS operations.

- Classifying the logical assets and components based on availability, integrity, and confidentiality, as well as HSE impact.

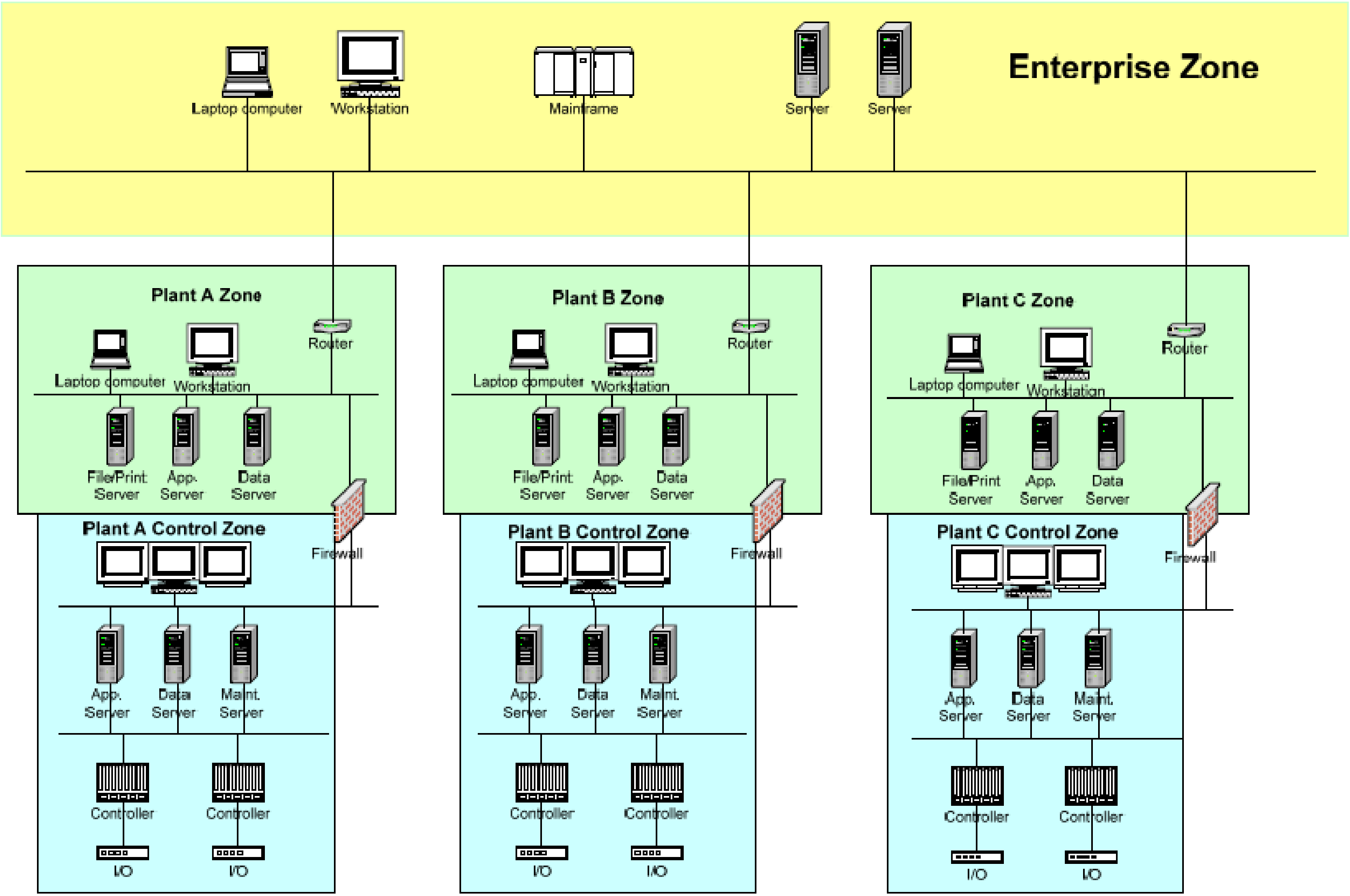
Developing a network diagram of the IACS



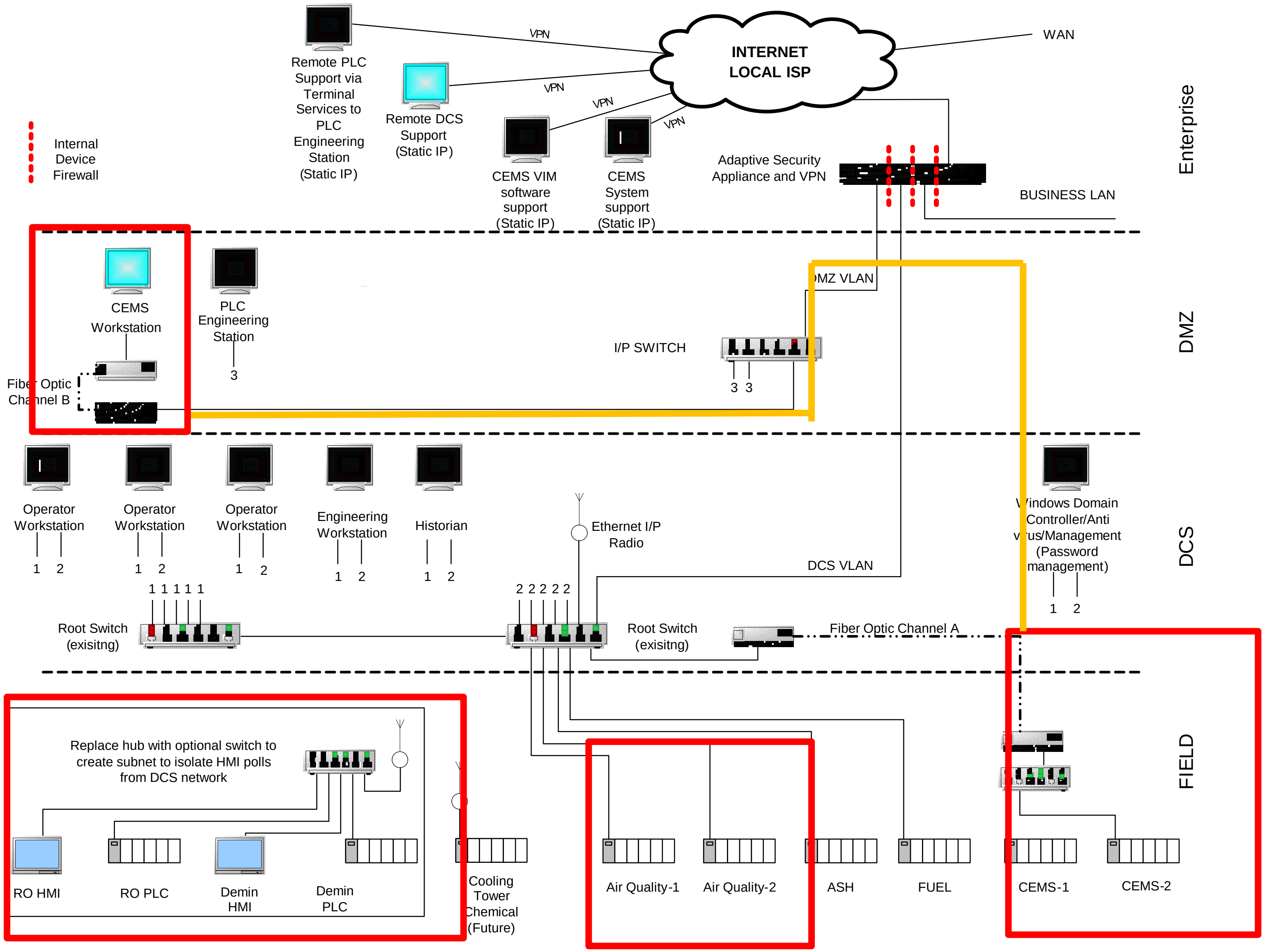
Developing a network diagram of the IACS



Developing a network diagram of the IACS



Developing a network diagram of the IACS



Annex A soon to be Annex C

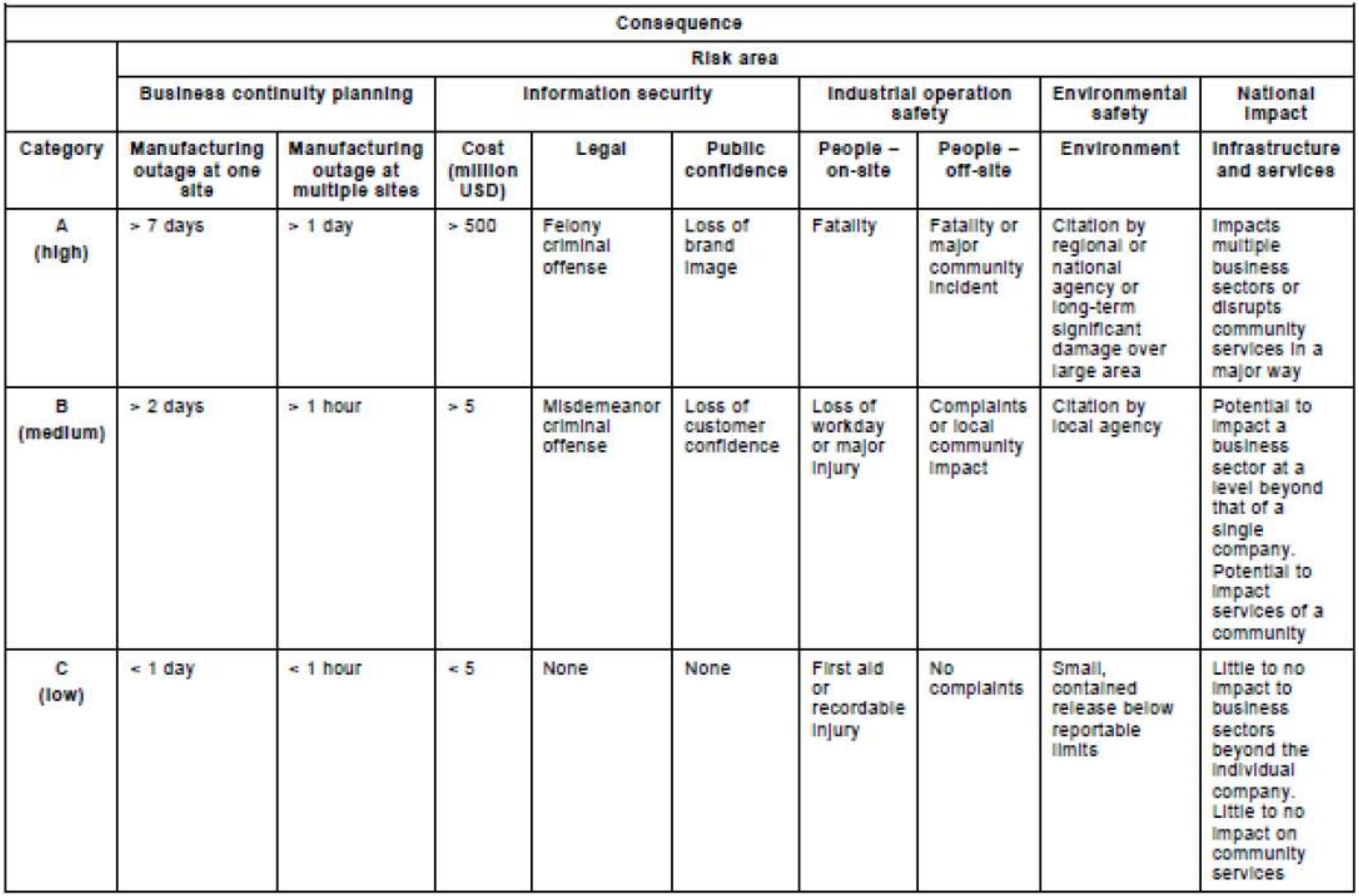
- Conducting a risk assessment through all stages of the technology l lifecycle (development, implementation, updating and retirement).

- Identifying reassessment frequency or triggering criteria based on technology, organization or industrial operation changes.

The risk equation

Risk = Likelihood of Event Occurring × Consequence

The risk equation



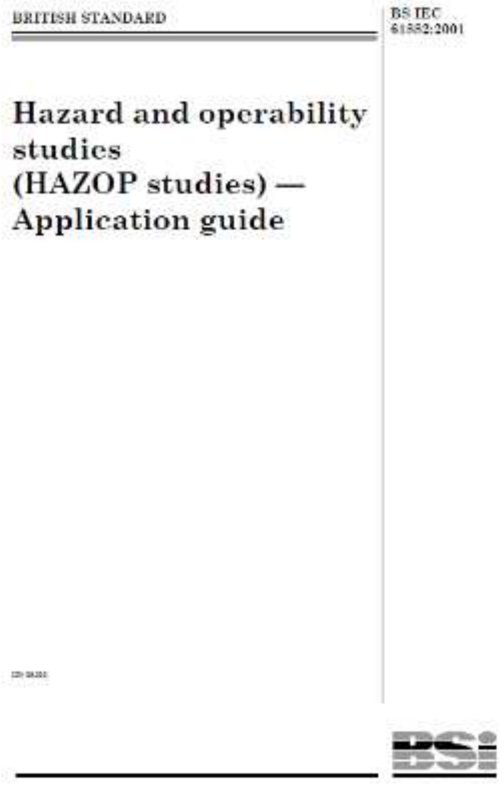
Consequence									
	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	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

If you done a HAZOP, you can do a cyber security risk assessment!

BS IEC 61882:2001 Hazard and Operability (HAZOP) Studies. **HAZOP** is a structured and systematic technique for examining a defined system, with the objective of:

Identifying potential hazards in the system. The hazards involved may include both those essentially relevant only to the immediate area of the system and those with a much wider sphere of influence, e.g. some environmental hazards;

Identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to nonconforming products.



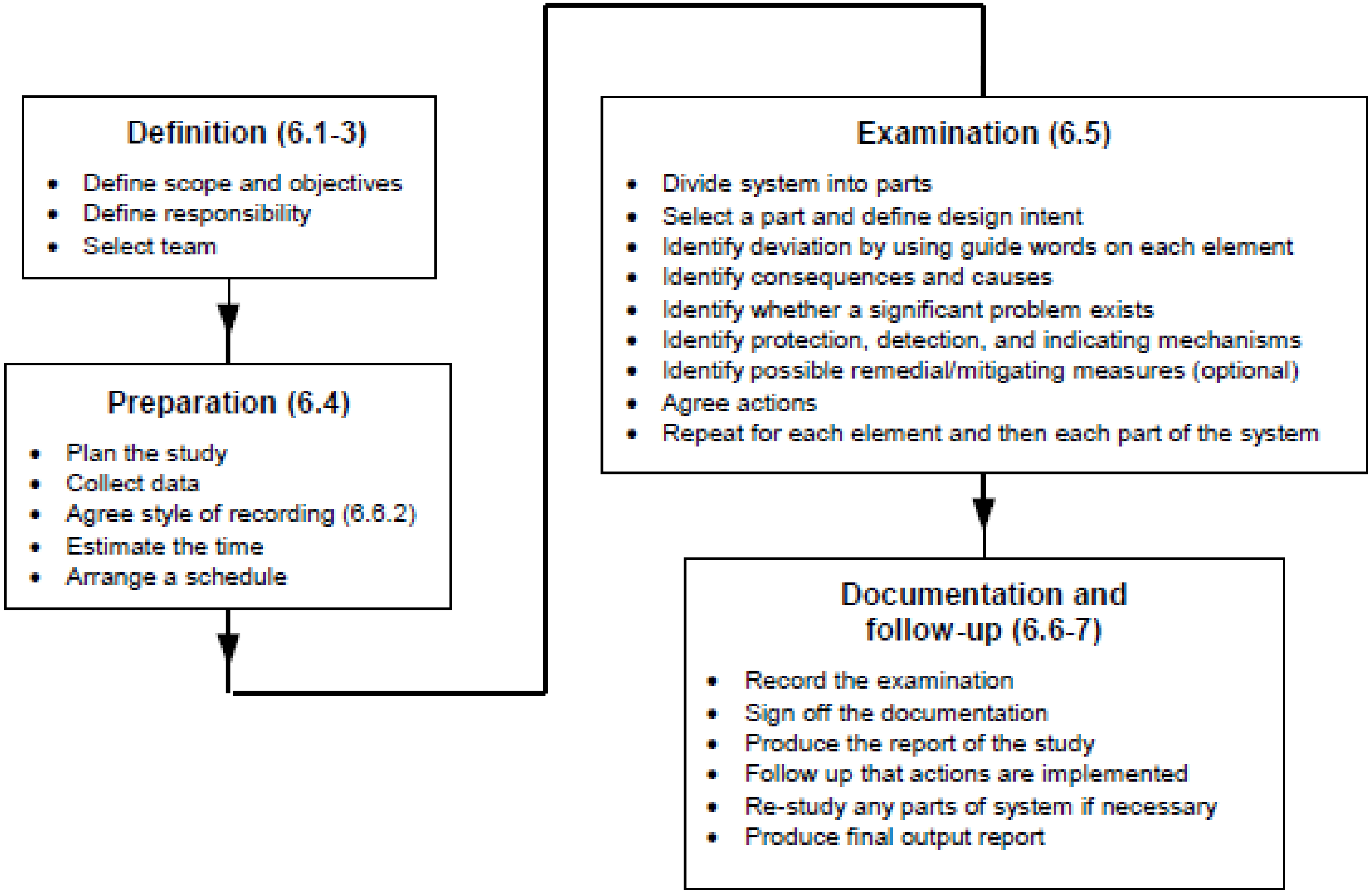
BRITISH STANDARD

BS IEC 61882:2001

Hazard and operability studies (HAZOP studies) — Application guide

[illegible]

The HAZOP Study Procedure



Definition (6.1-3)

- Define scope and objectives
- Define responsibility
- Select team

Preparation (6.4)

- Plan the study
- Collect data
- Agree style of recording (6.6.2)
- Estimate the time
- Arrange a schedule

Examination (6.5)

- Divide system into parts
- Select a part and define design intent
- Identify deviation by using guide words on each element
- Identify consequences and causes
- Identify whether a significant problem exists
- Identify protection, detection, and indicating mechanisms
- Identify possible remedial/mitigating measures (optional)
- Agree actions
- Repeat for each element and then each part of the system

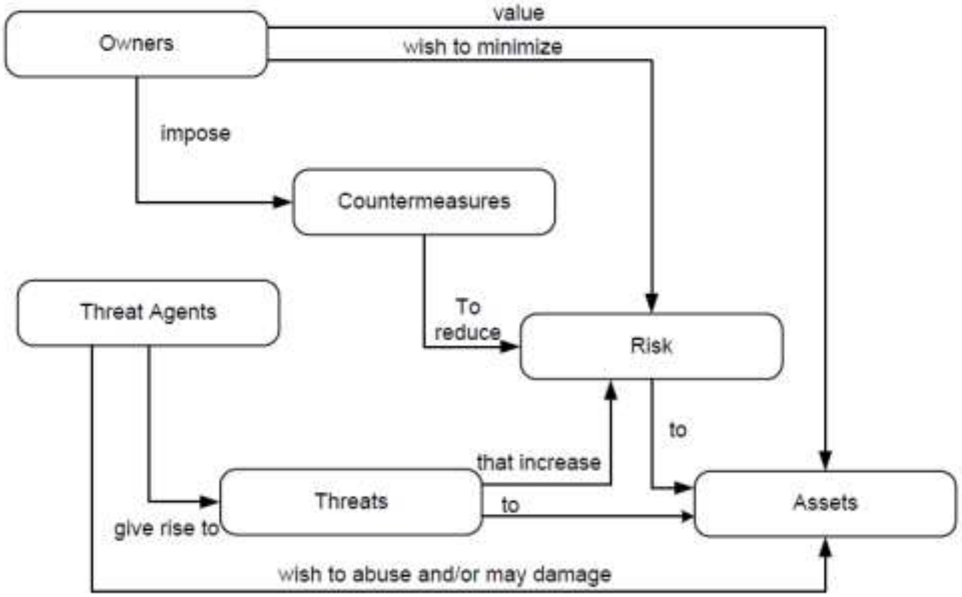
Documentation and follow-up (6.6-7)

- Record the examination
- Sign off the documentation
- Produce the report of the study
- Follow up that actions are implemented
- Re-study any parts of system if necessary
- Produce final output report

IEC 450/01

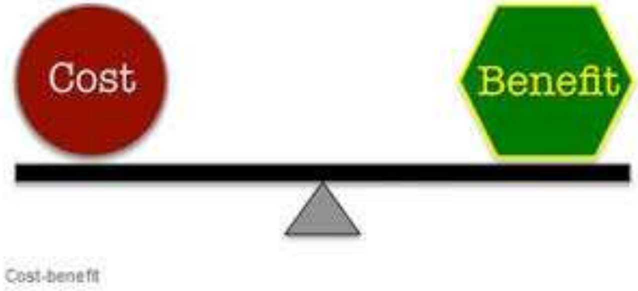
Risk Response (For the MBAs)

- Assess initial risk
- Implement countermeasures
- Assess residual risk



ISA/IEC 62443-1-1 6.1

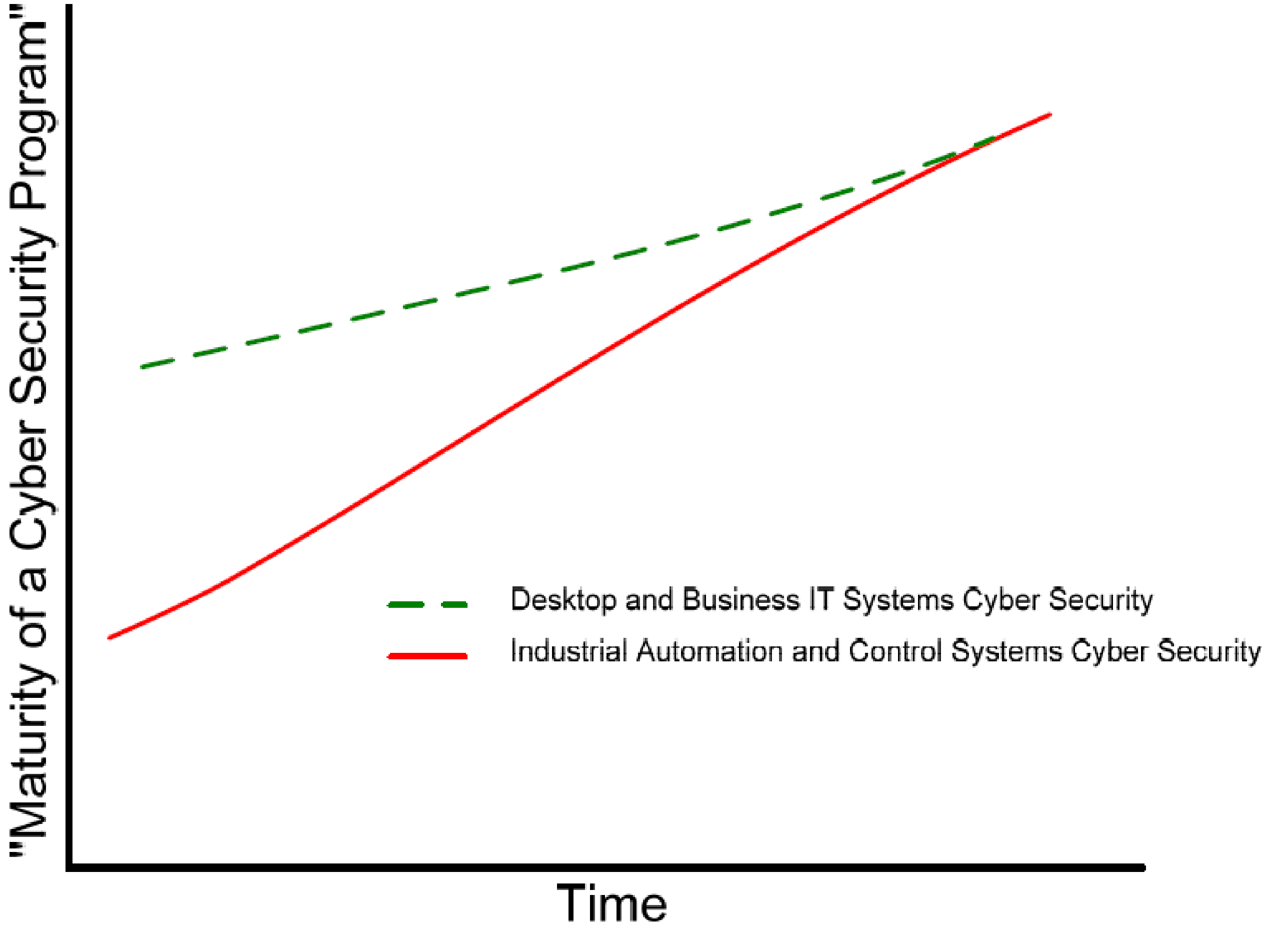
Risk Response (For the Engineers)



Cost-benefit

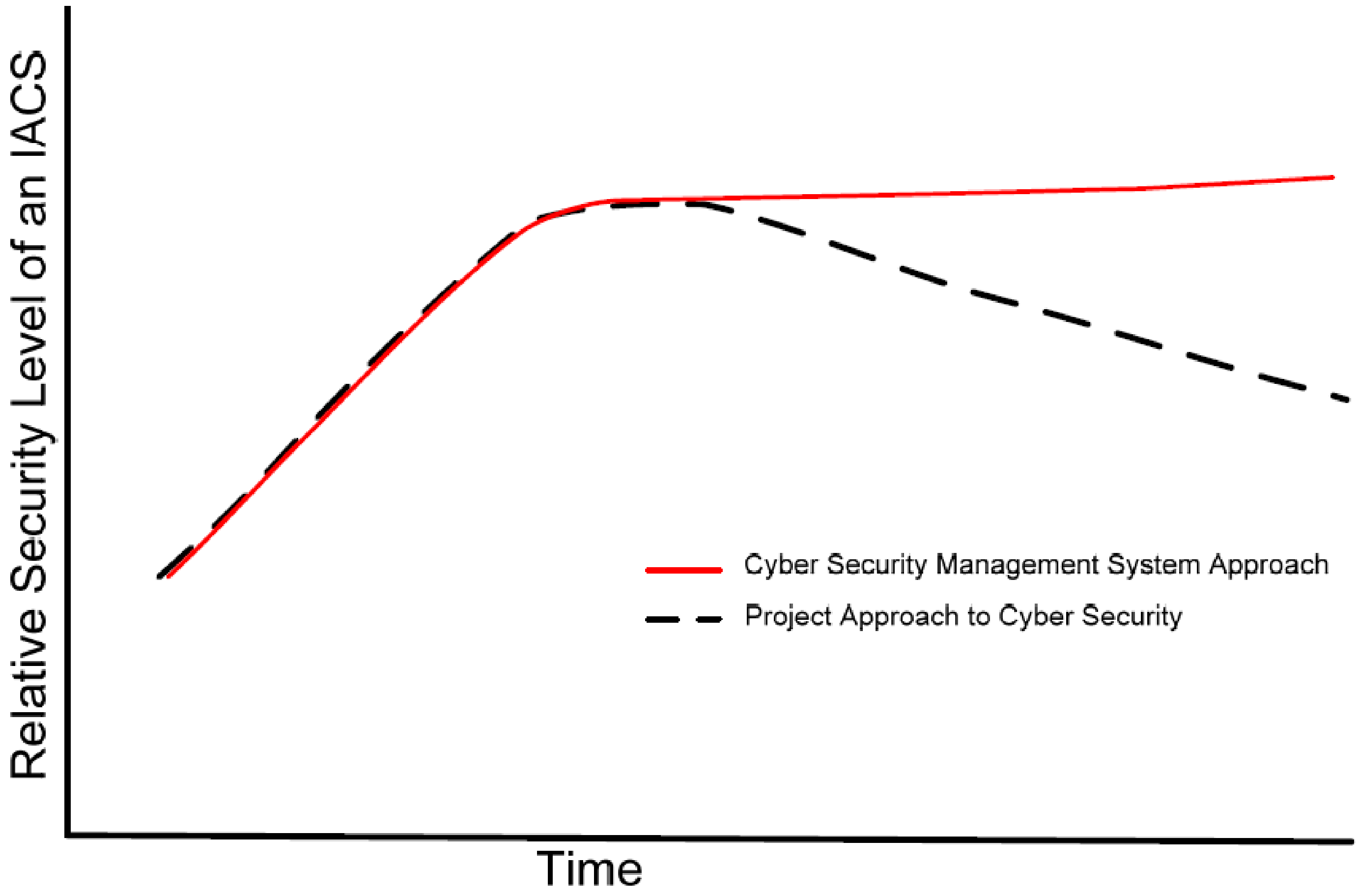
- Design the risk out
- Reduce the risk
- Accept the risk
- Transfer or share the risk
- Eliminate or fix outdated risk control measures

The goal!



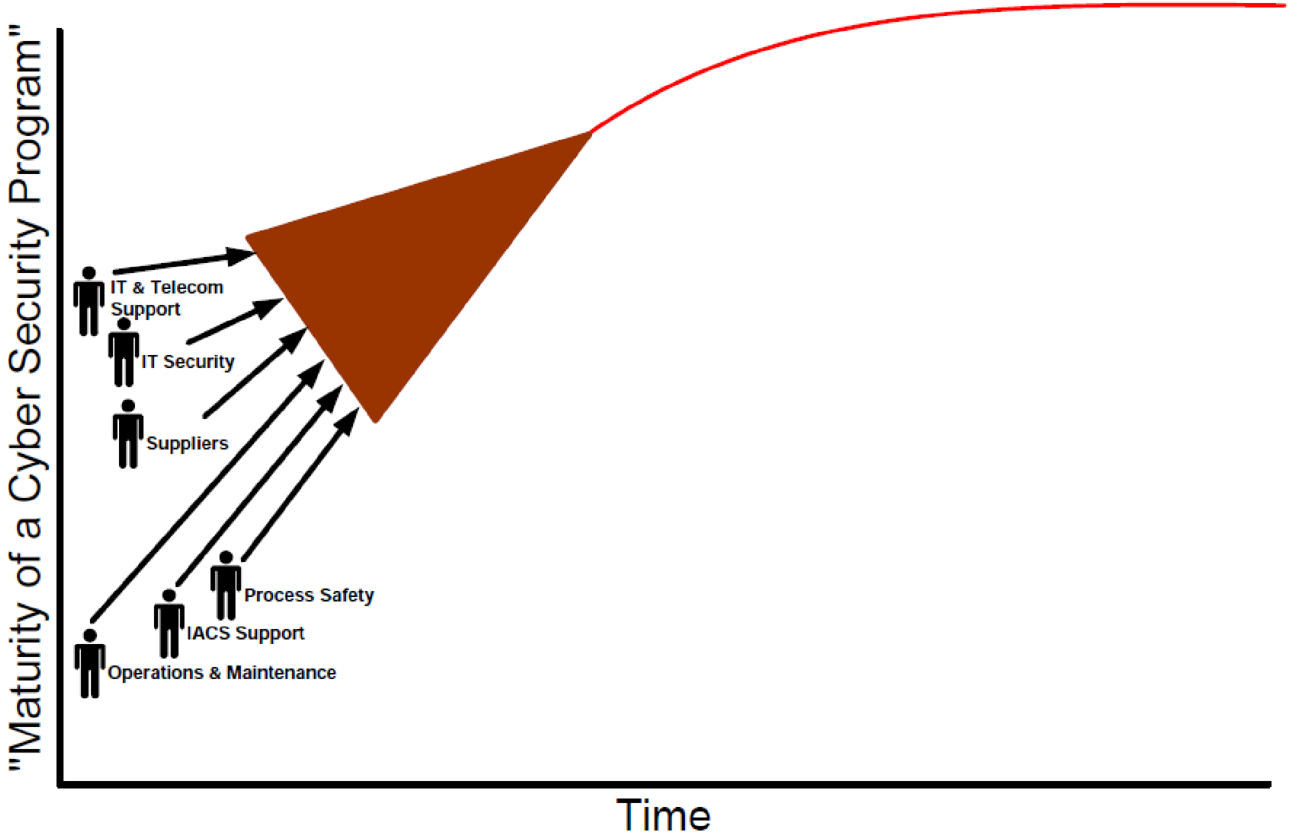
ISA/IEC 62443-1-1 5.6

So why a entire new program
(or why cant we just specify a solution?)



ISA/IEC 62443-1-1 5.6

It takes a team!



ISA/IEC 62443-1-1 5.6

Pitfalls

- Designing the solution during the assessment
- Minimizing or overstating the consequence
- Failing to gain consensus on the risk assessment results
- Assessing the system without considering the assessment results from other similar systems

Cyber security is much less about technology then it is just good management.