ISA

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

rêal

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.
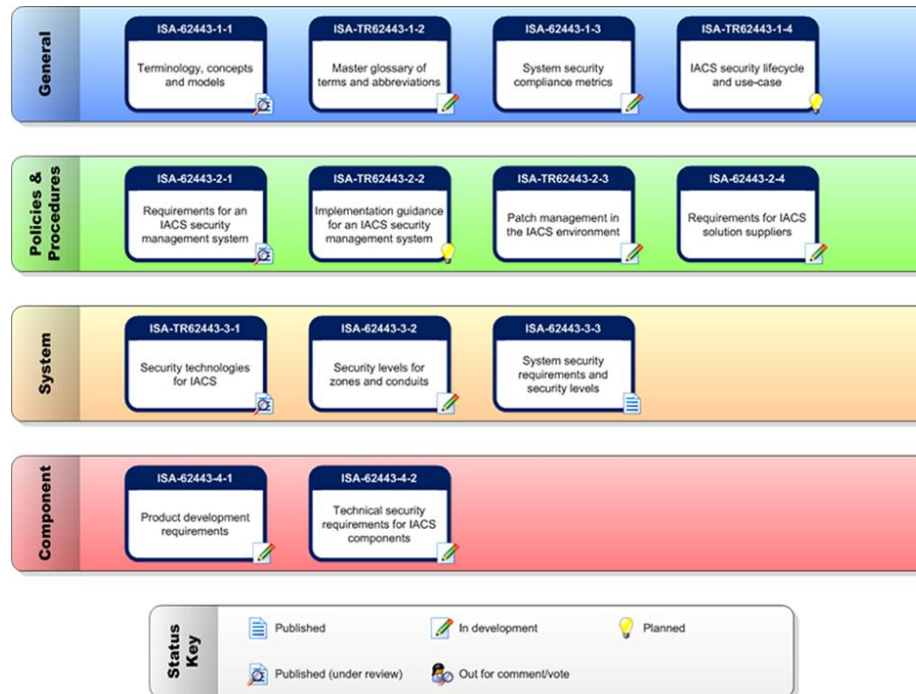
What is ISA 62443?

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.

ISA-62443-1-1	ISA-TR62443-1-2	ISA-62443-1-3	ISA-TR62443-1-4
Terminology, concepts and models	Master glossary of terms and abbreviations	System security compliance metrics	IACS security lifecycle and use-case

General

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	ISA-TR62443-2-2	ISA-TR62443-2-3	ISA-62443-2-4
Requirements for an IACS security management system	Implementation guidance for an IACS security management system	Patch management in the IACS environment	Requirements for IACS solution suppliers

ISA/IEC 62443-2-1

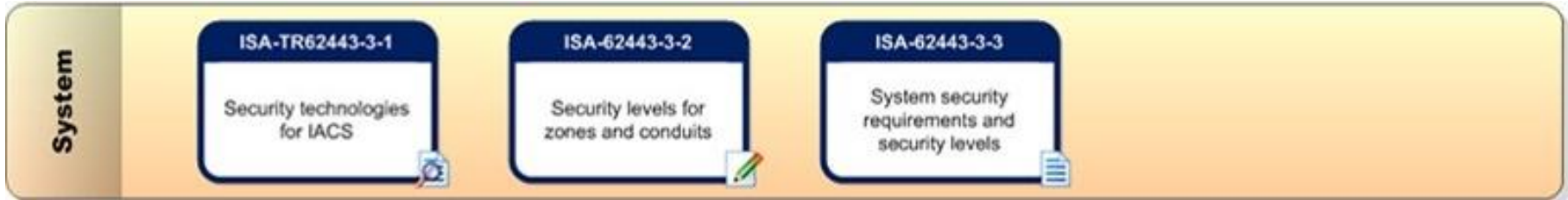Establishing an Industrial Automation and Control Systems Security

ISA/IEC 62443-2-1

Requirements for an IACS Security Management System

New Name!

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.
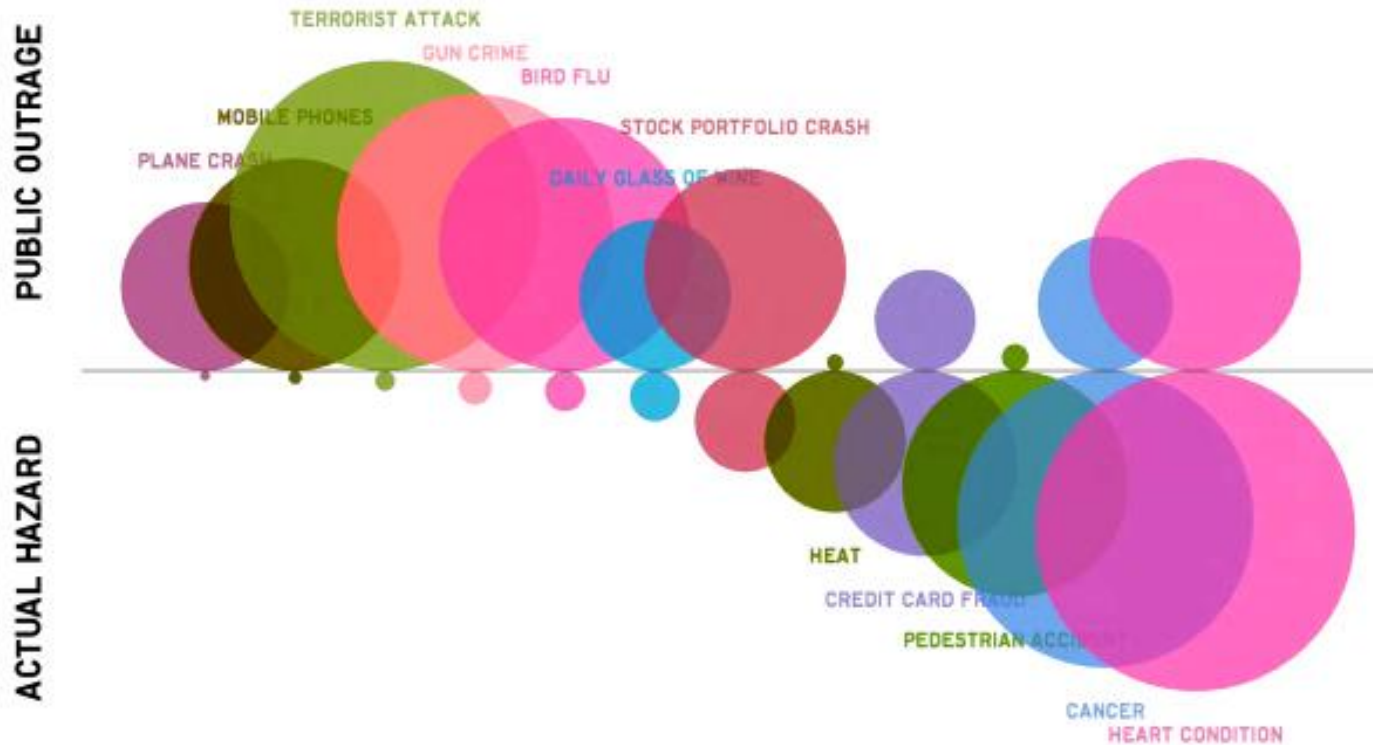
System

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

ISA/IEC 62443-2-3

System security requirements and security levels

Just approved!

Overstating the Risk and Consequence

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.

The root cause…

In a report released earlier this month, 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.

Your current likely internal cyber <u>threats</u>

- 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
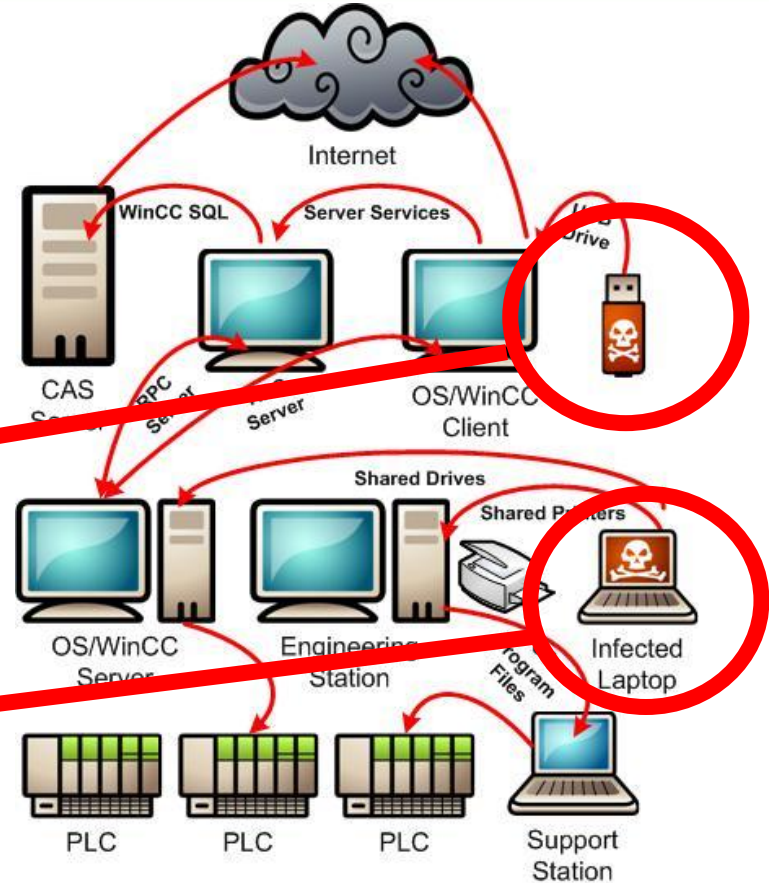
- Curious employees

- Power failure

ISA/IEC 62443-1-1 5.5.4

Suxtnet is not your problem

It's the USB

Or the contractors laptop

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
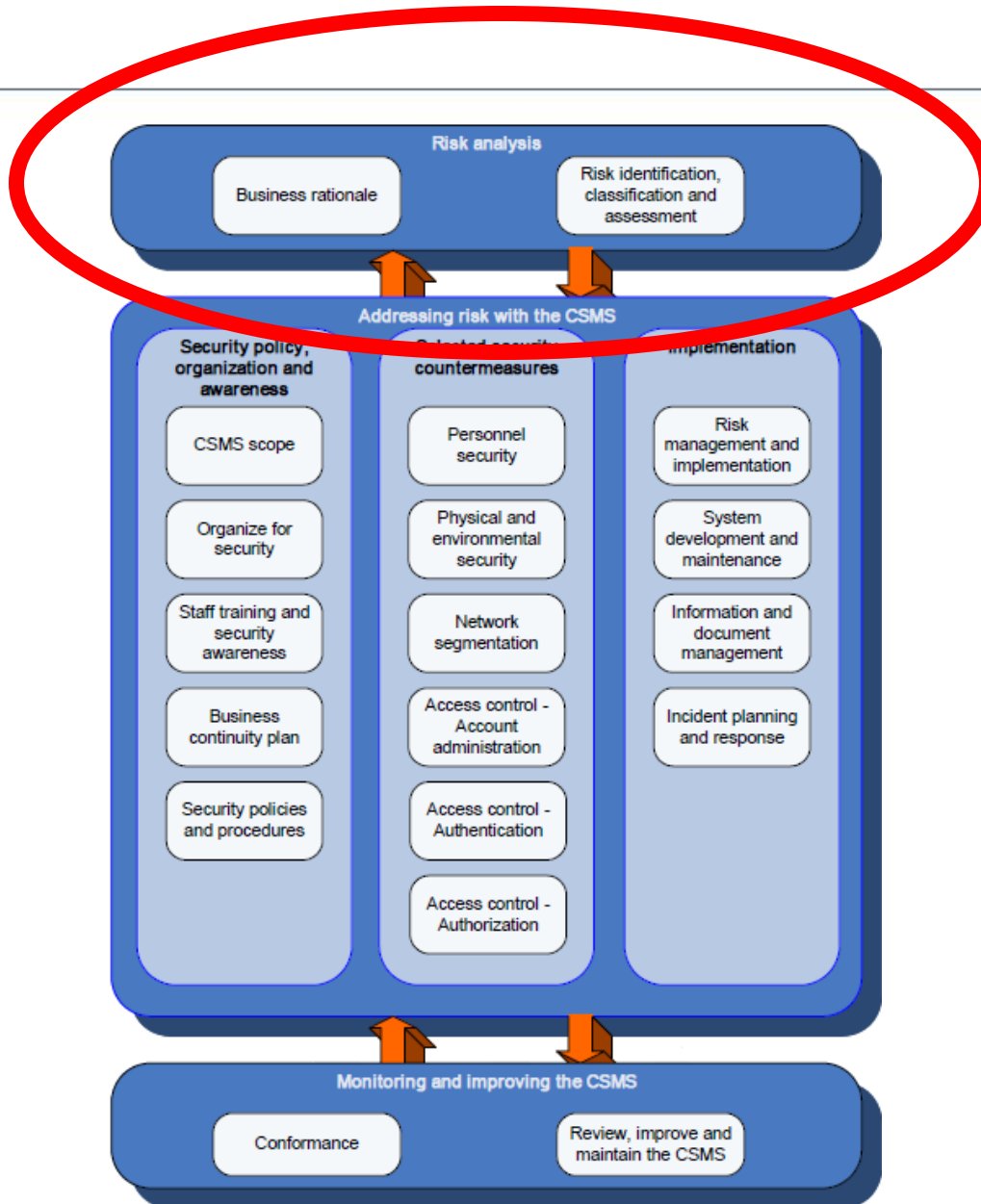
ISA/IEC 62443-2-1 4.1

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

Business <u>risks</u> 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

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.
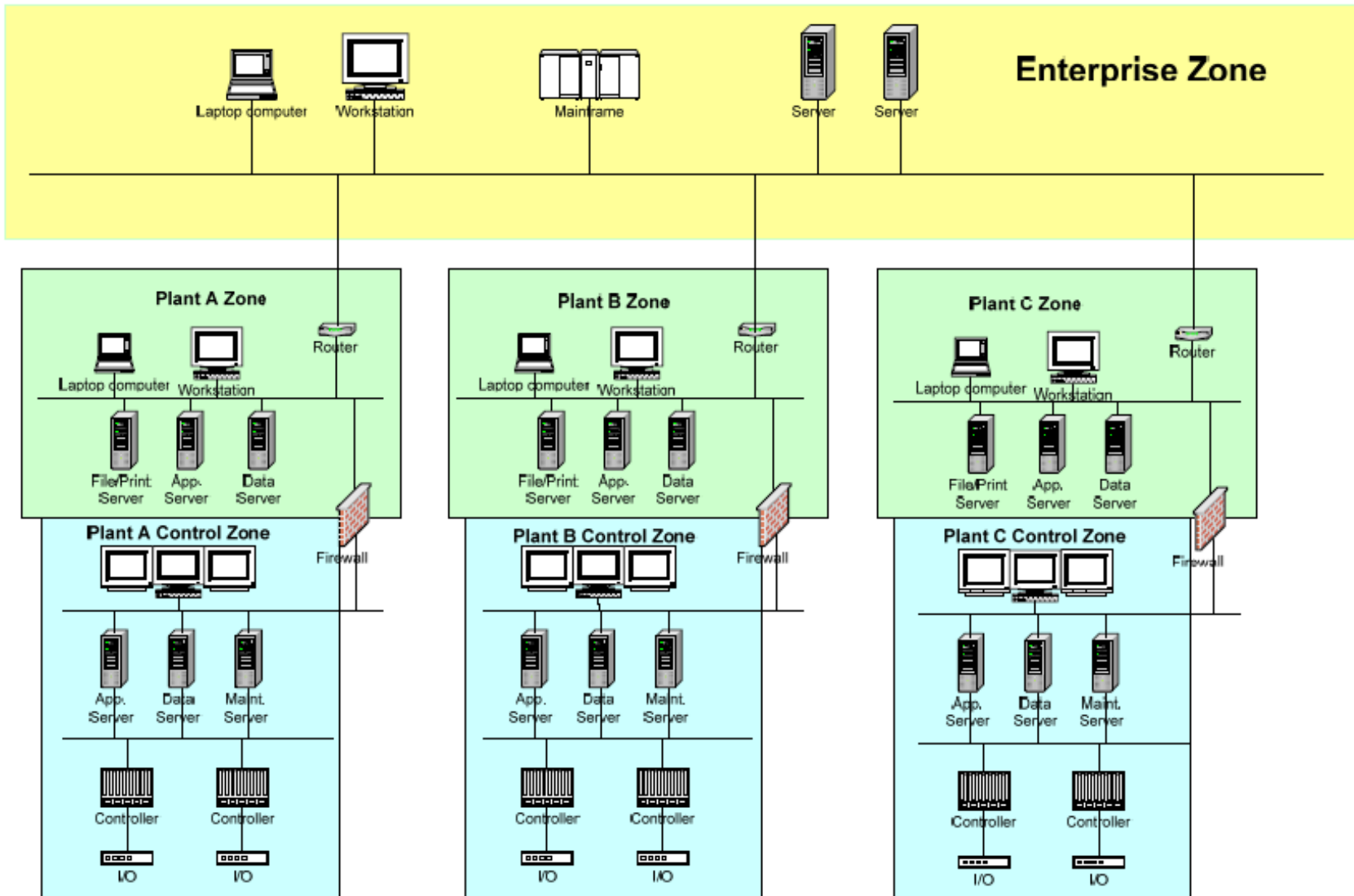
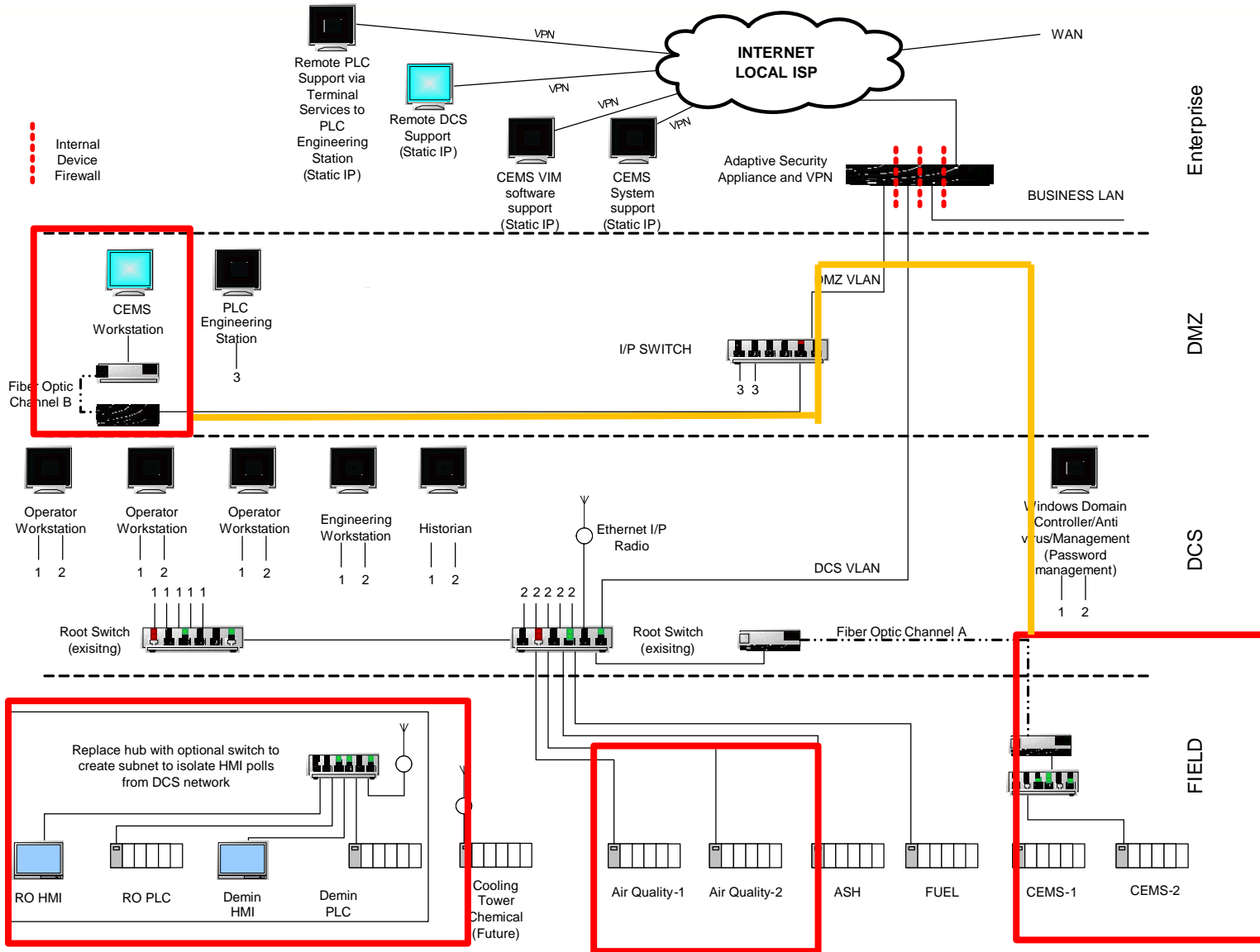# Developing a network diagram of the IACS
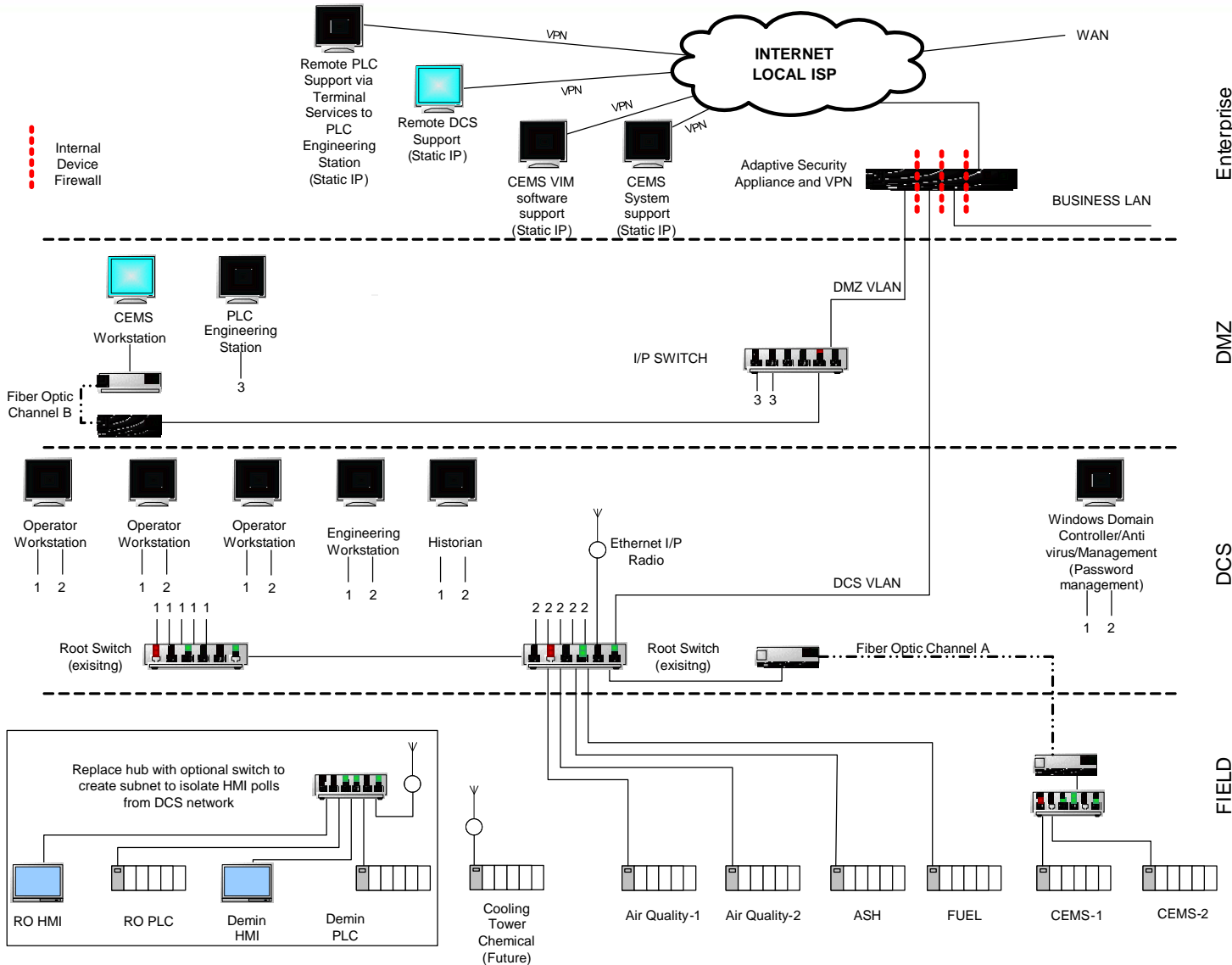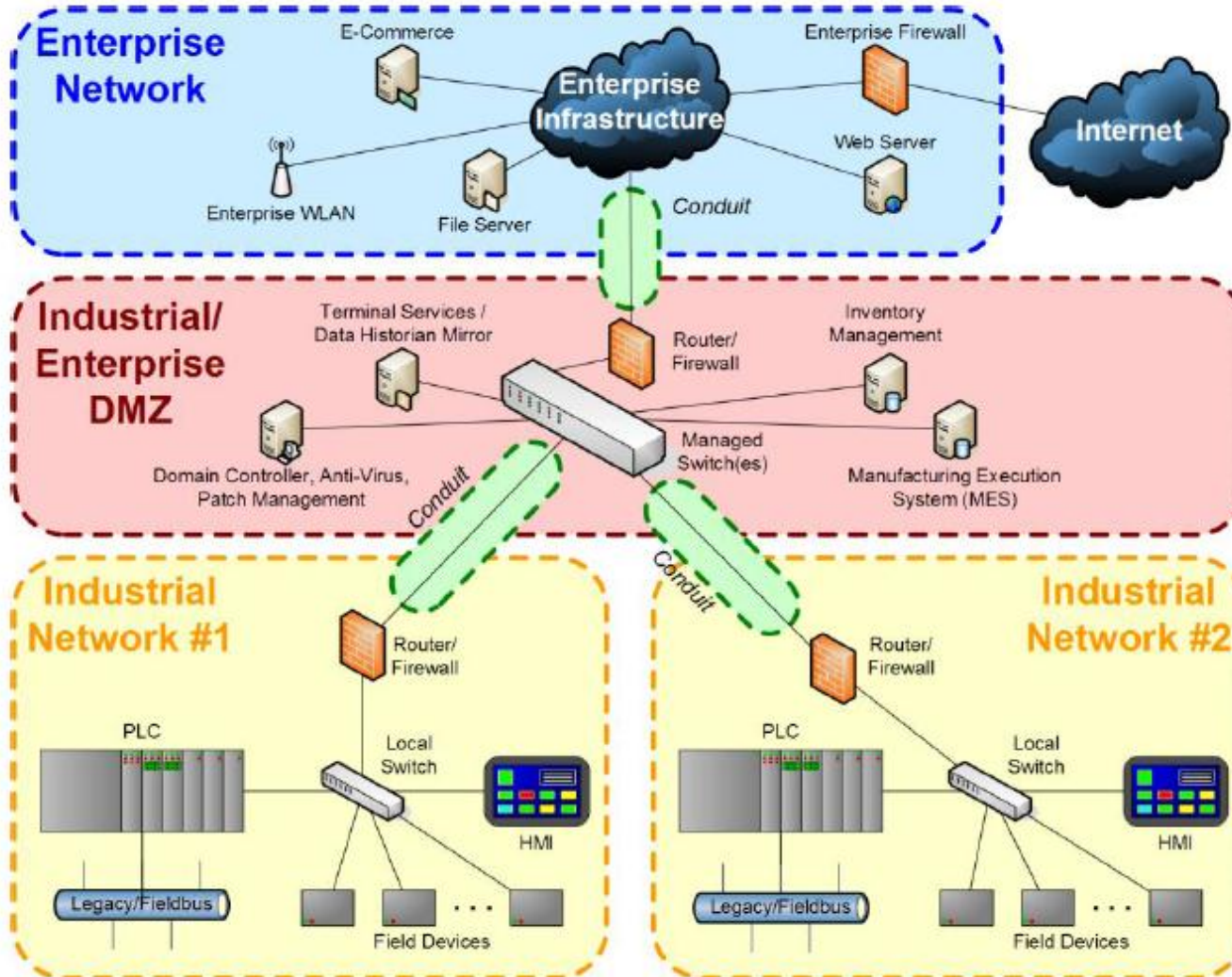
Developing a network diagram of the IACS

Developing a network diagram of the IACS

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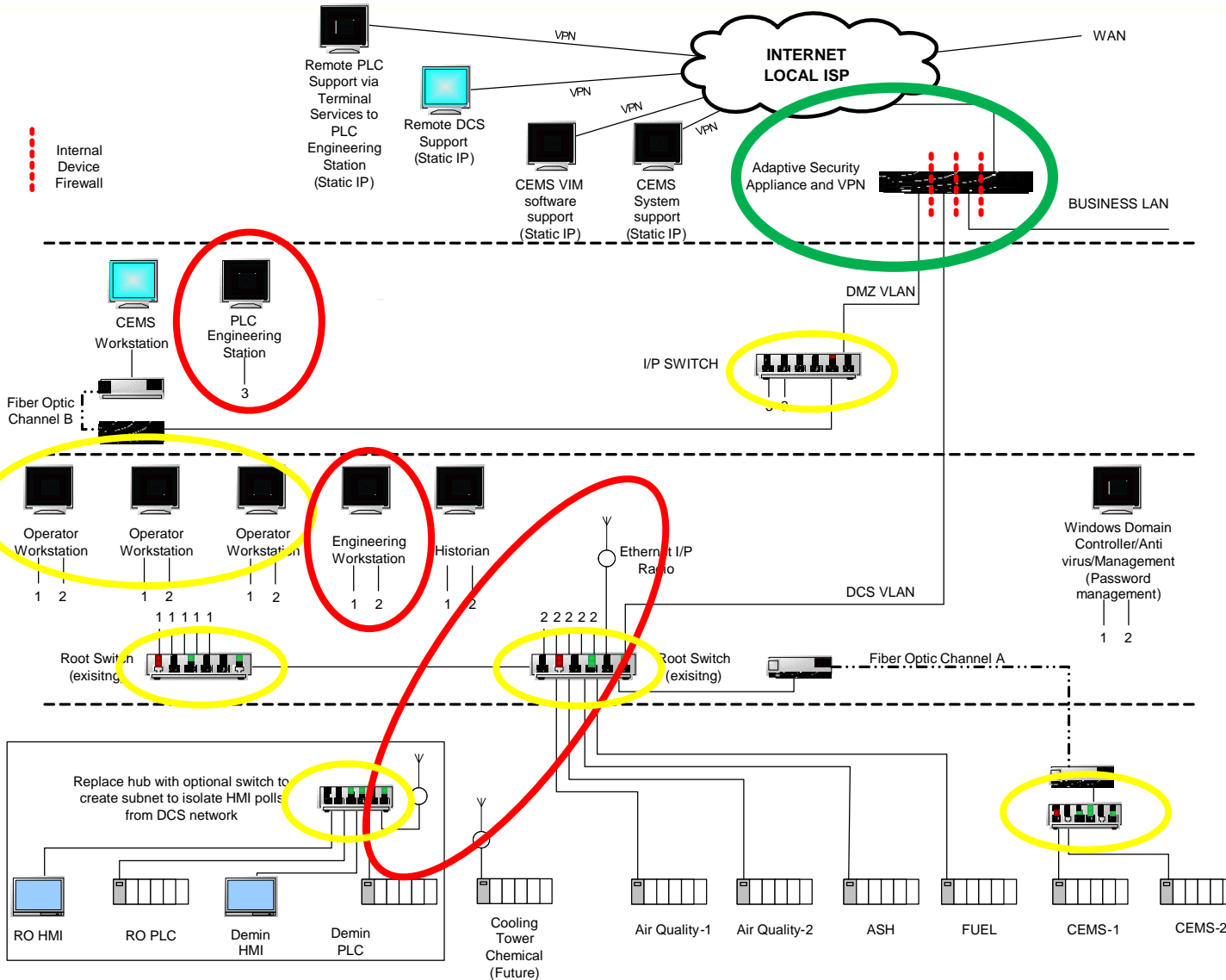
BRITISH STANDARD

BS IEC
61882:2001

Hazard and operability studies (HAZOP studies) — Application guide

ICS 29.020

BSi

Consequences

- Loss of life
- Damage to equipment
- Loss of production
- Environmental reporting fines
- Bad Press

Risk Assessment

The risk equation

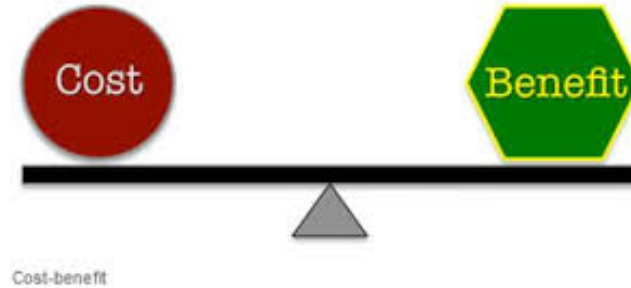|	Consequence								
	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National Impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site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

Risk Response (For the MBAs)

- Assess initial risk
- Implement countermeasures
- Assess residual risk
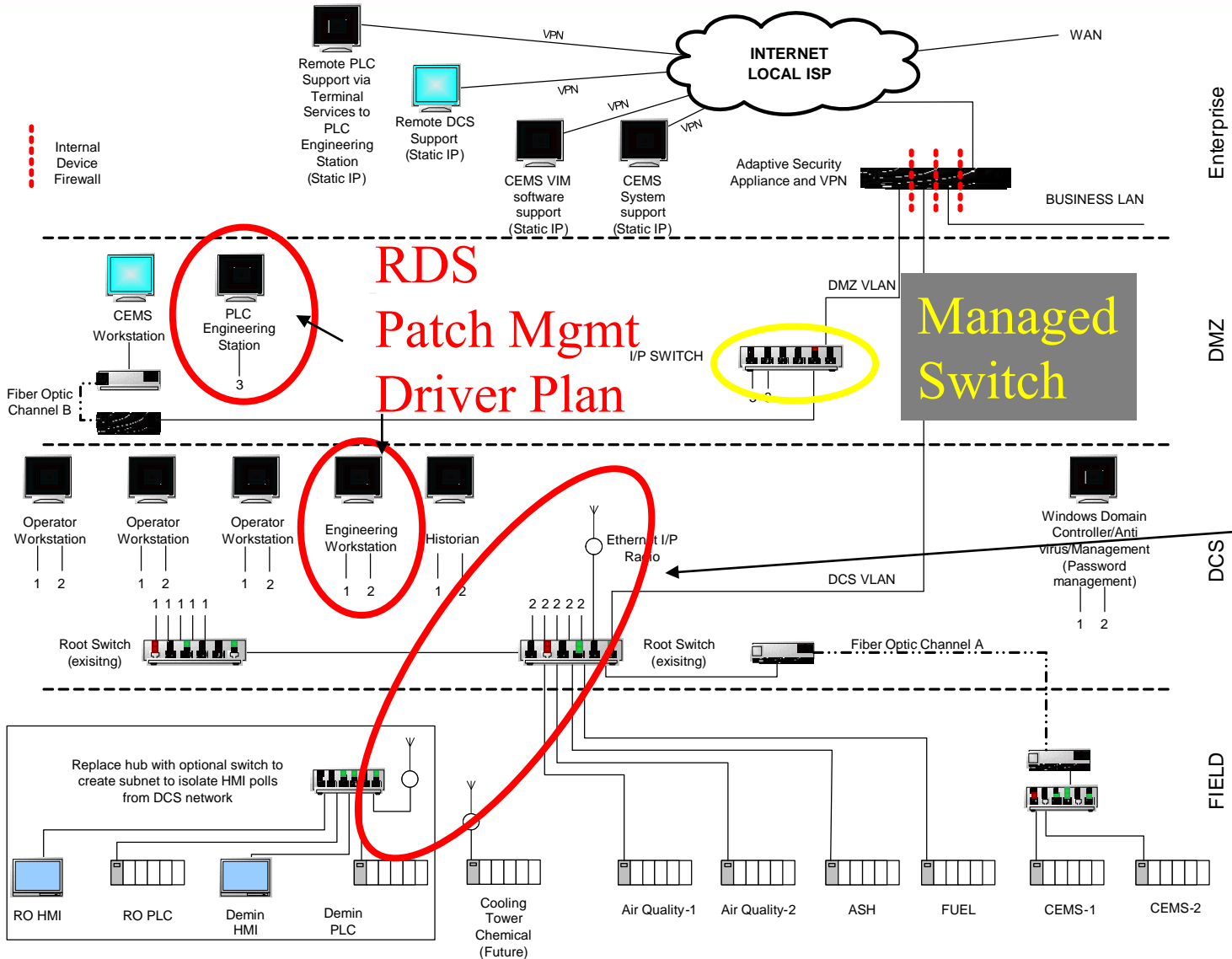

ISA/IEC 62443-1-1 6.1
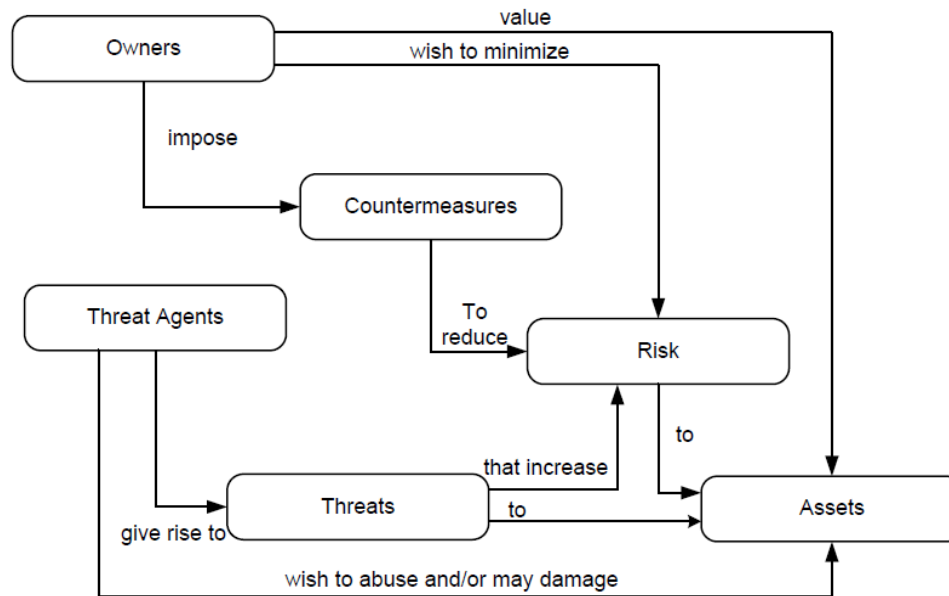
Risk Response (For the Engineers)

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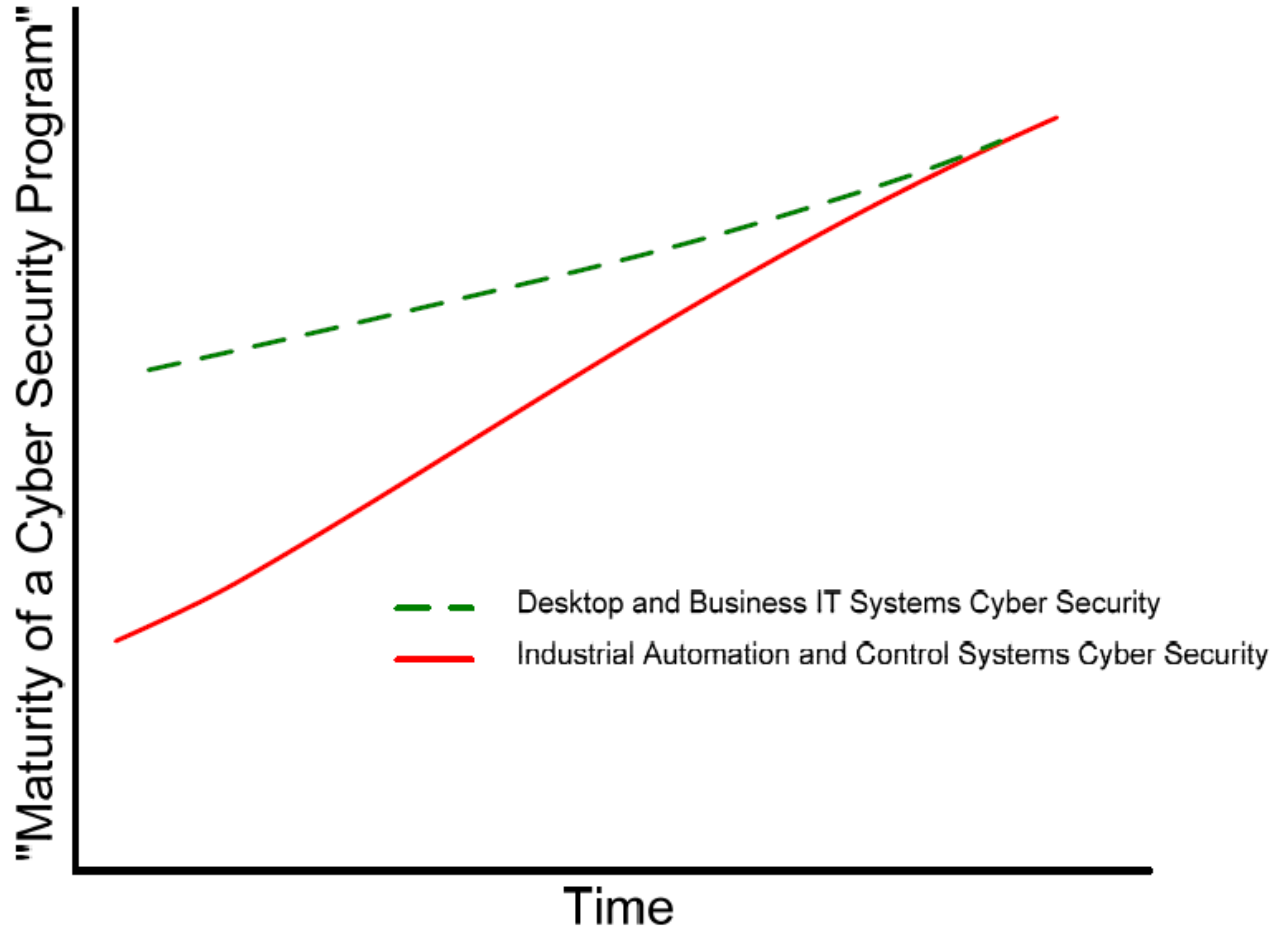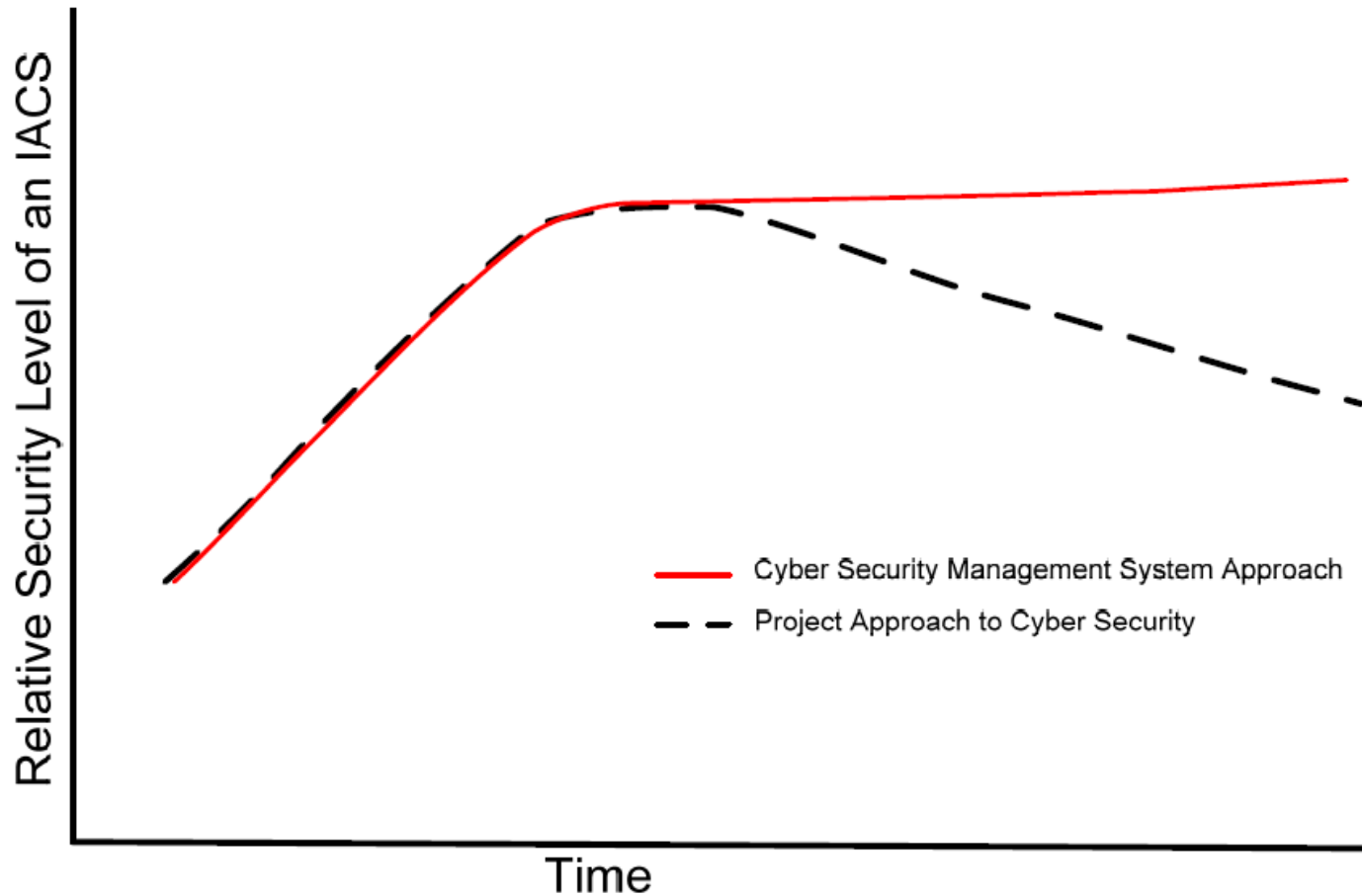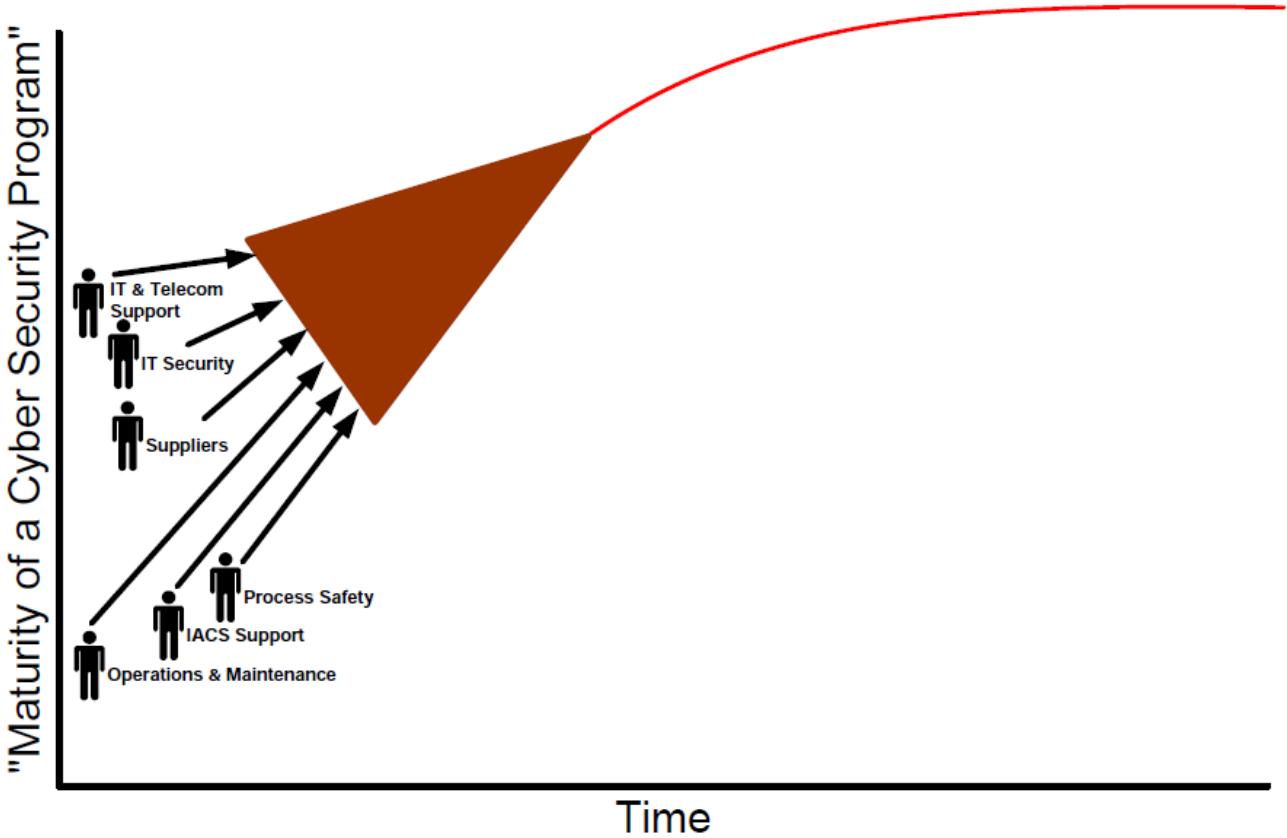- Eliminate or fix outdated risk control measures

Cost

Benefit

Cost-benefit

Midigations

39

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.

Heckle the presenter

Discussion, Questions, More Beer?