

://Arena_Digital_& Software/



Umberto Cattaneo, Rappresentante WG Software Industriale di ANIE Automazione
PMP, Security+, ISA99/IEC62443 Certified specialist

“Cybersecurity and Safety systems: un approccio integrato a protezione di impianti e infrastrutture industriali” - Parma 30-5-2019

Federazione ANIE

Federazione Nazionale Imprese Elettrotecniche ed Elettroniche

- ❖ 14 Associazioni
- ❖ Oltre 1.300 Aziende
- ❖ Membro permanente di Confindustria

ANIE Automazione

ANIE Automazione rappresenta i fornitori di componenti e sistemi per l'automazione industriale manifatturiera, di processo e delle reti.

I Gruppi operanti in ANIE Automazione lavorano su aree principali: Prodotto e Sistema.

Il settore elettrotecnico ed elettronico

Fatturato: 78 Mld di €

Addetti: 468.000

Incidenza della spesa in R&S intra-muros sul fatturato: 4%

Il settore dell'automazione manifatturiera e di processo

Fatturato: 4,7 Mld di €

Esportazioni: 1,2 Mld di €

PRODOTTO	SISTEMA
CONTROLLO DI PROCESSO	MECCATRONICA
AZIONAMENTI ELETTRICI	SOFTWARE INDUSTRIALE
COMPONENTI E TECNOLOGIE PER LA MISURA E IL CONTROLLO	TELECONTROLLO SUPERVISIONE E AUTOMAZIONE DELLE RETI
HMI-IPC-SCADA	TELEMATICA APPLICATA A TRAFFICO E TRASPORTI
PLC-I/O	
UPS	

WG software industriale



con la partecipazione di



La costituzione di questo gruppo di lavoro consente ad ANIE Automazione di inserire nel dibattito associativo i temi di **Industria 4.0** e della **fabbrica digitalizzata** sempre più attuali anche per l'Italia

Obiettivi del gruppo di lavoro

- definizione di linee guida per l'implementazione e benefici derivanti dall'utilizzo di soluzioni software avanzate e delle tecnologie abilitanti I4.0 anche attraverso la pubblicazione di «libri bianchi»;
- promuovere e supportare la crescita culturale delle aziende sui temi 4.0 e sul ruolo del software industriale in questo contesto;



White Paper

IL SOFTWARE INDUSTRIALE 4.0

A cura del WG Software Industriale
ANIE Automazione

Dicembre 2017

 ANIE AUTOMAZIONE



Partecipazione a fiere (es. SPS Italia), seminari, convegni, tavole rotonde, articoli e approfondimenti

Obiettivi del gruppo di lavoro

- definire dei modelli di calcolo del ROI con riferimento ad aree applicative specifiche;
- aiutare a comprendere ed utilizzare gli acceleratori di ROI disponibili (incentivi di legge);
- organizzare eventi di divulgazione dei temi relativi al software industriale ed in particolare organizzare un forum di riferimento per questa tecnologia abilitante.



Realizzato un modello di stima del ROI con l'Università di Pisa, l'Università degli Studi di Firenze e la Scuola Superiore Universitaria Sant'Anna di Pisa

In fase di implementazione una Guida operativa per l'utilizzo del modello avanzato ROI



forum  Software Industriale

www.forumsoftwareindustriale.it

TAVOLA ROTONDA

Software Industriale 4.0
IL MOTORE DELLA CRESCITA

Casi pratici raccontati dai fornitori di tecnologia



Cybersecurity what does it mean?

Assure *data Confidentiality, Integrity and Availability* by:

Protecting the systems against hacking

- Intentional

Protecting the system against errors

- Non intentional

Improve operation and maintenance processes

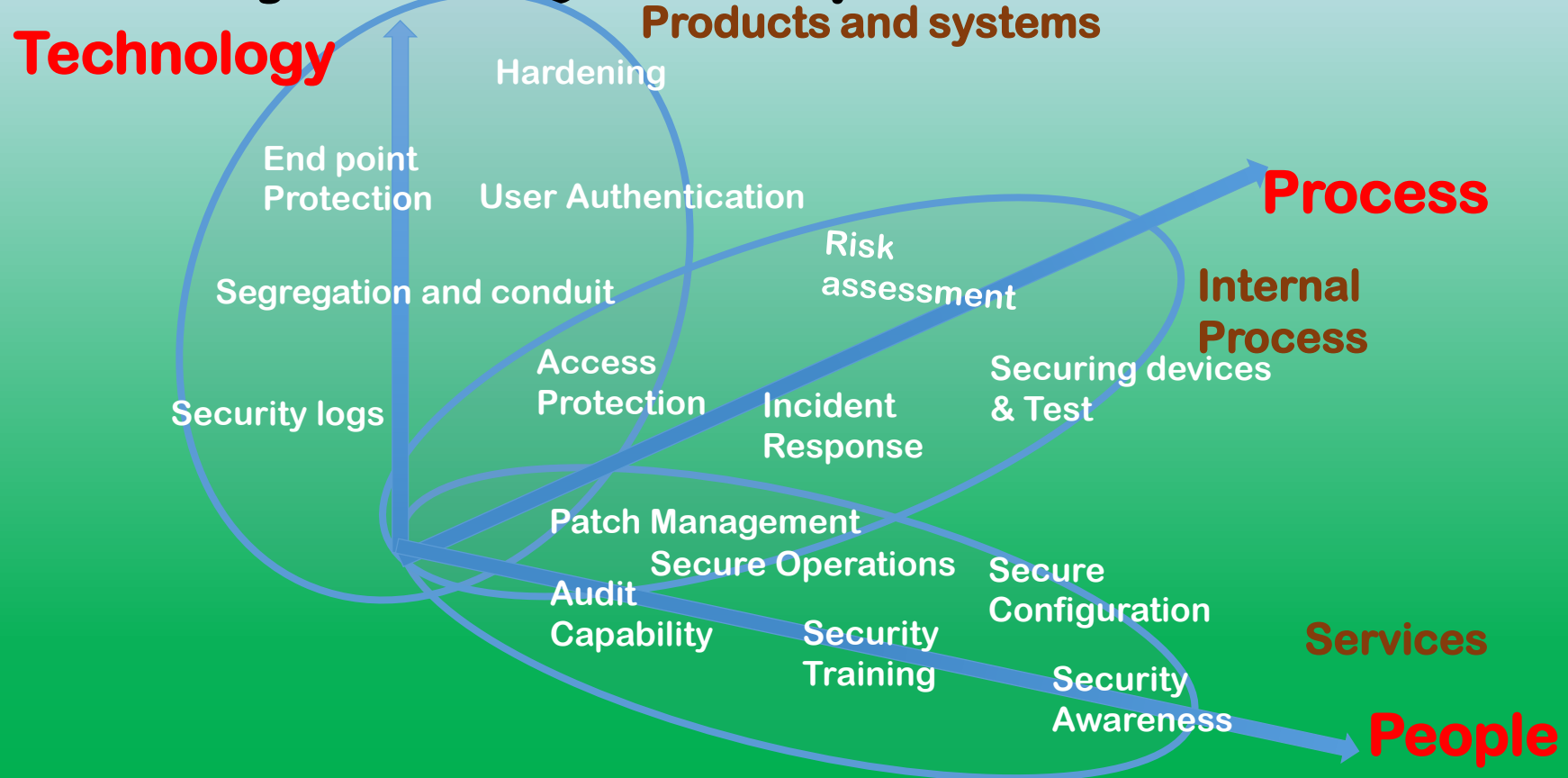
Improve process organisation

Cybersecurity is a continuous process

- Organisation is changing
- New vulnerabilities are always discovered
- Products evolves
- Threats changes



Cybersecurity driving concepts



Safety means protection of:

- Health
- Environment
- Assets

What is a Safety Instrumented System (SIS)?

Formal Definition:

SIS – “Instrumented System used to implement one or more safety instrumented functions (SIF). A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).”

[IEC61511 / ISA 84.01]

Informal Definition:

Instrumented Control System that detects “out of control” conditions and automatically returns the process to a safe state

SIS is: “Last Line Of Defence”





Safety System

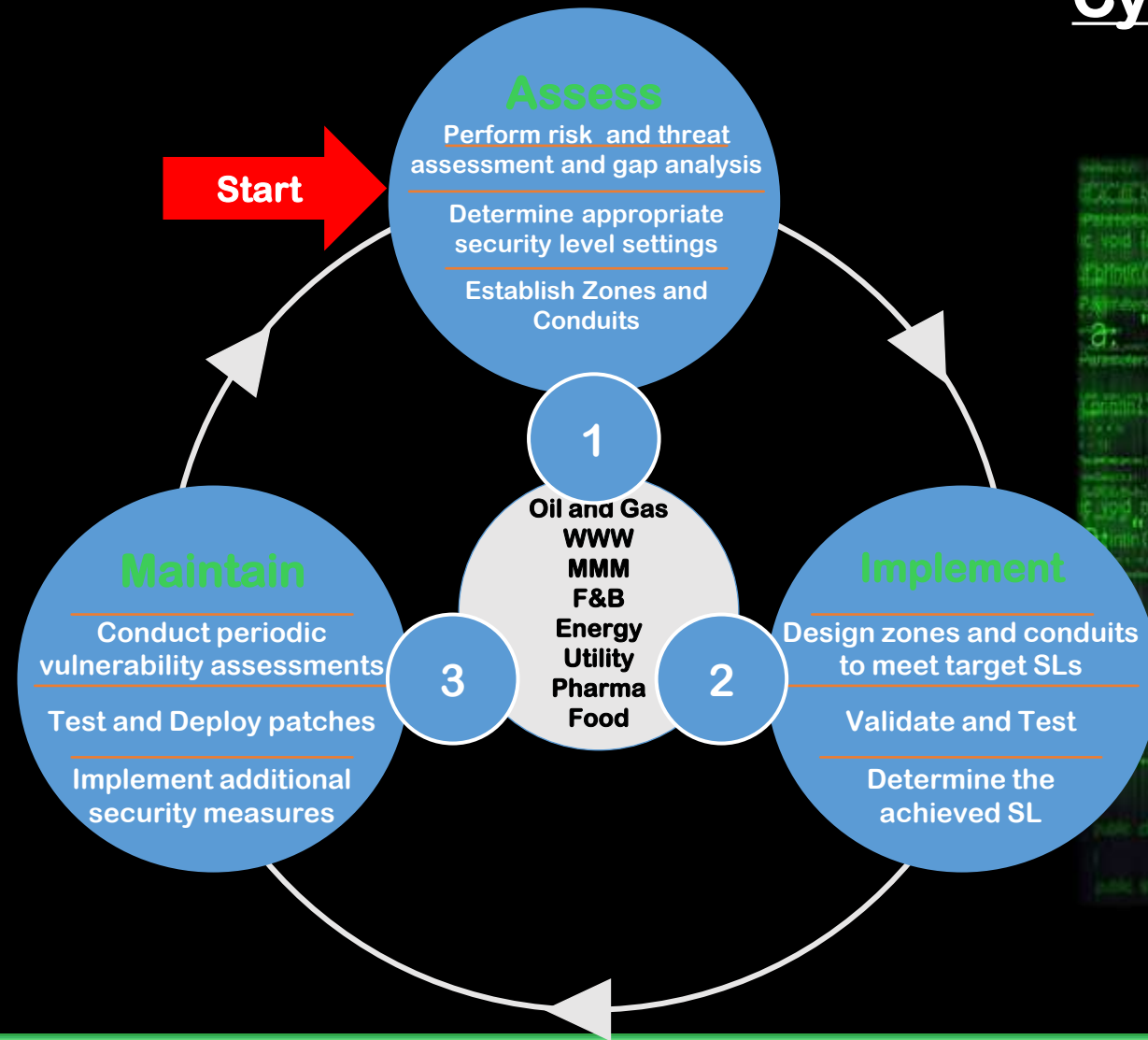
Distributed Control System

Corporate

SIS must be protected against cyber attacks

- Modern SIS systems are micro-processor based, programmable systems configured with a Windows PC
- Now it's common 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
- IEC 61508 (Safety Integrity Level (SIL) certification) doesn't evaluate security

Cybersecurity Lifecycle model

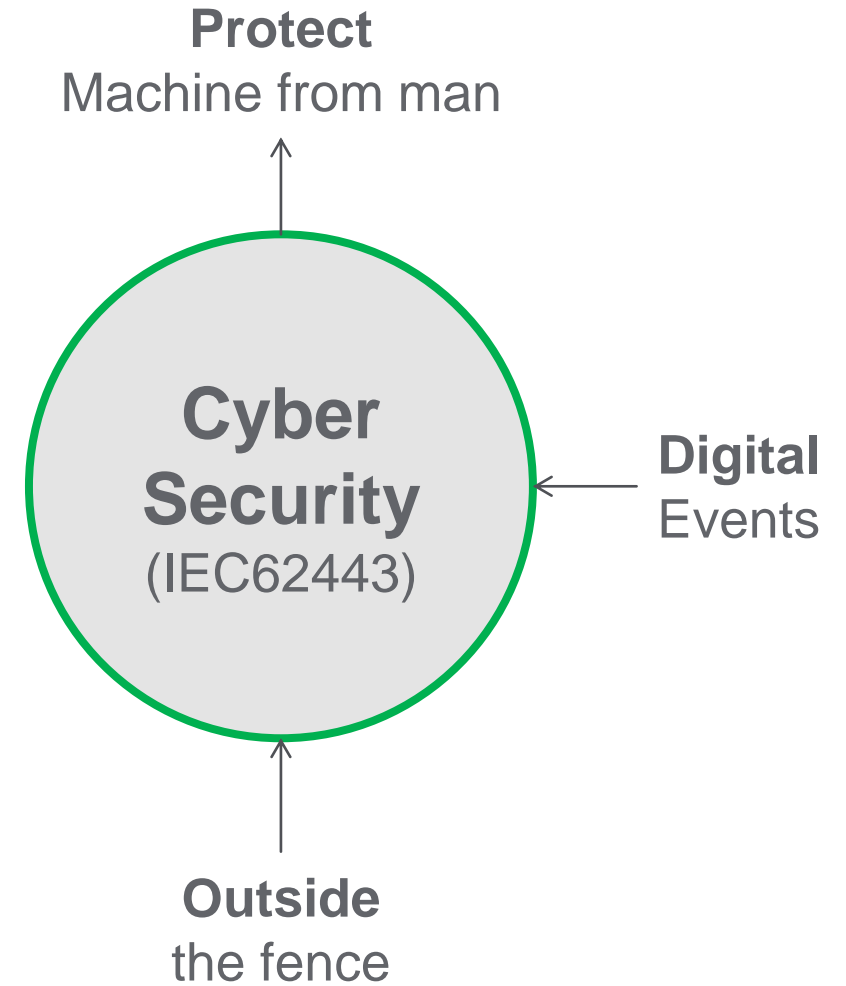
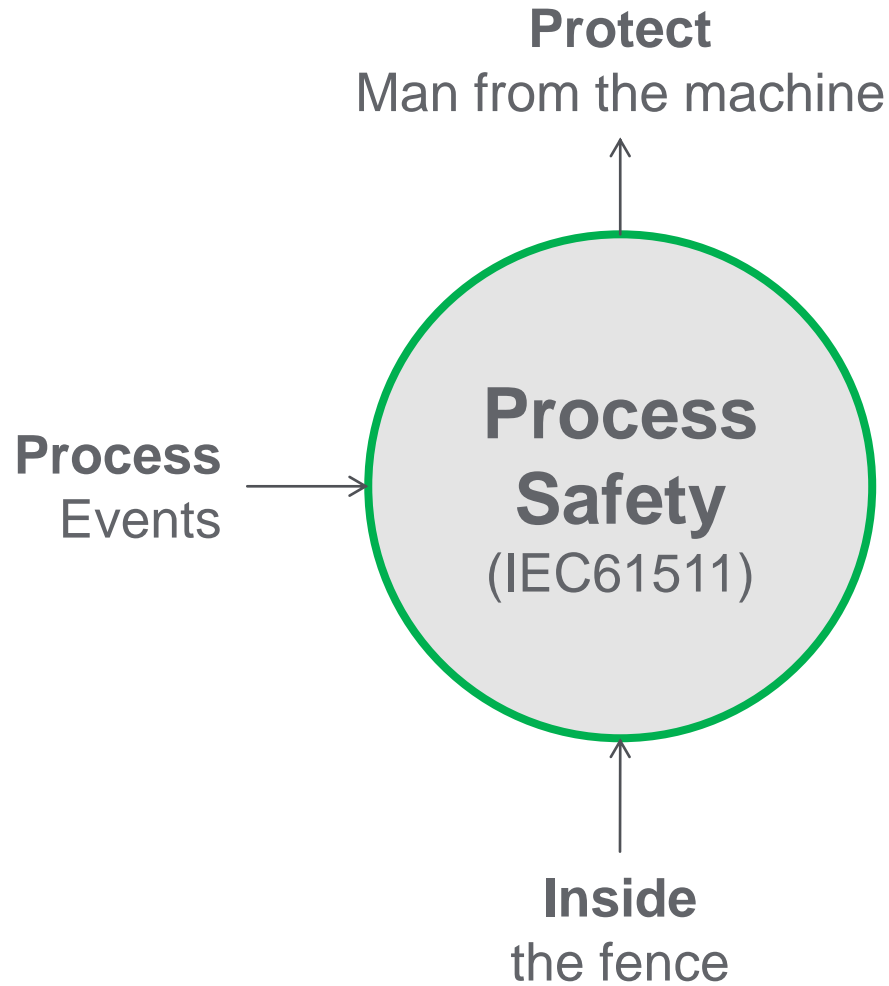


Adapted from IEC62443-1-1

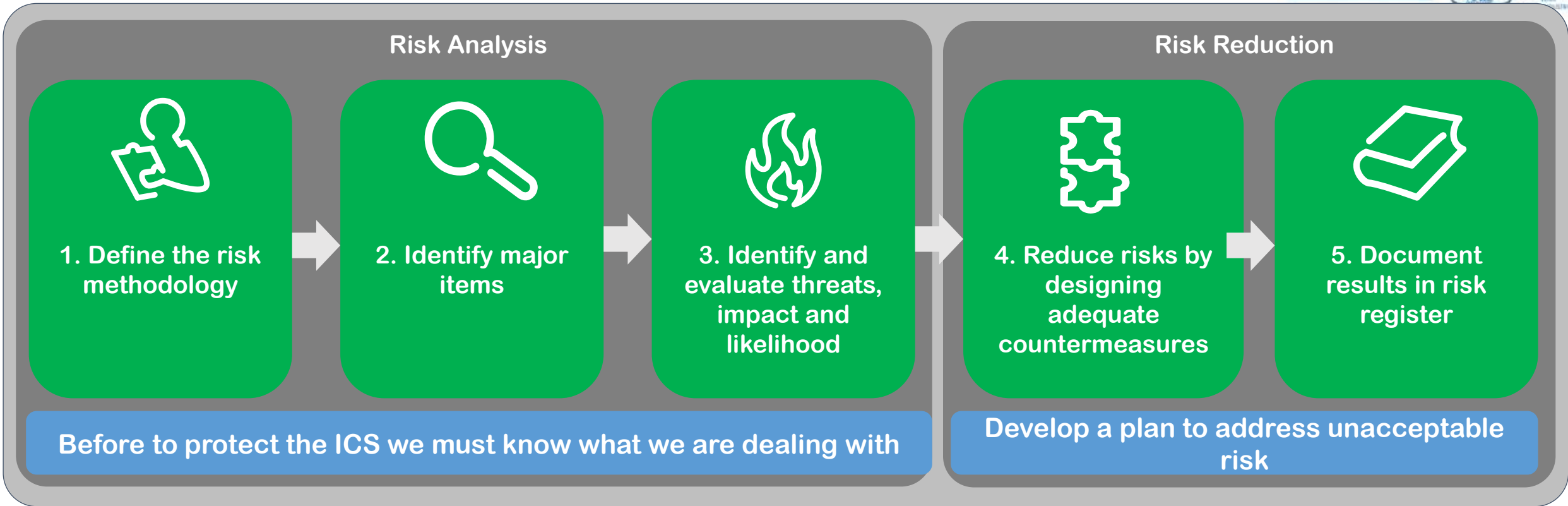
Assess

The risks and
threats

Know the risks



Cyber Security Risk Assessment



Each assessment must be site specific



Implement Defence in depth

Defense in depth

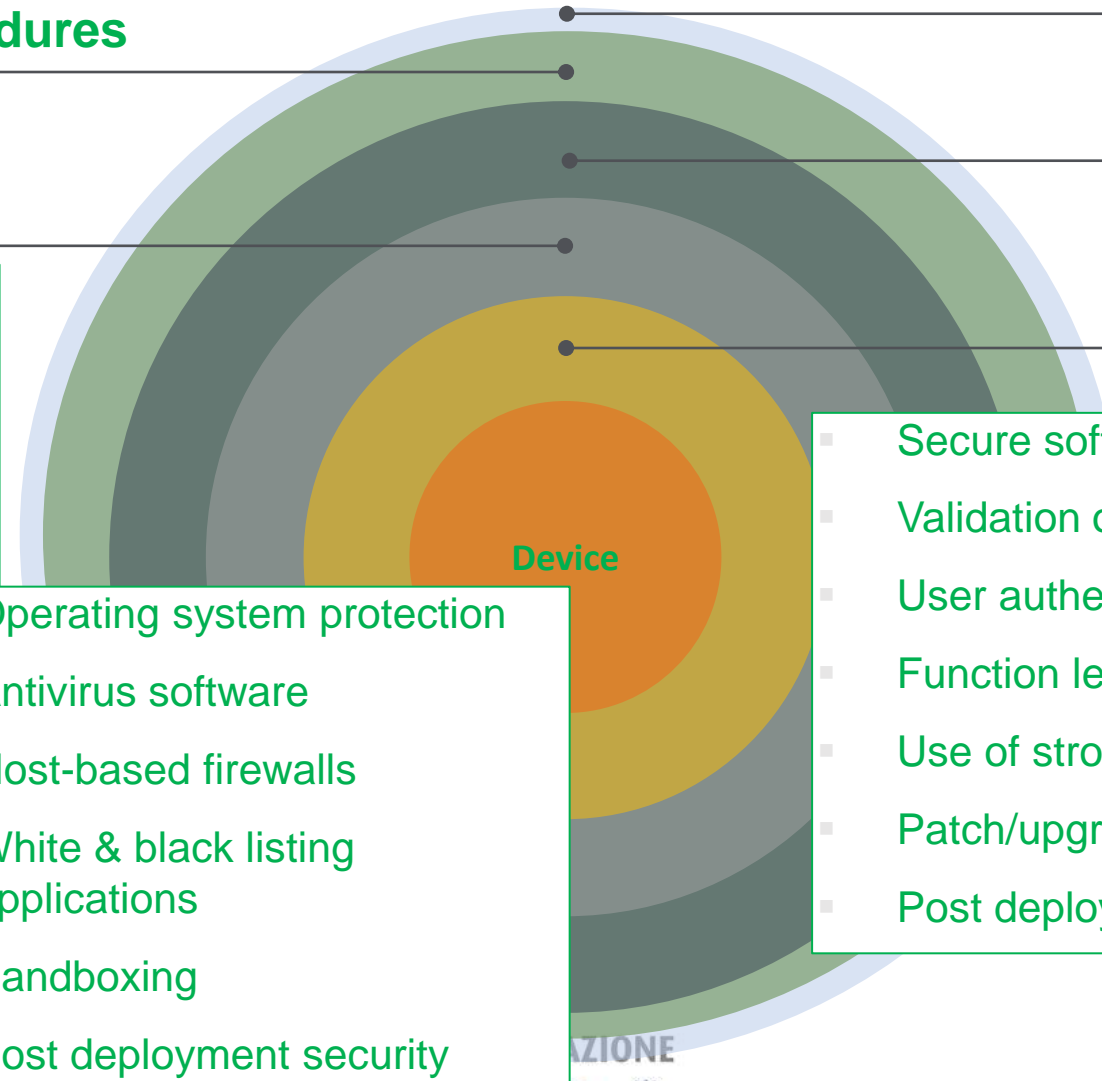
Policy and procedures

Physical security

Network security

Host Security

Application Security



- Secure architecture design
- Zone and conduit
- Least of privileges
- IDS
- NG Firewalls
- Patch/upgrade

- Operating system protection
- Antivirus software
- Host-based firewalls
- White & black listing applications
- Sandboxing
- Post deployment security

- Secure software design
- Validation of user input
- User authentication
- Function level access control
- Use of strong cryptography
- Patch/upgrade
- Post deployment security

Certification



Use Certified Products

- Any embedded product with an interface and IP Stack now undergo Embedded Device Security Assurance (EDSA) certification.
- For long development cycles devices will undergo Achilles certification in the interim. Workstations will also be Achilles certified



Developed in certified development centres

- Follow the Secure Development Lifecycle
- All Policies, Practices & Procedures reviewed / updated every quarter.



By certified authorities

- For Process Automation: exida, ISAsecure and TÜV for Safety

Certification underpins cybersecurity technology

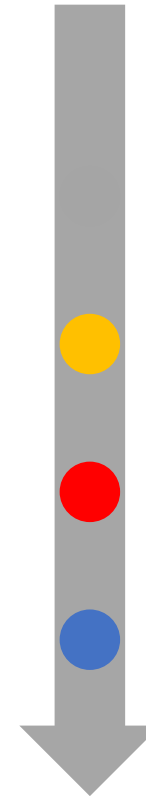
Security Profiles

Cyber Security

Security Level	Definition (IEC62443)
SL 1	Casual or coincidental violation
SL 2	Intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Intentional violation using sophisticated means with moderate resources , IACS specific skills and moderate motivation
SL 4	Intentional violation using sophisticated means with extended resources , IACS specific skills and high motivation

Safety

Safety Integrity Level	Safety	Probability of failure on demand
SIL 1	90% to 99%	1% to 10%
SIL 2	99 to 99.9%	0.1% to 1%
SIL 3	99.9% to 99.99%	0.01% to 0.1%
SIL 4	>99.99%	0.001% to 0.01%



Most stringent



Maintain

The highest
levels of cyber
protection

Owner / Operator Security Program

- Know the security risks that an organization faces
- Quantify and qualify risks
- Use key resources to mitigate security risks
- Define each resource's core competency and identify any overlapping areas
- Abide by existing or emerging security standards for specific controls
- Create and customize specific controls that are unique to an organization



-Patch Management

-Antimalware
-Backup and restore









Global Customer Support

Home SiteMap Links Support Documents Contact Us

Endpoint Protection

ALL Patches/Docs

Last Update: 23-Mar-17

Download	Filename	Date	Description	Size	Prod./Version	Product
	epo5800eng.zip	3/23/2017	McAfee 8.8 5800 Scan engine	3.55 Mb	McAfee 8.8 5800 Scan engine	VirusScan
	VSE880P7.zip	5/9/2016	Patch 7 is deemed a mandatory release for all environments and should be immediately installed to avoid potential security breaches. For additional details, including improvements and fixes, reference the McAfee VSE 8.8.0 Patch 7 Release Notes (P026382). Note - Patch 7 supports specific versions of McAfee Agent. The McAfee agent may be required to be updated prior to apply VSE patch 7.	67.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880MLRP7.zip	5/9/2016	VSE 8.8.0 With Patch 7 Reprint. For new installations, this install will include Patch 7 with the 8.8.0 install. In addition, McAfee Agent 4.8.0.1500 is also included which meets the minimum McAfee Agent version as noted in KB51111	35.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880P5.zip	8/23/2016	VSE 8.8.0 Patch 5 Required for VSE 8.8.0 installations running older Patch versions. Patch 5 is required in order to update to VSE 8.8.0 Patch 7.	43.9 Mb	VirusScan 8.8.0	VirusScan
	VSE880P2.zip	8/14/2012	This release contains a variety of improvements and fixes. Please review the PATCH2.HTM file embedded within the .zip file. Virus Scan 8.8 Patch 2 must be installed prior to attempting to install Patch 4 and later on 64 bit systems.	16.8 Mb	VirusScan 8.8.0	VirusScan
	SOLDCOR620-S08_WDL.zip	3/16/2016	Solid Core Update. Required for VSE 8.8 Patch 7 installation on ePO 5.3.0.	130 Mb	ePO 5.3.0, ePO 5.1.1	SolidCore
	MA503WDL.zip	2/15/2016	McAfee Agent 5.0.3. While primarily used as a client-side component providing secure communications between ePO and managed products, the McAfee agent also serves as an updater for McAfee Products. As noted in McAfee KB51111, the McAfee Agent may require an update to support the VSE 8.8 Patch 7 installation. In some instances, the Patch 7 update has been noted to hang or the setup will fail to start when attempting the install with no warning message provided to the end user. Updating the McAfee Agent will correct these installation issues.	37.4 kb	Agent 5.0.3	McAfee Agent
			McAfee Agent 4.8.0.1995 Upgrade. While primarily used as a client-side component providing secure communications between ePO and managed products, the McAfee agent also serves as an updater for McAfee Products. As noted in McAfee			

Steve Elliott
United Kingdom
EURA
FOXBORO






IEC 62443 Security Levels in ICS

Practical Implementations

sps ipc drives
ITALIA

 **ANIE**
AUTOMAZIONE
 

 messe frankfurt

Which Cybersecurity Model apply?

Single Layer

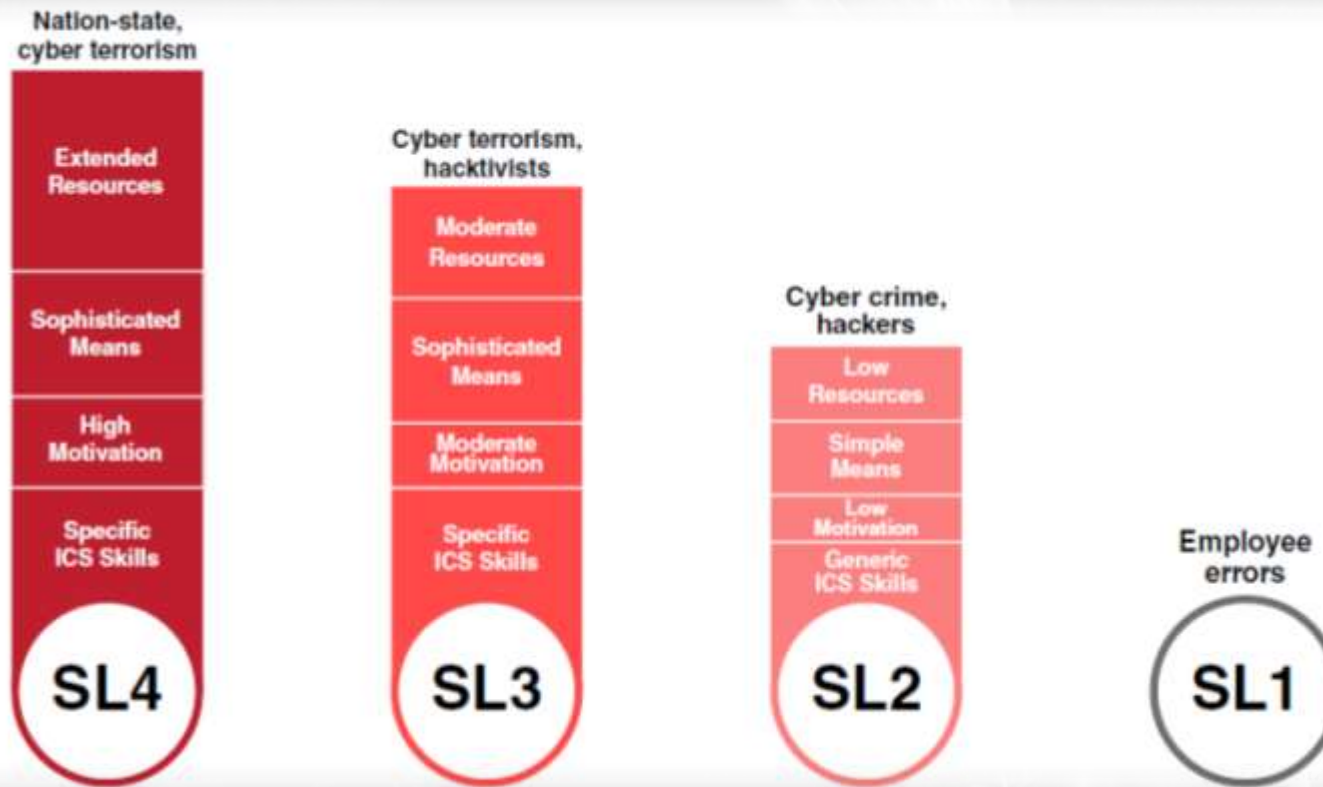


OR

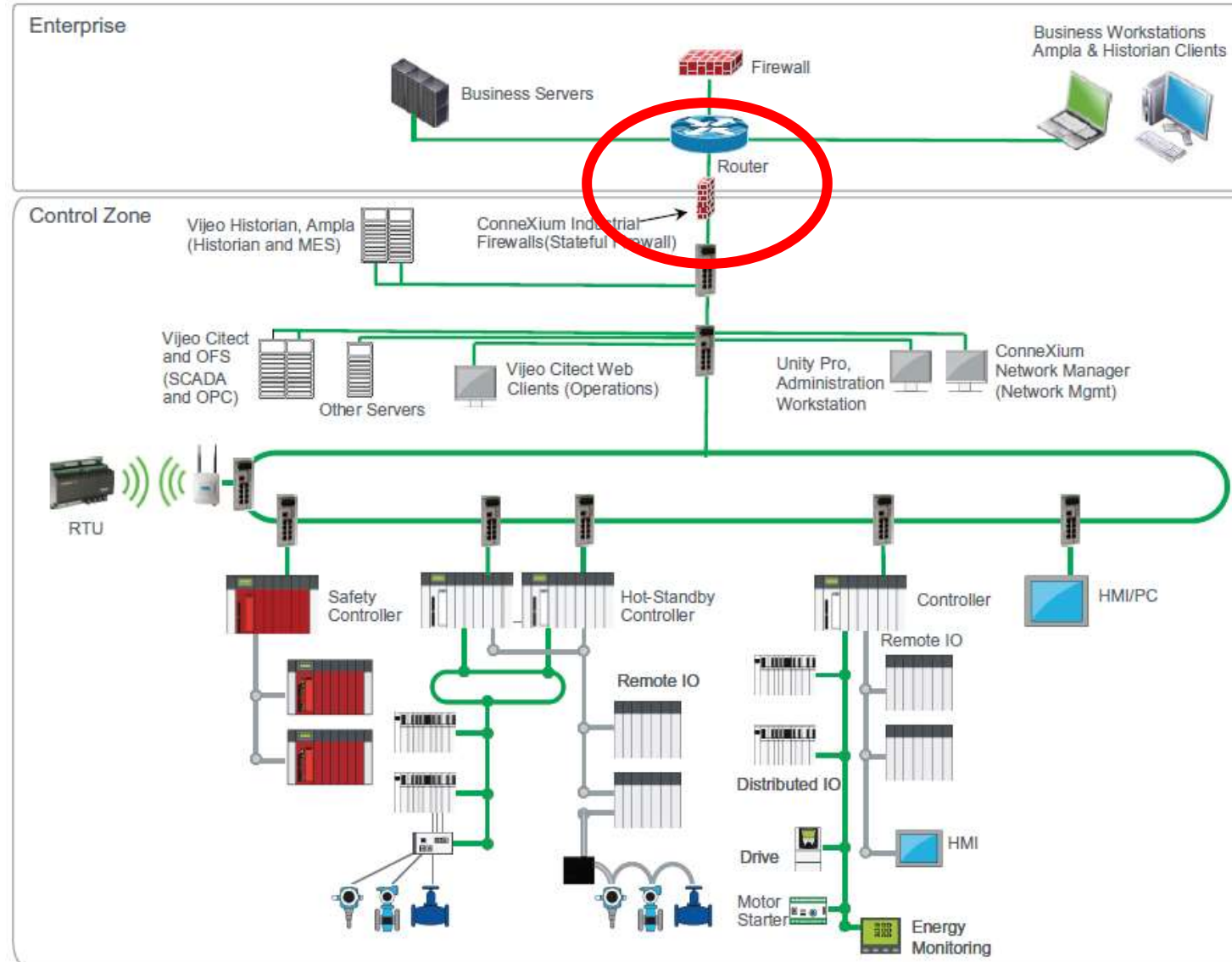
Defense in Depth



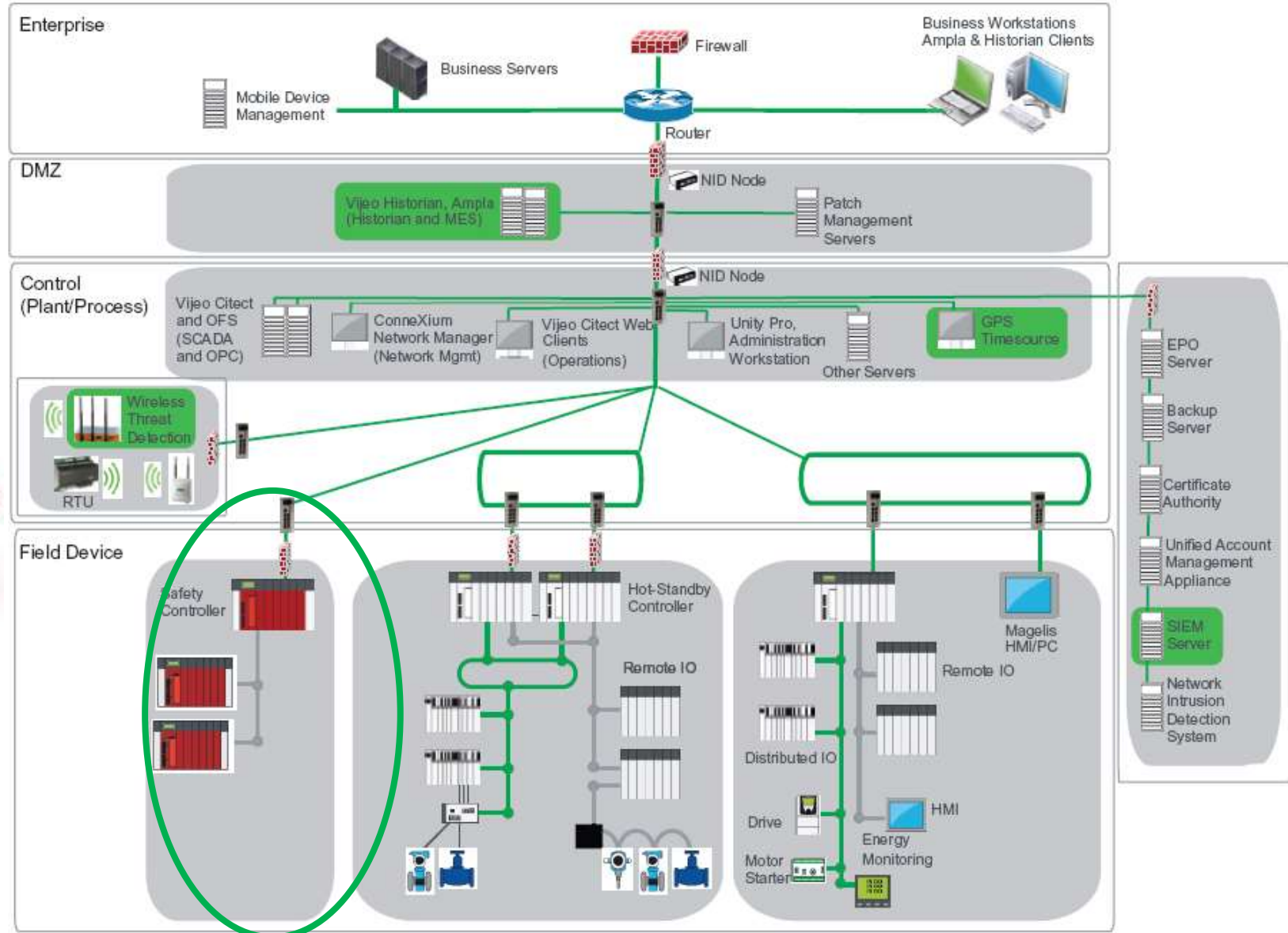
IEC 62443.3.3 Security Level (SL)



SL 0




SL 3



Network Information Security (NIS) Directive

EU 2016/1148

- The first European Union (EU) wide cybersecurity legislation
- As an EU directive, every EU member has to adopt national legislation
- DL 65/2018: Italy receipt NIS Directive in June 2018 

Part 1

National capabilities

Part 2

Cross-border capabilities

Part 3

National supervision of critical sectors



<https://www.enisa.europa.eu/>

Directive identifies “Operators of Essential Services” as target



Grazie per l'attenzione.

Umberto Cattaneo, *PMP, Security+, ISA99/IEC62443 Certified Specialist*