://Arena_Digital_&_Software/

Software Industriale

ANIE

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

sps ipc drives
ITALIA

ANIE AUTOMAZIONE

messe frankfurt

Federazione ANIE

Federazione Nazionale Imprese Elettrotecniche ed Elettroniche

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

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 €

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.

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

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

Software Industriale

- 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;

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

sps ipc drives ITALIA

ANIE AUTOMAZIONE

messe frankfurt

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);

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

- organizzare eventi di divulgazione dei temi relativi al software industriale ed in particolare organizzare un forum di riferimento per questa tecnologia abilitante.

www.forumsoftwareindustriale.it

forum Software Industriale

NAPOLI
08_10_2019
Stazione Marittima, Centro Congressi
Molo Angioino, Napoli Porto

TAVOLA ROTONDA

Software Industriale 4.0
IL MOTORE DELLA CRESCITA

Casi pratici raccontati dai fornitori di tecnologia

ANIE AUTOMAZIONE

messe frankfurt

Software Industriale

sps ipc drives
ITALIA

ANIE AUTOMAZIONE

messe frankfurt

Cybersecurity what does it mean?

Software Industriale

Assure *data Confidentiality, Integrity and Availability* by:

Protecting the systems against hacking

- Intentional

Protecting the system against errors

- Non intentional

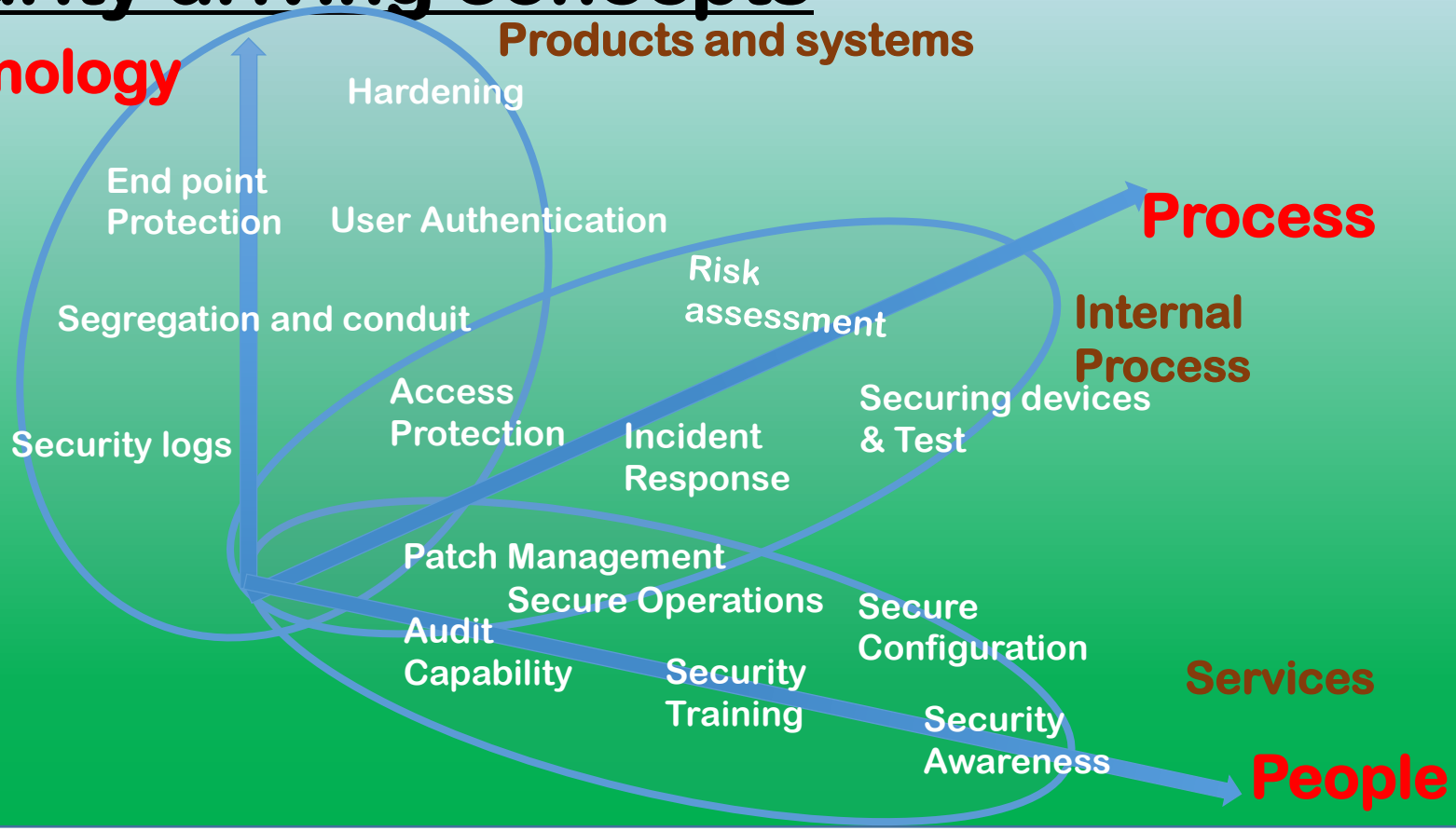
Improve operation and maintenance processes

Improve process organisation

Cybersecurity is a continuous process

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

Cybersecurity driving concepts



Software Industriale

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

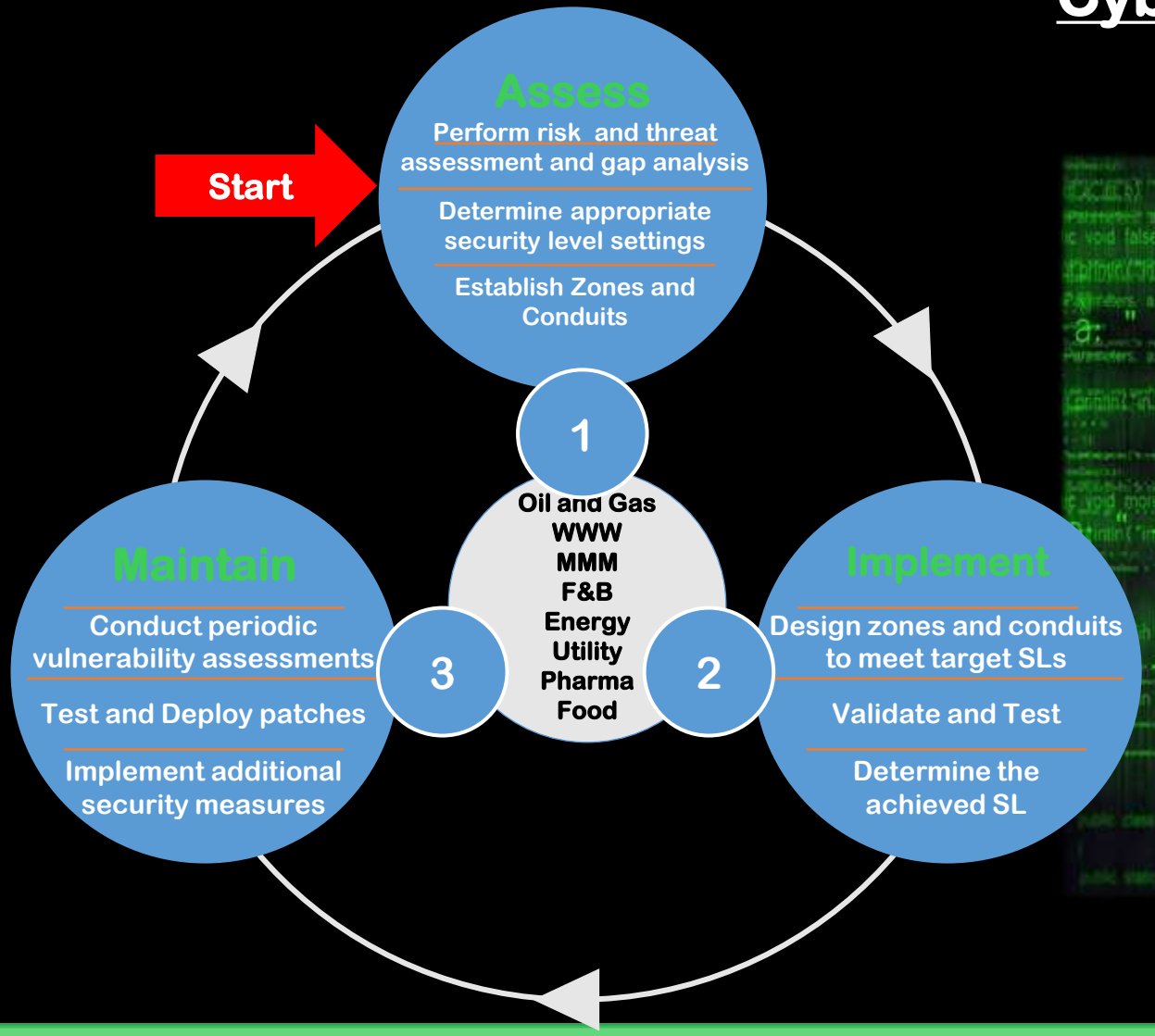
SIS is: "Last Line Of Defence"


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

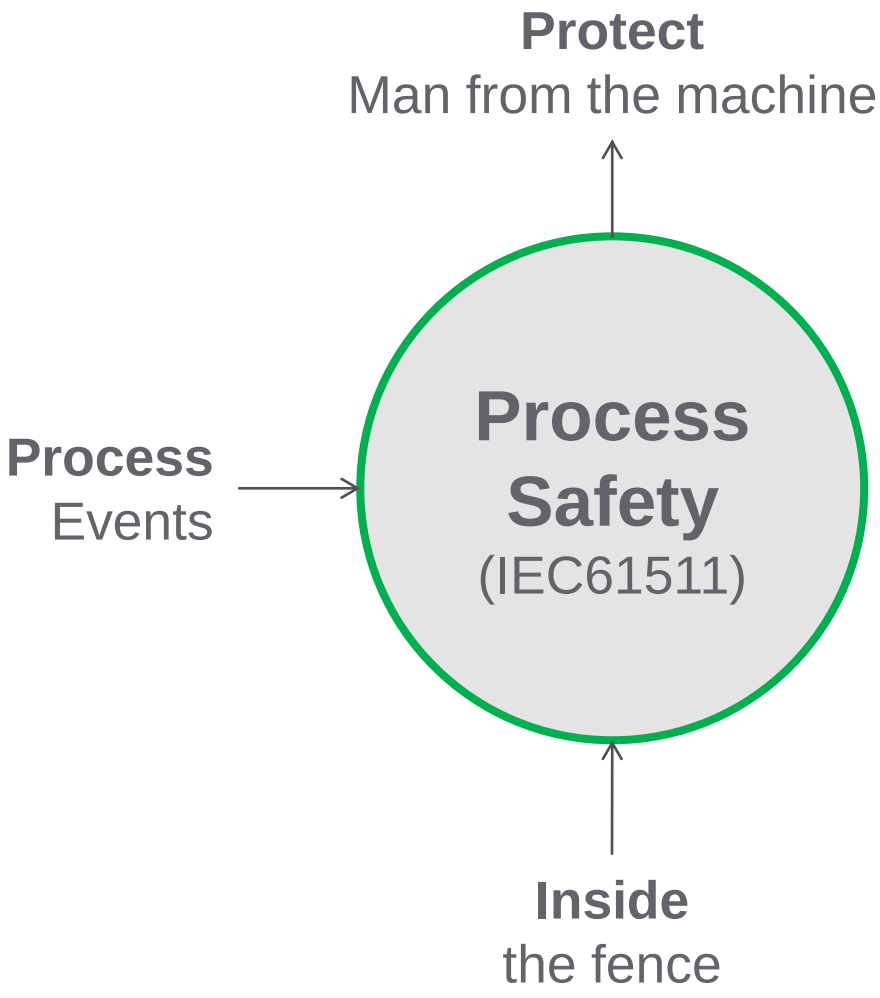


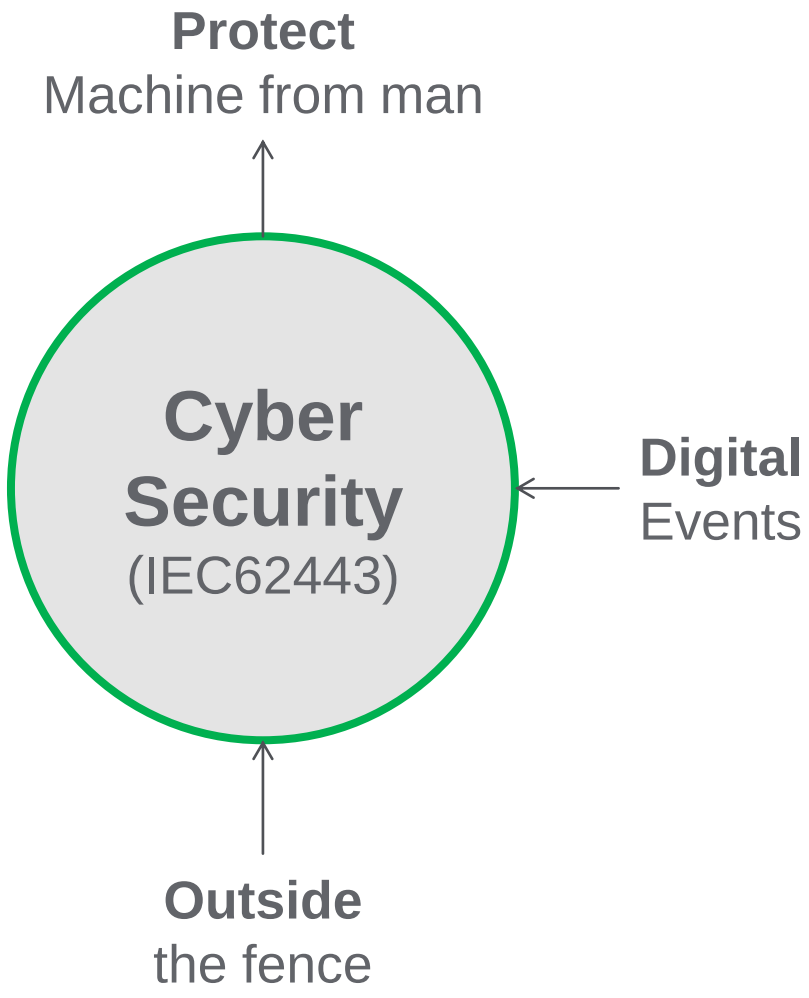
Adapted from IEC62443-1-1

Assess

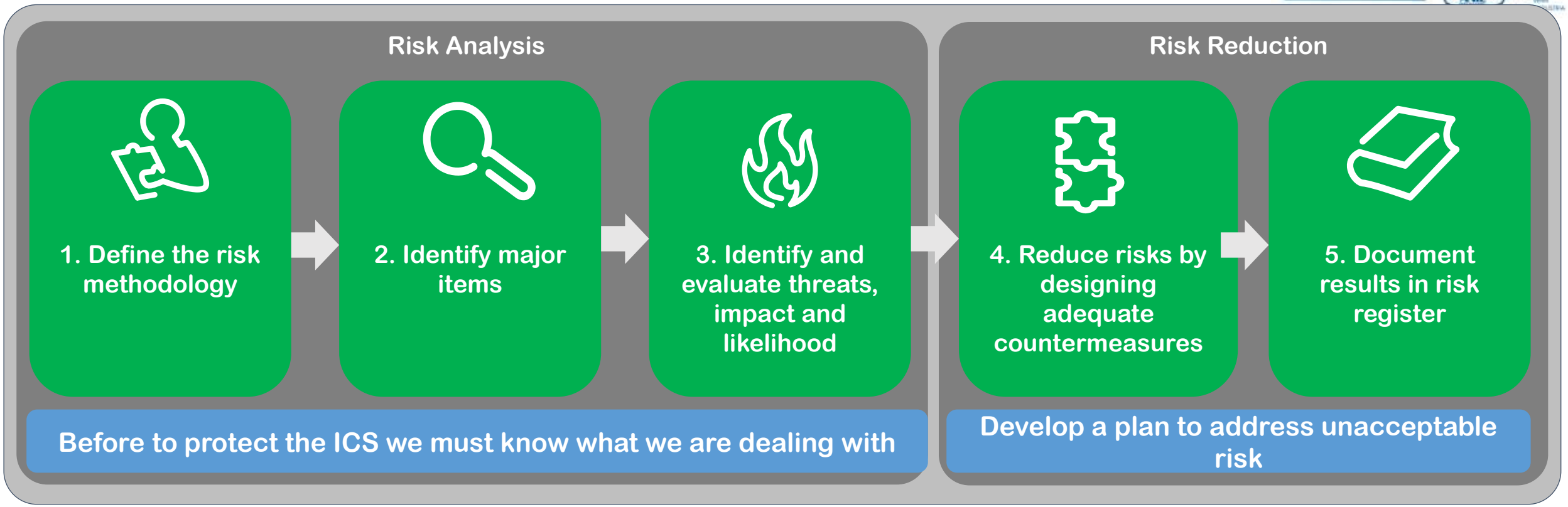
The risks and threats

Know the risks

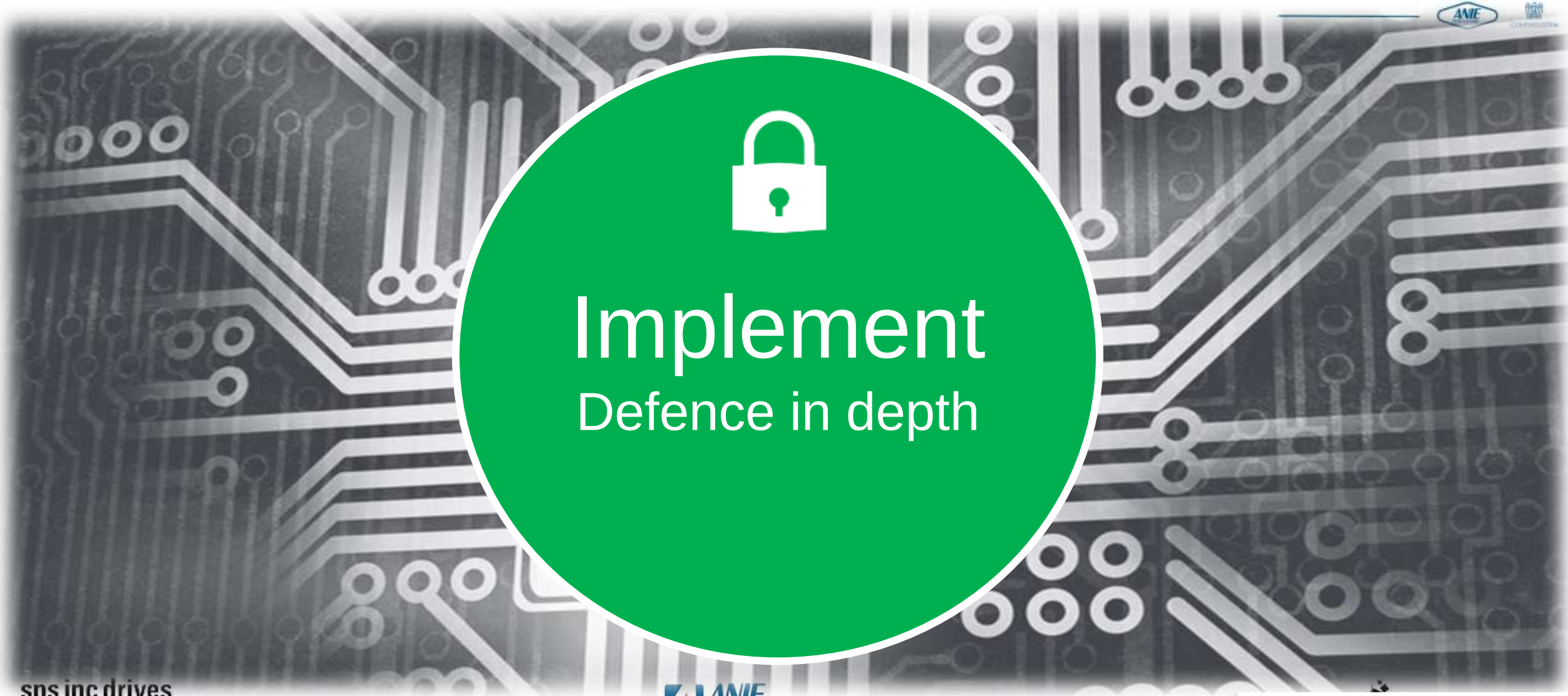




Cyber Security Risk Assessment



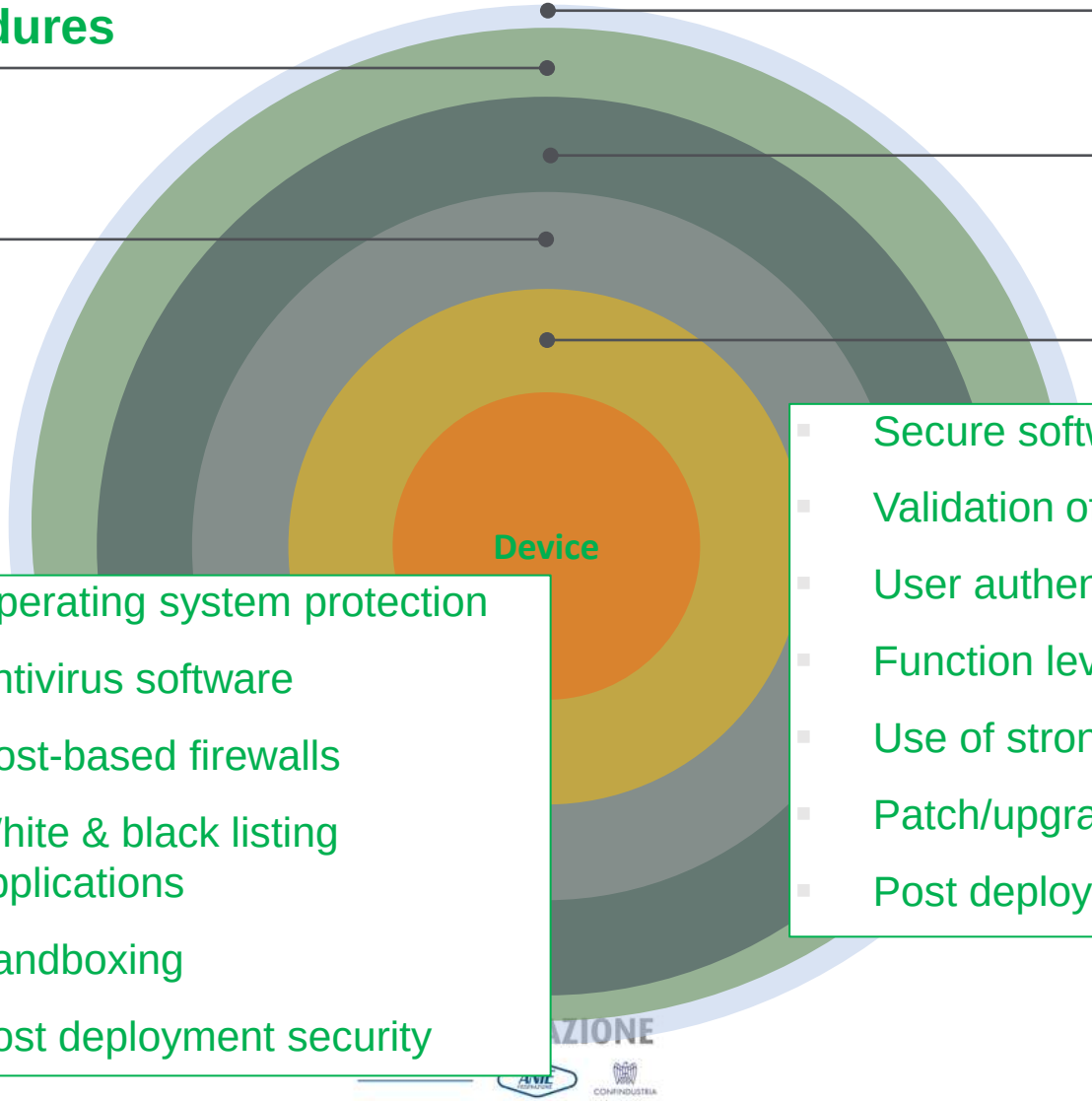
Each assessment must be site specific



Implement

Defence in depth

Defense in depth



Physical security

Policy and procedures

Network security

Host Security

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

Application Security

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

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

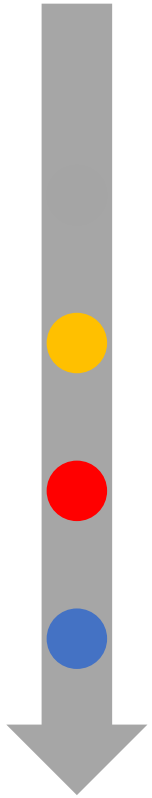
- For Process Automation: exida, ISAsecure and TÜV for Safety

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



Most stringent

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%

Software Industriale

sps ipc drives
ITALIA

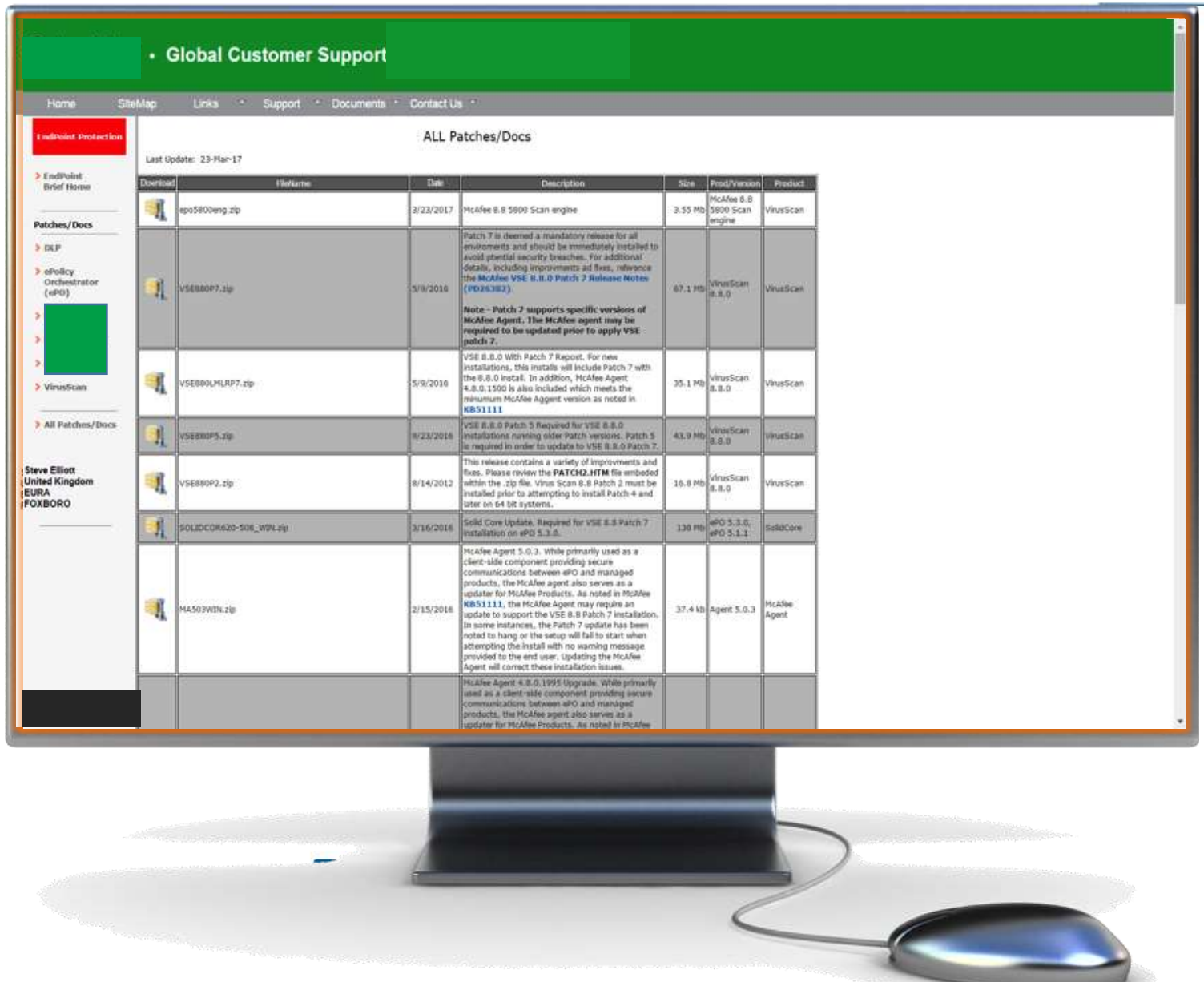
ANIE AUTOMAZIONE

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



Software Industriale

Software Industriale

IEC 62443 Security Levels in ICS

Practical Implementations

sps ipc drives
ITALIA

ANIE AUTOMAZIONE

messe frankfurt

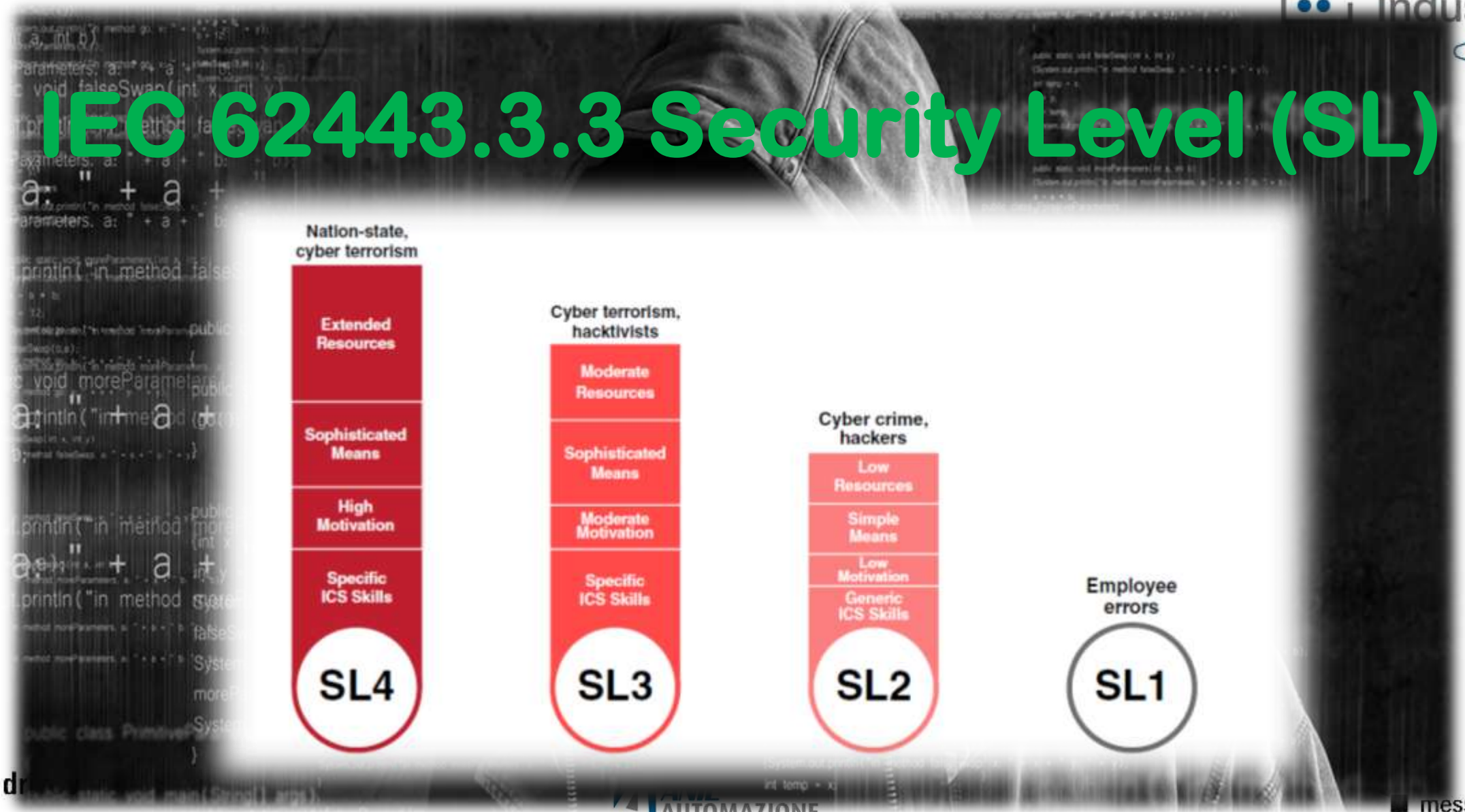
Which Cybersecurity Model apply?

Single Layer

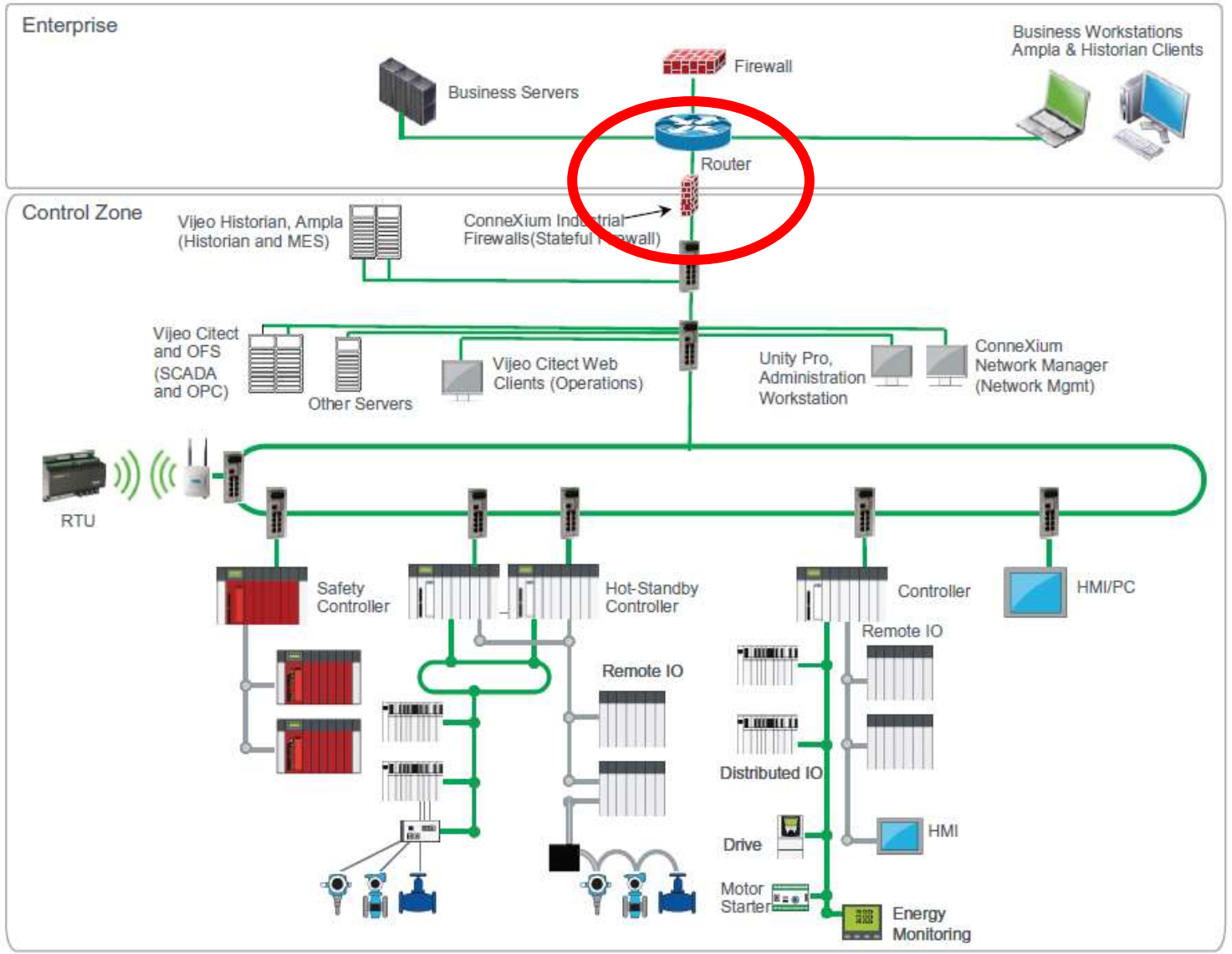
OR

Defense in Depth

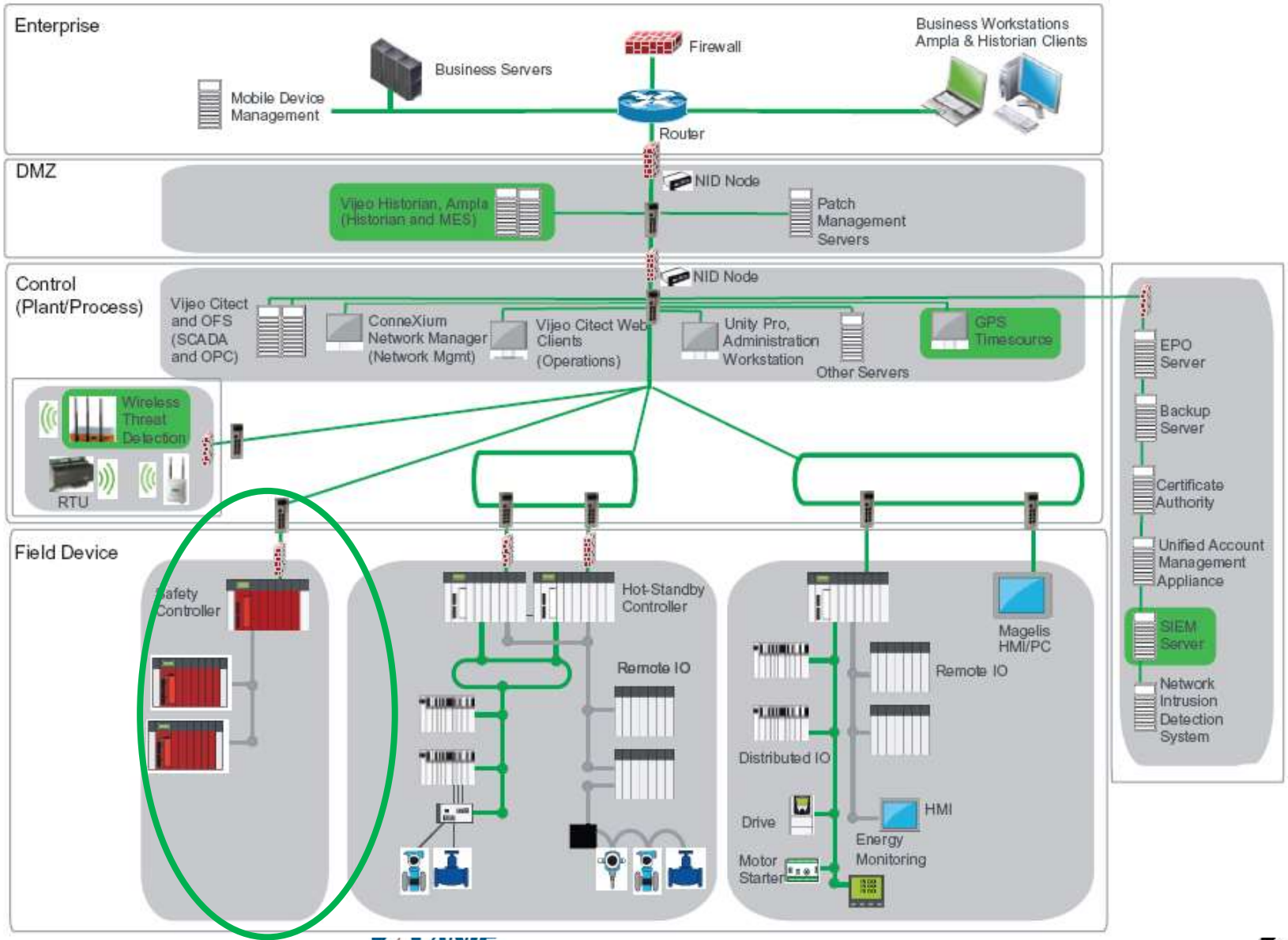
IEC 62443.3.3 Security Level (SL)



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	Part 2	Part 3
National capabilities	Cross-border capabilities	National supervision of critical sectors

enisa European Union Agency for Network and Information Security

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*