Cybersecurity OT

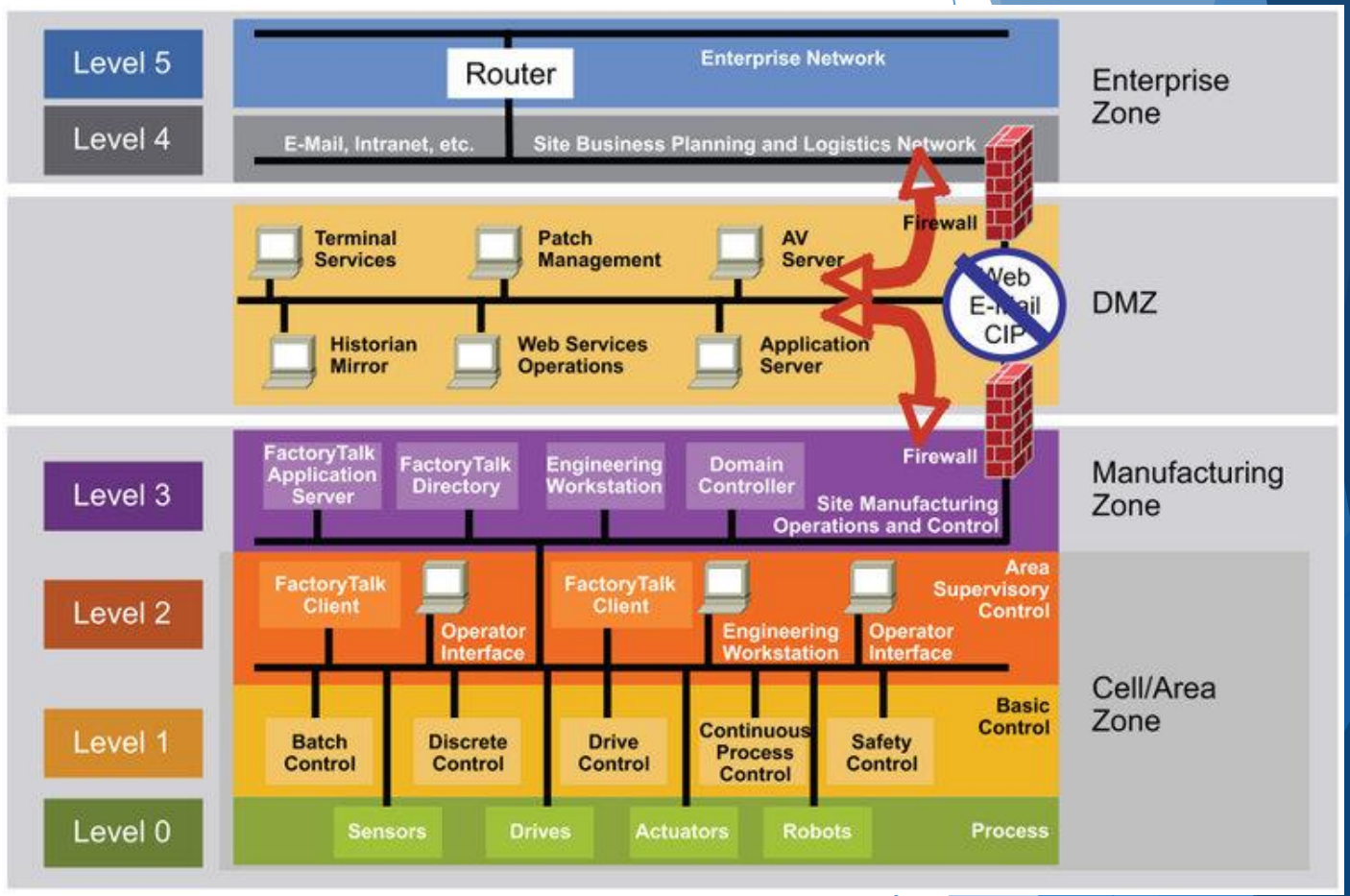
Micaela Caserza Magro

Modello di riferimento

Purdue model 1990

(PERA)
Purdue
Enterprise
Reference
Architecture

Comparrimentazione chiara
.
Divisione tra IT e OT per mezzo di DMZ



Che cosa è la cyber security?

Cyber security si riferisce alla protezione dei dati..

I dati devono essere protetti contro:

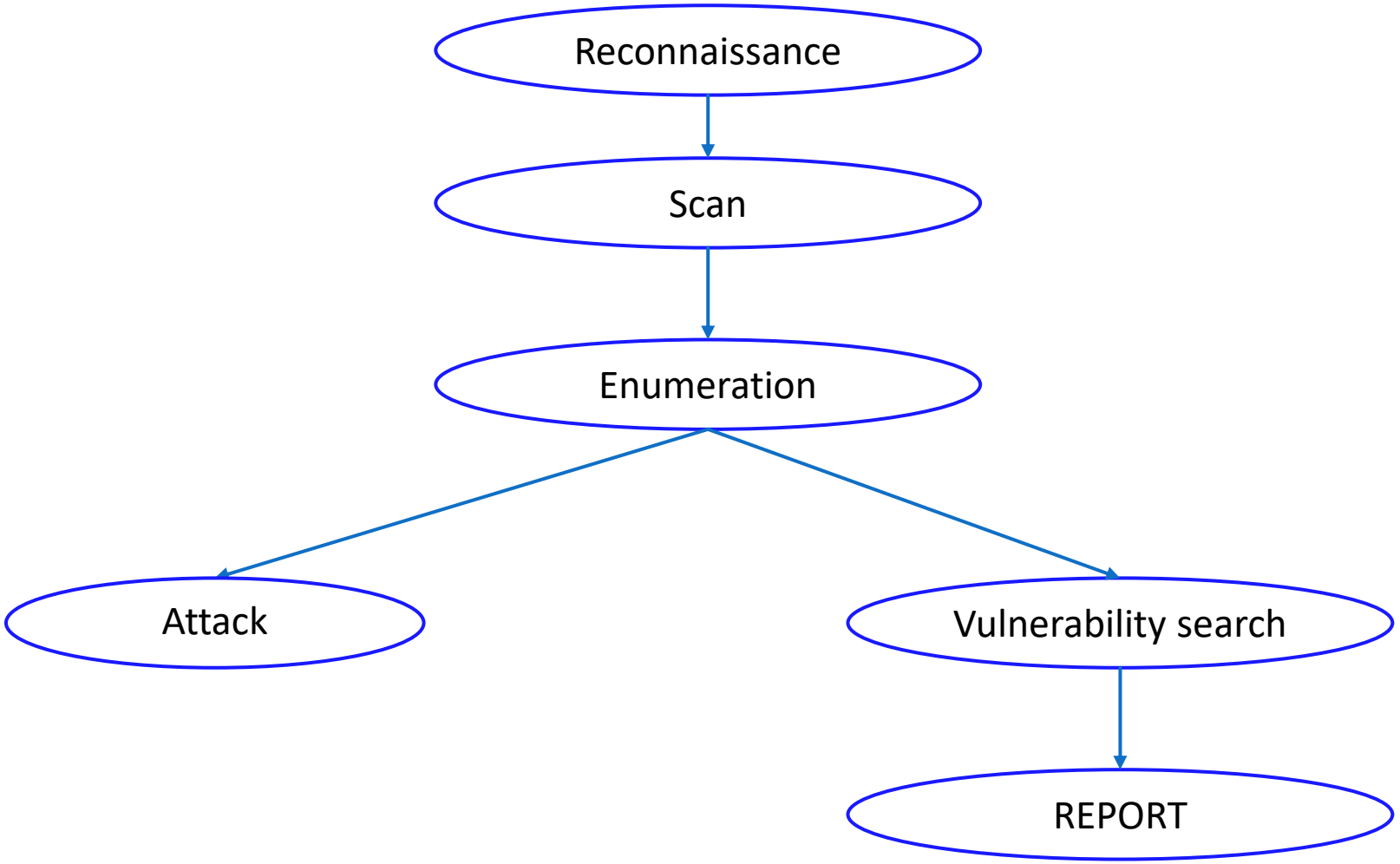
- Intercettazione e divulgazione
- Manipolazione fraudelente

Dove devo assicurare la sicurezza dei dati?

- Residenti su un host
- In transito

Se i dati sono compromessi devo essere in grado di accorgemene

Struttura di attacco cyber



Quali sono i requisiti della cyber security?

Availability

Integrity

Confidentiality

Authentication

Authorization

No-repudiation

Auditability

Risk analysis

- Il rischio nel mondo safety è calcolato come:

RISK = PROBABILITY X IMPACT

- Il rischio nel mondo security è calcolato come:

RISK = THREAT X VULNERABILITY X IMPACT

Minacce

Minacce	Descrizione
Non-intentional accidental errors	Employees actions that can cause cybersecurity issues.
Amatorial Hacker	They have access to tools and onliune resources that can find systems connected to internet and to interfere with their operations, both for challenge and prestige
Professional Hacker	Hackers with more abilities and resources that attack organizations with ransomware and other techniques to obtain profits
Hacktivist	Hackers groups with the scope of create damages to organizations which have opposite social and politics ideas
Disgruntled employee	They use their knowledge and their privileged accesses to interfere with production or planning, or steel sensible data.
State and terrorists	Organizations with very large resources that attack critical infrastructures to create instabilities or to create fear, they can also steel strategical information.

IEC 62443

Struttura:

È divisa in 4 sezioni

14 pubblilcazioni

- 8 standard
- 6 technical report

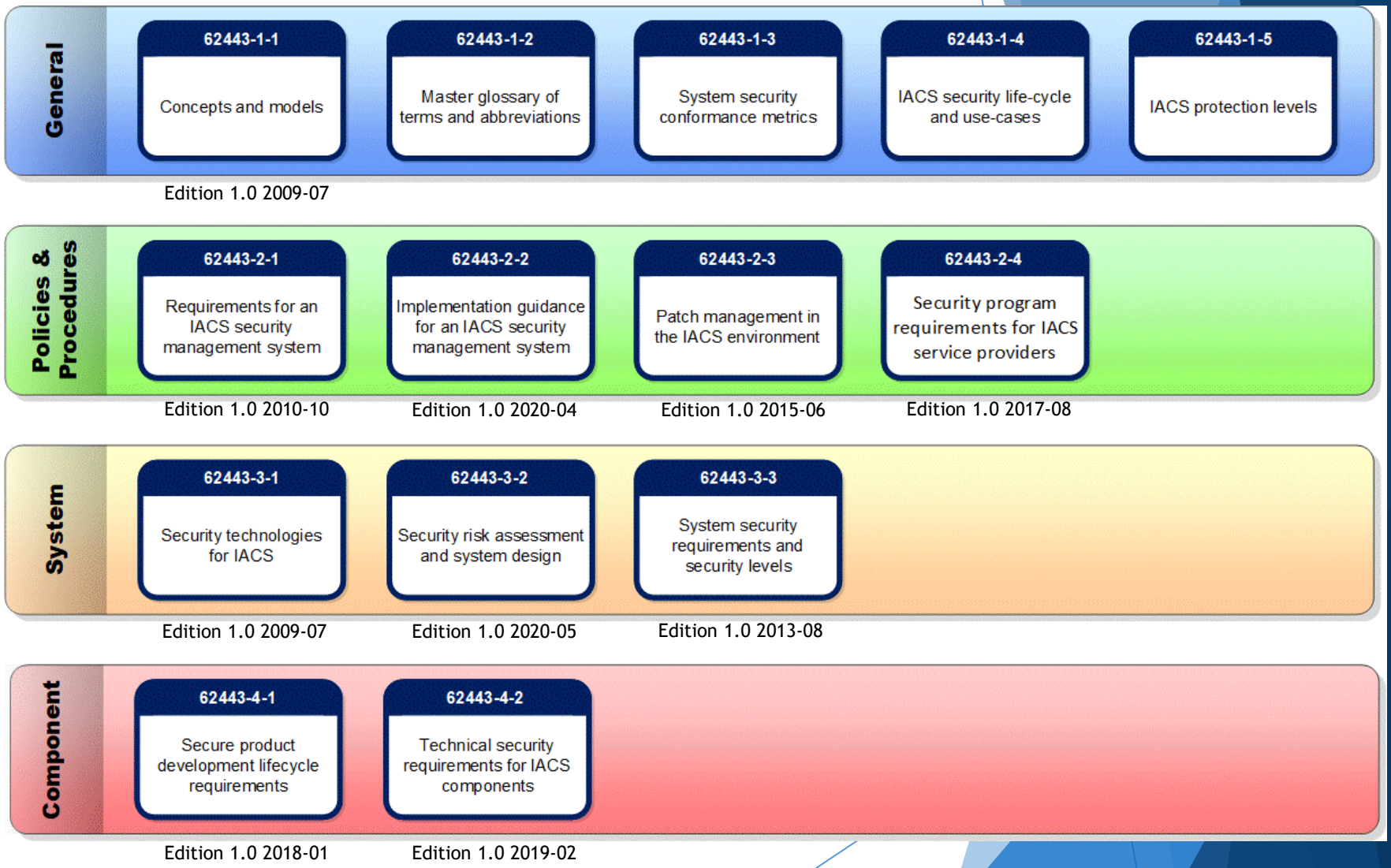
10 disponibili

Vengono definiti 3 ruoli:

-Asset owner

-System integrator

-Product developer



IEC 62443

Asset owner

Documental:

- IEC 62443 2-1
- IEC 62443 2-4

Requirements:

- IEC 62443 2-4

System integrator

Documental:

- IEC 62443 2-4
- IEC 62443 3-2

Requirements :

- IEC 62443 3-3

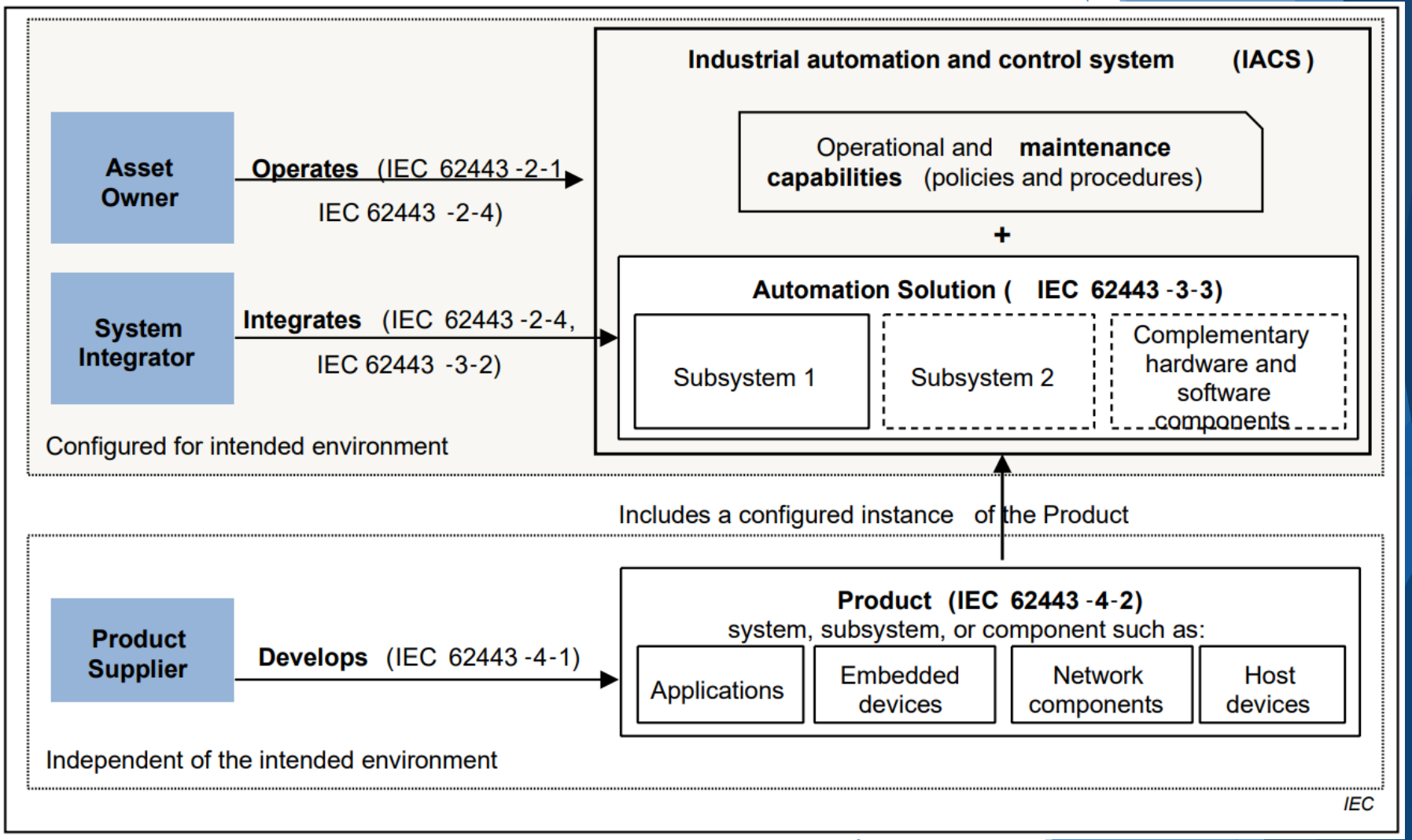
Product developer

Documental:

- IEC 62443 4-1

Requirements :

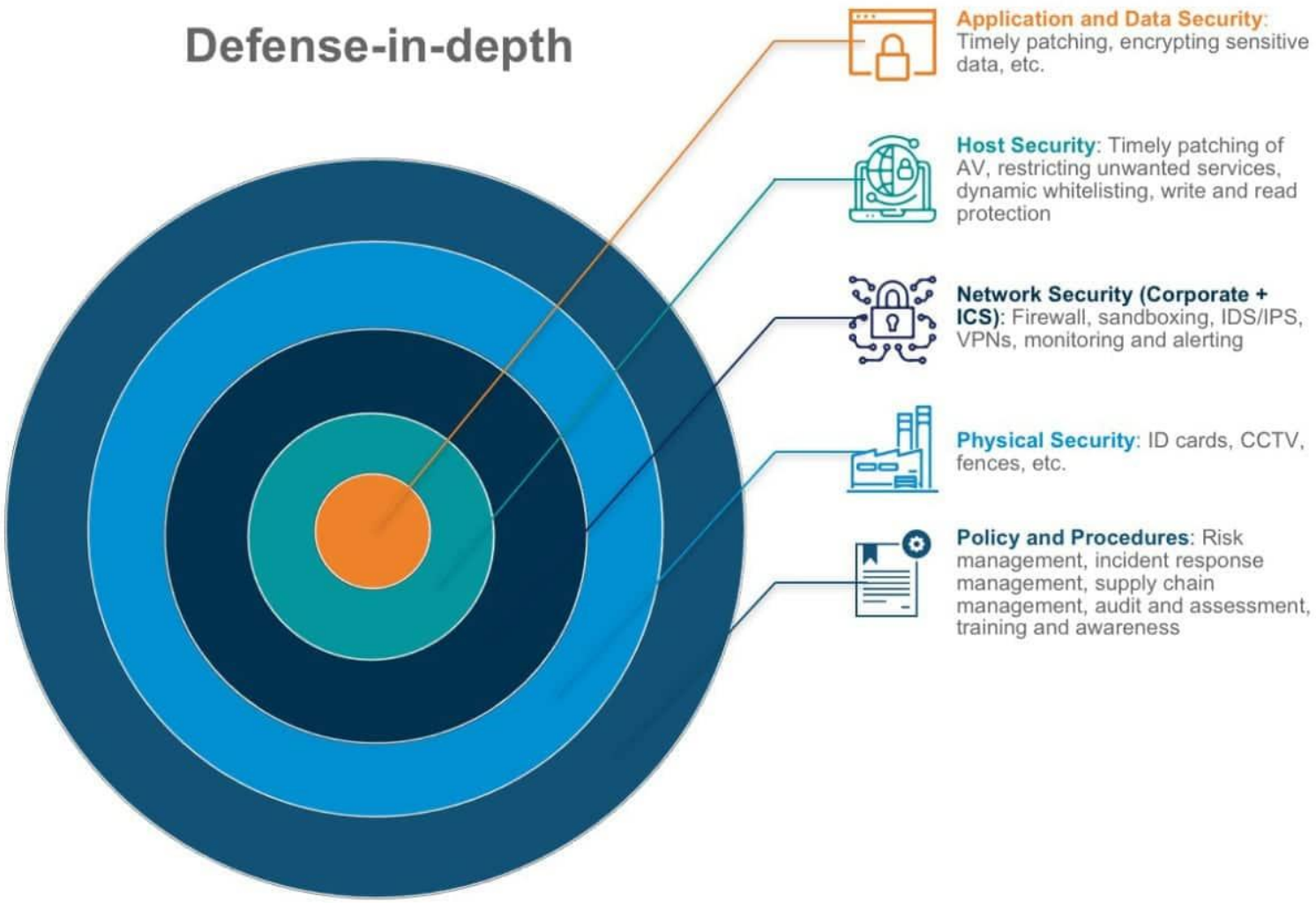
- IEC 62443 4-2



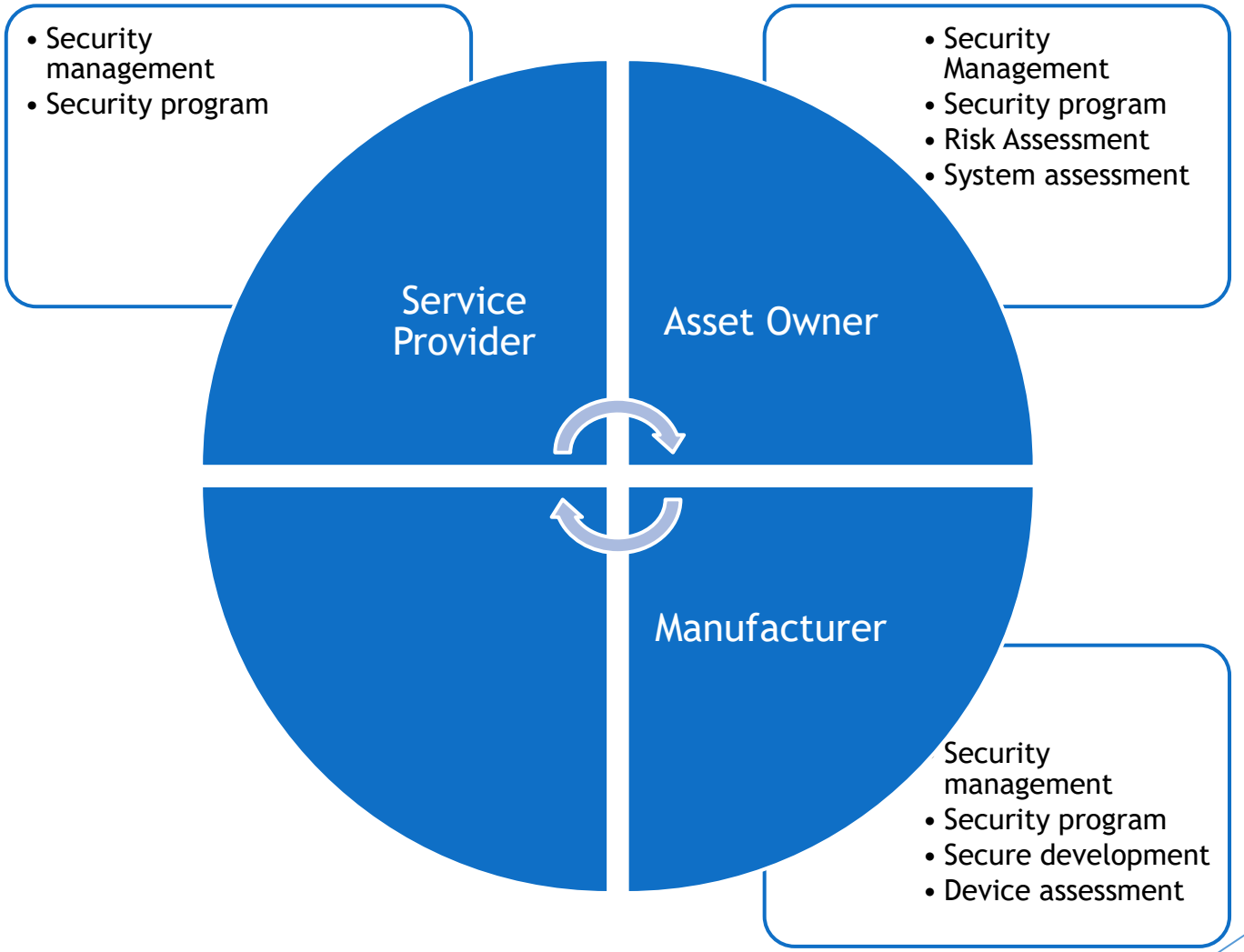
Security Process

IEC 62443

Lo standarda prevede l’approccio di defense in depth e di security by design



Security roles



Maturity level

- In alcune parti dello standard che richiedono parti più legate alla parte documentale(ad esempio 2-4, 3-2, 4-1), i requisiti richiesti in termini di processi, policies e procedure vengono valutati tramite i maturity level.
- Vengono definiti 4 livelli:
    1. Livello **iniziale**: quanto richiesto nel requisito è presente, ma viene svolto in una maniera non documentata
    2. Livello **gestito**: le policies e procedure sono state scritte ed il personale è stato formato ed ha le competenze tali da soddisfare quel requisito
    3. Livello **definito**: si aggiunge al livello precedente che il processo è stato applicato almeno una volta
    4. Livello **ottimizzabile**: il processo si può misurare ed è possibile applicare un continuo miglioramento

LIVELLI DI SICUREZZA (SL)

- Livello 0
  - non sono necessari né specifici requisiti né protezioni di sicurezza
- Livello 1
  - necessaria protezione contro errori accidentali (errori degli impiegati)
- Livello 2
  - necessaria protezione contro azioni volontarie compiute da soggetti con mezzi comuni, poche risorse, skills generiche riguardo I sistemi di controllo e bassa motivazione (Hacker amatoriali)
- Livello 3
  - necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse moderate , skill specifiche riguardo I sistemi di controllo e moderata motivazione (Hacker professionisti, hacktivisti)
- Livello 4
  - necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse estese , skill specifiche riguardo I sistemi di controllo e alta motivazione (nazioni e terrori

Recap

Maturity level

- IEC 62443-2-2
- IEC 62443-2-4
- IEC 62443-4-1

Security Level

- IEC 62443-3-3
- IEC 62443-4-2

IEC 62443 3-3, 4-2

Security requirements

Fundamental requirements	IEC 62443 3-3		IEC 62443 4-2	
	SR	RE	SR	RE
Identification and authentication control (IAC)	13	11	14	10
Use control (UC)	12	12	13	12
System integrity (SI)	9	9	14	9
Data confidentiality (DC)	3	3	3	2
Restricted data flow (RDF)	4	7	3	3
Timely response to events (TRE)	2	1	2	1
Resource availability (RA)	8	6	8	3

SR: Security Requirements RE: Requirement Enhancement

IEC 62443

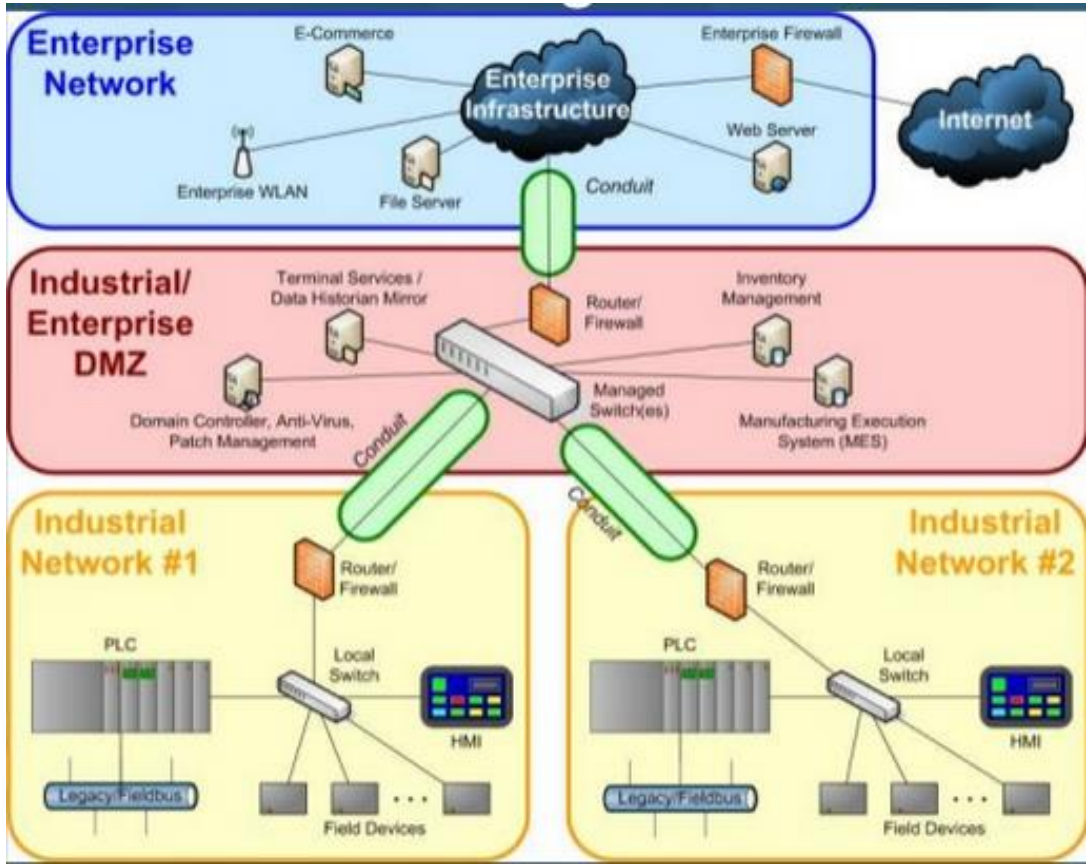
L’impianto deve essere diviso in condotti e zone

- Zona:

Porzione fisica o logica dell’impianto composta da asset che condvidono la stessa posizione e gli stessi requisiti di security

- Condotti:

È un caso particolare di zona dedicato al flusso di dati/Informazioni. È rappresentato da un canale di comunicazione che consente la comunicazione in una zona, tra le zone e tra la zona ed i limiti del trust.



GENOA FIELDBUS

G F

C C

COMPETENCE CENTRE

Grazie per l’attenzione!

Micaela.caserzamagro@gfcc.it