Cybersecurity nella trasformazione digitale di imprese e impianti: IEC 62443 e aspetti applicativi

Sergio Saponara, sergio.saponara@unipi.it
Delegato Terza Missione del DII (Dipartimento Ingegneria dell'Informazione)
Presidente LT e LM in Ingegneria Elettronica
Università di Pisa

Trasformazione Digitale in Imprese e Impianti

Le tecnologie digitali stanno cambiando radicalmente il modo in cui le aziende lavorano, producono, competono e creano valore

Maggiore connettività porta ad una maggiore superfice di attacco (spesso da remoto) per la cybersicurezza

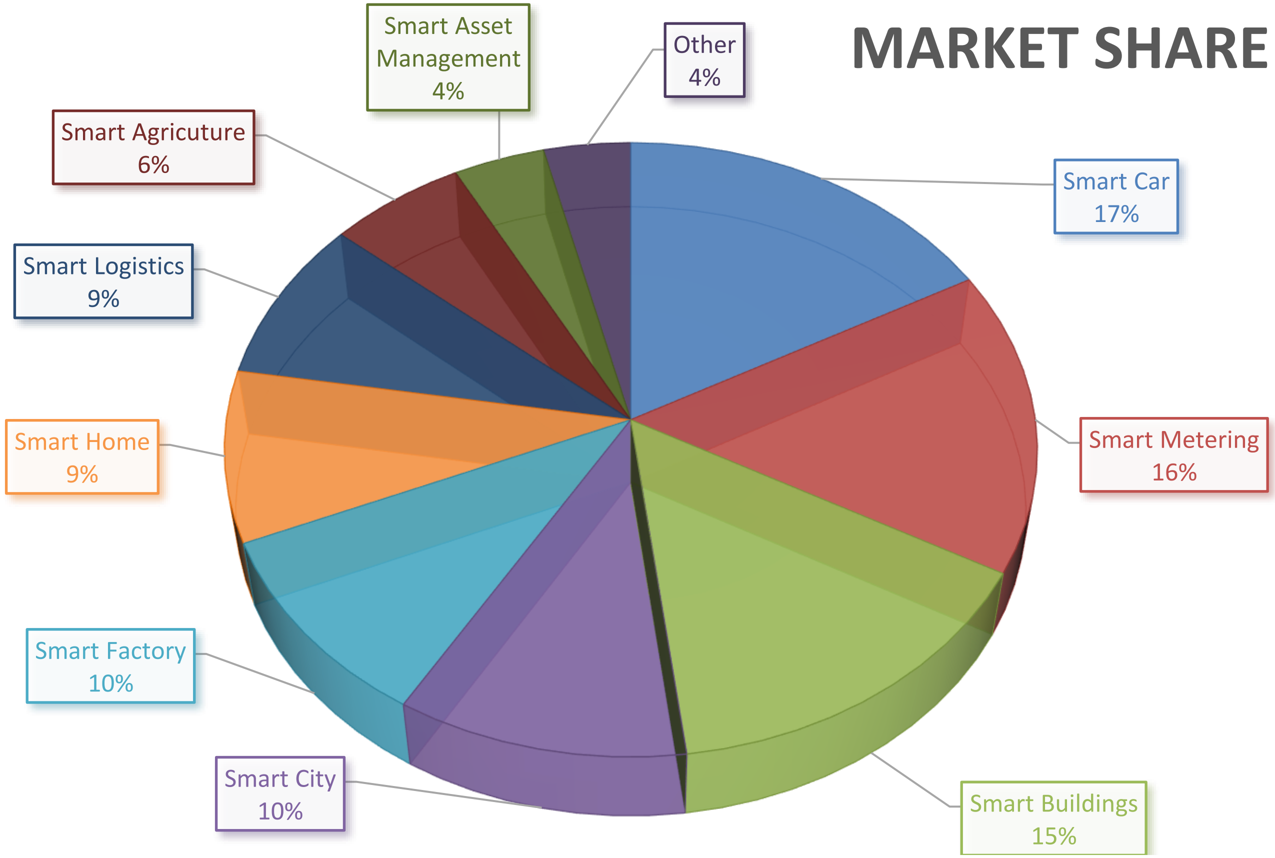
Uso di sistemi autonomi/automatizzati (Robotica, AI) aumenta la severità delle conseguenza di un attacco di cybersicurezza

Internet of Things (IoT) in Italia

IoT in Italia (2023)

- 140 Milioni dispositivi connessi
- 2.4 dispositivi IoT per abitante
- 9 Miliardi di € (+ 9% rispetto a 2022)

MARKET SHARE



https://www.osservatori.net/it/ricerche/comunicati-stampa/internet-of-things-italia-mercato

Intelligenza Artificiale

migliorare l'accuratezza e la precisione delle diagnosi mediche

rendere più veloce la scoperta di nuovi farmaci

mitigare le vulnerabilità di reti e sistemi

aumentare l'accuratezza dei sistemi di identificazione facciale

individuare le misure di **sicurezza informatica**

contrastare le frodi

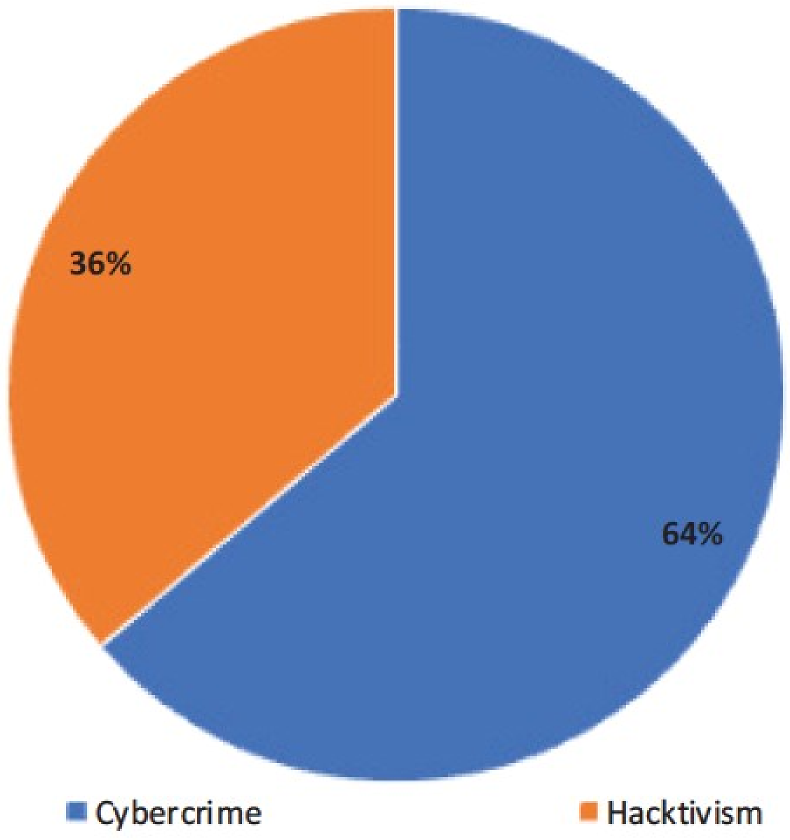
AI generativa usa tecniche di Machine Learning e Deep Learning per generare nuovi contenuti, tra cui immagini, musica e testo, che non esistevano in precedenza

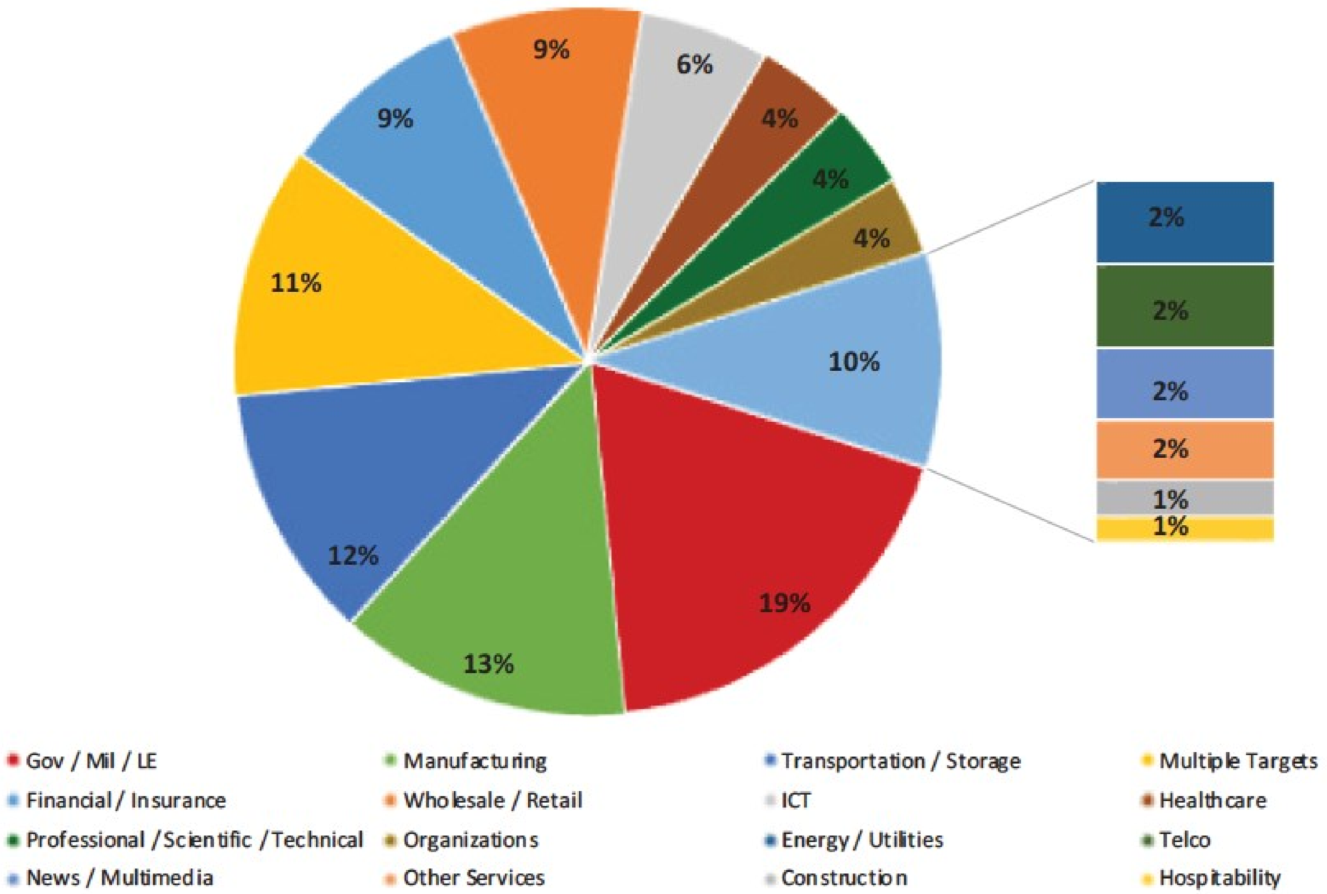
È progettata per non fare distinzioni tra input, ma per sviluppare una comprensione dei dati che gli vengono presentati e dare vita a qualcosa di nuovo (rischi di uso per deep fake)

Cybersecurity in Italia

Attacchi Informatici nel 2023		Crescita del numero di attacchi informatici nel 2023, rispetto al 2022		Crescita del numero di attacchi informatici nel 2019- 2023	
Globale: 100%	Italia: 11.2%	Globale: +12%	Italia: +65%	Globale: +67%	Italia: +738%

Attaccanti e Vittime per Cybersecurity in Italia





Limiti sulla Cybersecurity in Italia

Investimenti in cybersecurity in Italia nel 2023

- ***2.15 miliardi di € (0,12 % del PIL)***
- *Germania e Francia: circa il doppio*
- *USA: 0,3 % del PIL*

Tessuto imprenditoriale di PMI

- *Non sufficiente consapevolezza*
- *Mancanza di risorse economiche*
- *Assenza di personale qualificato*

Capitale umano insufficiente per la trasformazione digitale

Direttiva NIS2

Strategia comune di cybersecurity per tutti gli Stati EU

Si integra con altre normative (GDPR, DORA, Cyber Resilience Act)

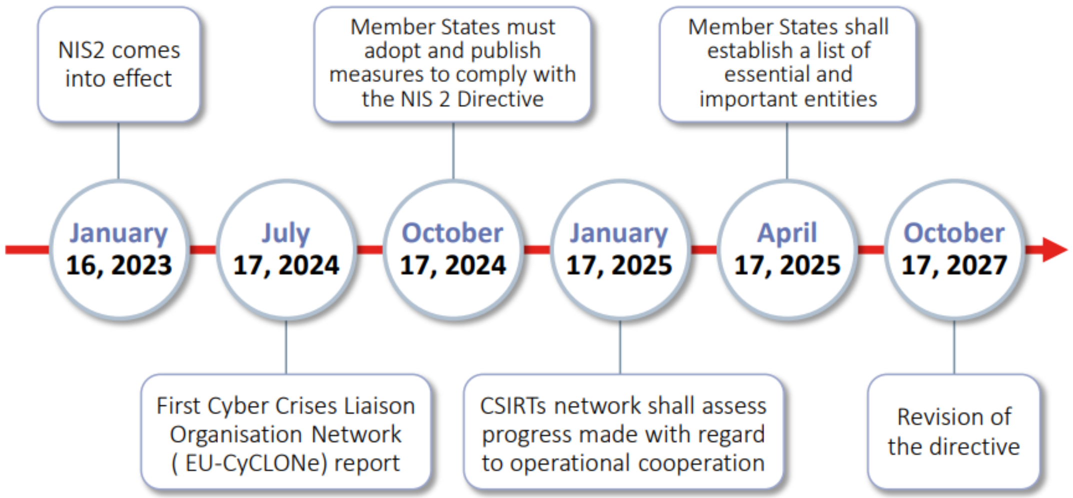
Nuove categorie di operatori, basate sulla criticità del servizio

Numero maggiore di settori e servizi critici (*piattaforme di cloud computing, data center e servizi sanitari*)

Requisiti per identificare, prevenire e rispondere alle minacce

Segnalazione tempestiva di incidenti significativi alle autorità competenti

Direttiva NIS2



- **17 Ottobre 2024**: Termine entro il quale la NIS2 dovrà essere recepita dalla normativa nazionale
- **Marzo 2025**: ACN definirà l'elenco dei soggetti che rientrano nella direttiva NIS2
- **Dicembre 2026**: Termine per implementare le misure di sicurezza previste da parte dei soggetti interessati

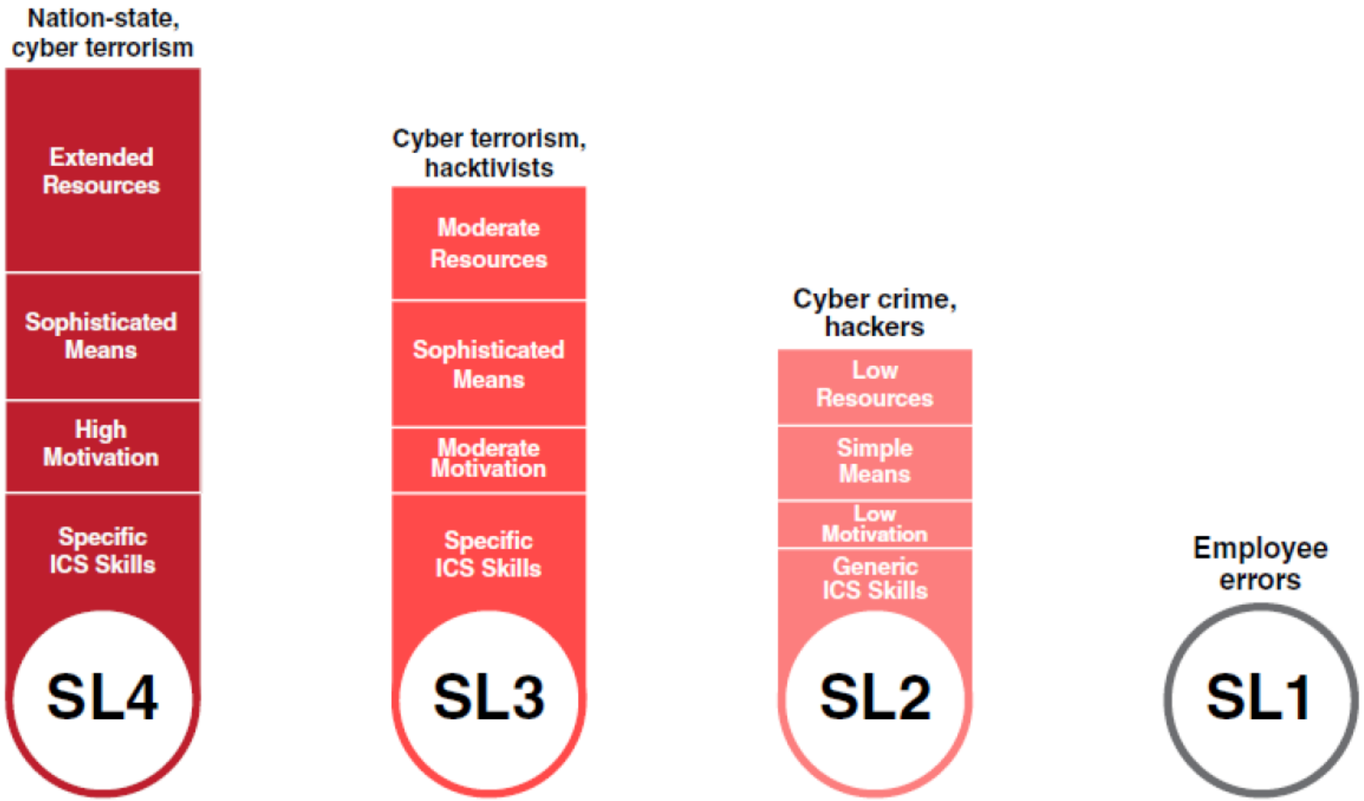
IEC 62443

General	Terminology, concepts, and models 62443-1-1	Terminology, concepts, and models 62443-1-2	Terminology, concepts, and models 62443-1-3	Terminology, concepts, and models 62443-1-4	
Policies & Procedures	Security program requirements for IACS asset owners 62443-2-1	IACS security program ratings 62443-2-2	IACS Patch management 62443-2-3	Security program requirements for IACS service providers 62443-2-4	Implementation guidance for IACS asset owners 62443-2-5
System	Technologies for IACS 62443-3-1	Risk assessments for system design 62443-3-2	System security requirements and security levels 62443-3-3		
Component	Product security development lifecycle requirements 62443-4-1	Technical security requirements for IACS components 62443-4-2	Application to Industrial Internet of Things (IIoT) 62443-4-3 (DRAFT)		

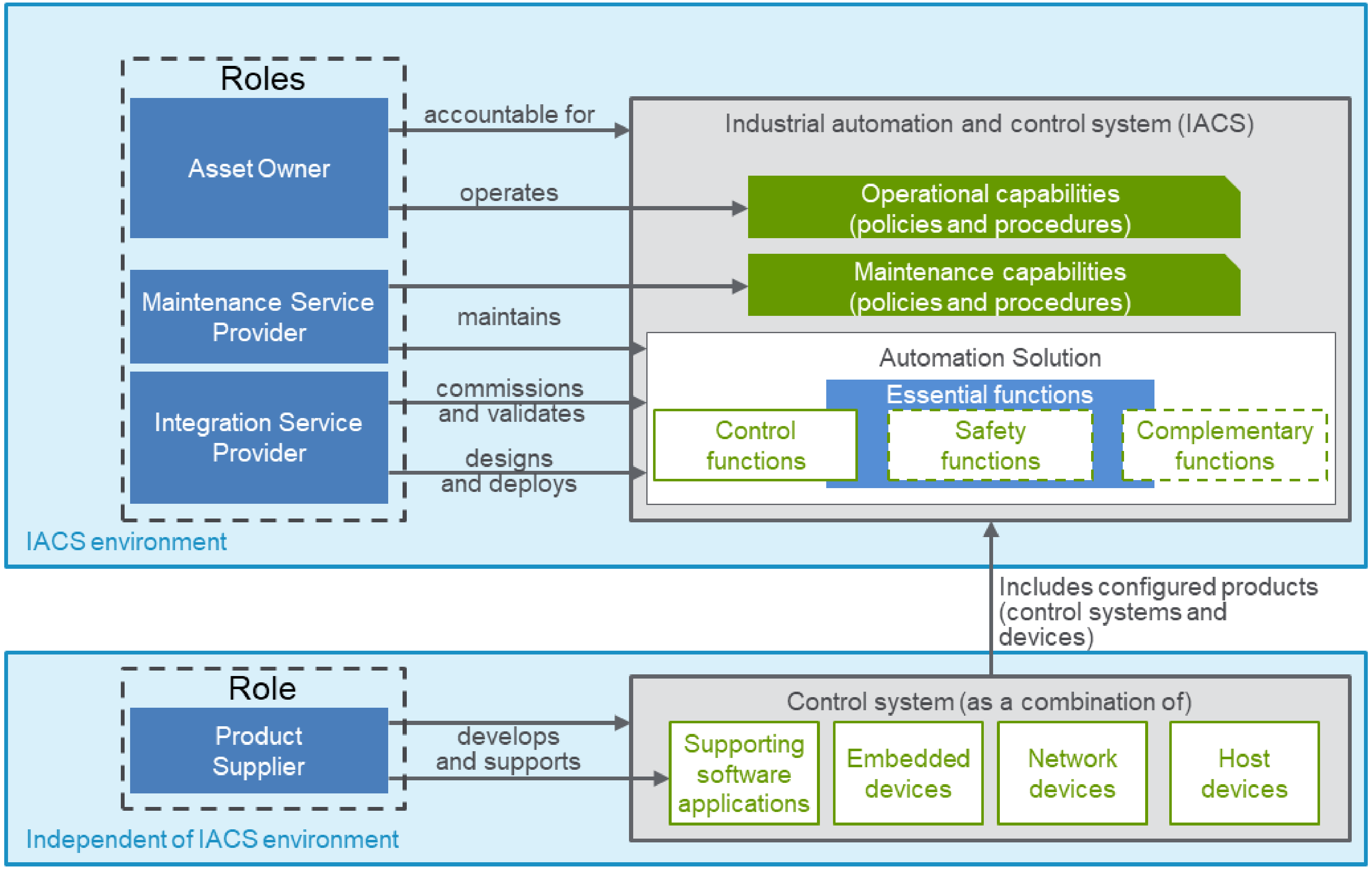
IEC 62443 – Maturity Level

Maturity Level	Description
Maturity Level 1	Initial: Product suppliers usually carry out product development ad hoc and often undocumented (or not fully documented).
Maturity Level 2	Managed: The product supplier is able to manage the development of a product according to written guidelines. To be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. The processes are repeatable.
Maturity Level 3	Defined (practiced): The process is repeatable throughout the supplier's organization. The processes have been practiced and there is evidence that this has been done.
Maturity Level 4	Improving: Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.

IEC 62443 – Security Levels



IEC 62443 – Industry roles

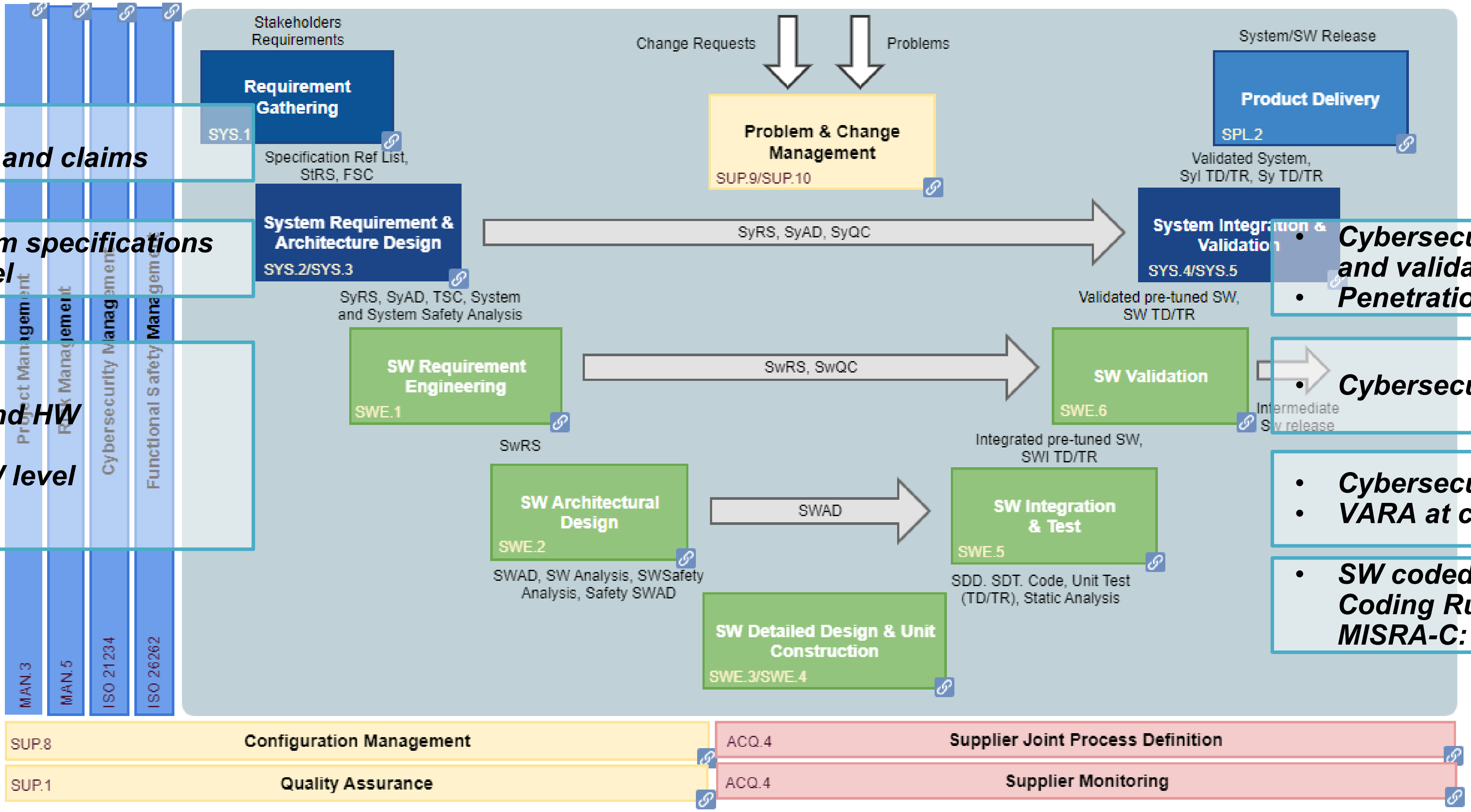


Cybersecurity activities within the development process

- ***TARA***
- ***Cybersecurity goals and claims***

- ***Cybersecurity system specifications***
- ***VARA at system level***

- ***Cybersecurity SW and HW specifications***
- ***VARA at SW and HW level***



- ***Cybersecurity system integration and validation***
- ***Penetration Tests***

- ***Cybersecurity SW and HW validation***

- ***Cybersecurity integration***
- ***VARA at code level***

- ***SW coded according to Secure Coding Rules following MISRA-C: 2012 + Amendment 1***

Cybersecurity impact on the organization

Cyber Threat Intelligence

Vulnerability Management

Preparation & Protection

Detection and analysis

Response

Post - incident Management

Asset	• Co-defined with OEM • Main deliverable is the set of vehicle assets to be protected
Accepted Risk	• Co-defined with OEM • Main deliverable is the accepted residual risk after the introduction of Cyber Security Solutions
Accepted Impact	• Co-defined with OEM • Main deliverable is the acceptable impact of the introduction of Cyber Security

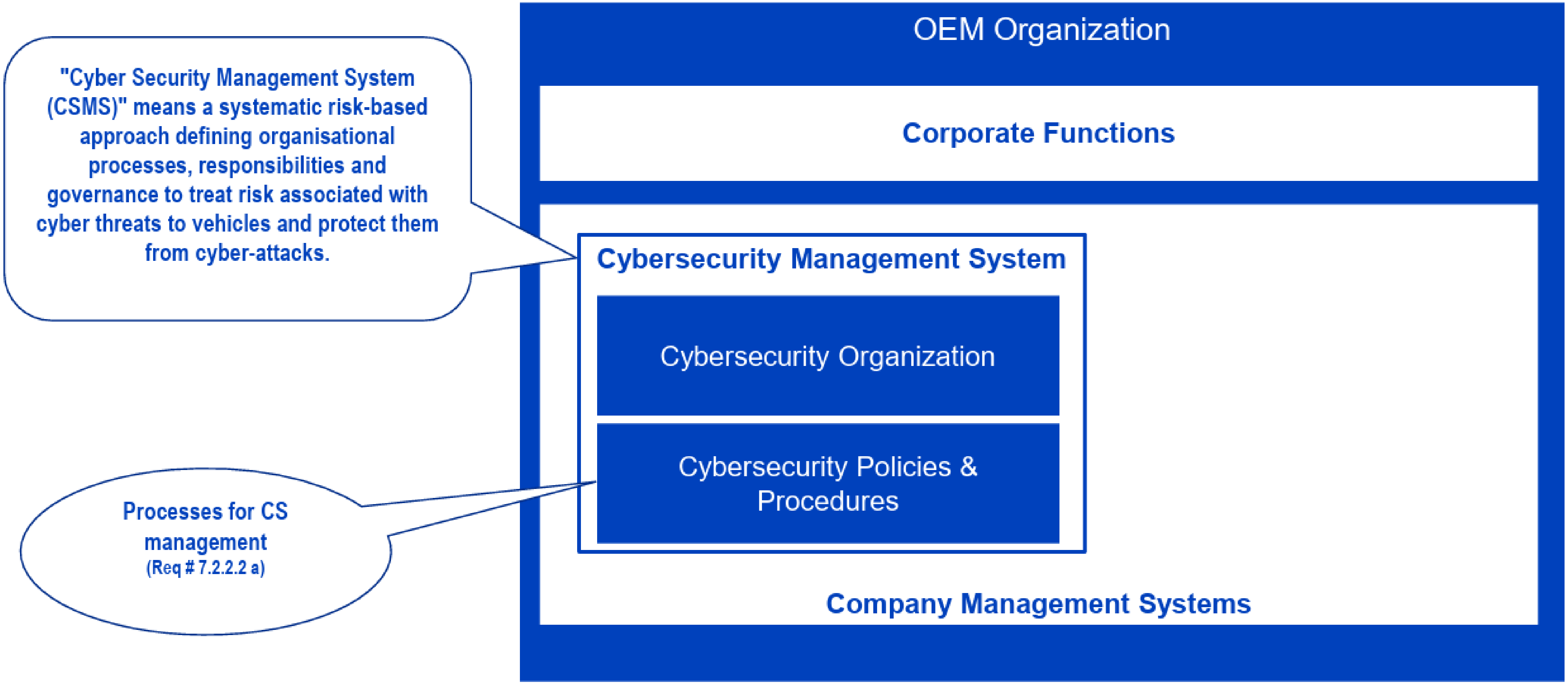
Cyber Security Solutions

Solution

COSTS

RESIDUAL RISKS

Cybersecurity impact on the organization



Trasformazione Digitale & Cybersecurity

Colmare il gap fra ricerca e impresa

CrossLab @ DII

Advanced Manufacturing

Additive Manufacturing   Augmented Reality

Industrial IoT   Cloud, BigData & Cybersecurity

CROSSLAB

artefici della trasformazione digitale

120 Docenti   100 Assegnisti   200 Dottorandi   4000 Studenti

CrossLab @ DII e Aziende

CROSSLAB
artefici della trasformazione digitale

Attrezzature
Know-how
Ricercatori
Tecnici

Processi
Prodotti
Competenze
Risorse Umane

Prototipo

Ingegnerizzazione

Domande?

Cybersecurity nella trasformazione digitale di imprese e impianti: IEC 62443 e aspetti applicativi

Sergio Saponara, sergio.saponara@unipi.it
Delegato Terza Missione del DII (Dipartimento Ingegneria dell'Informazione)
Presidente LT e LM in Ingegneria Elettronica
Università di Pisa