Connected Factories 2

CyberSecurity Expertise Sharing

SeCoIIA- CyberSecurity

Reda Yaich– IRT SystemX

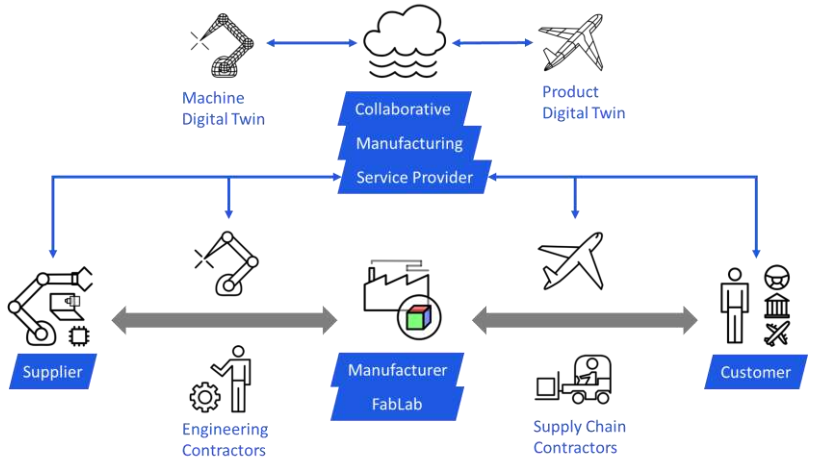
ConnectedFactories 2

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 873086)

SeCoIIA

Collaborative Manufacturing ecosystem

- **Title: SeCoIIA** (Secure Collaborative Intelligent Industrial Assets)
- **Mission:** Bringing a higher level of security and safety to manufacturing industries of transport sectors towards a more digitalized and collaborative production and manufacturing techniques.
- **EC Call heading:** ICT8-2019 - Security and resilience for collaborative manufacturing environments
- **Project duration:** 30 Months
- **Application sectors:**
  - Aerospace (Airbus)
  - Automotive (Continental)
  - Naval (Naval Group)
  - Collaborative Robots (Pal Robotics)



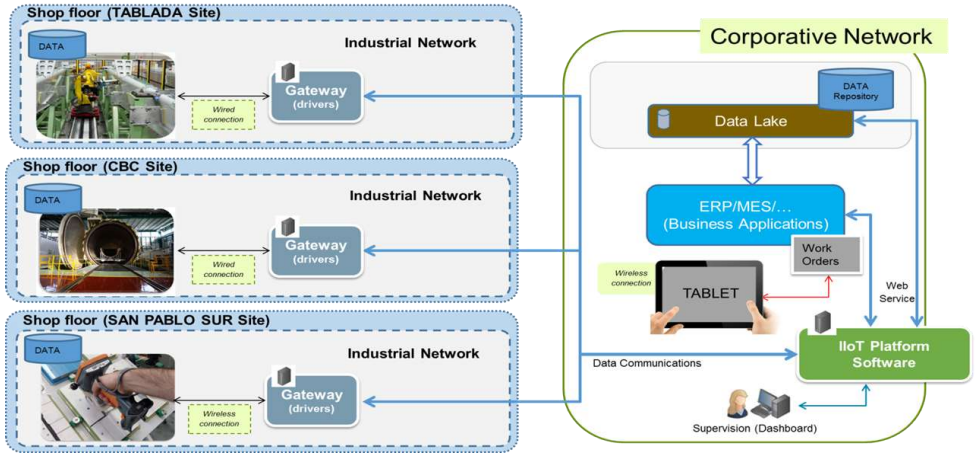
AIRBUS · Continental · NAVAL GROUP · isep · Fraunhofer AISEC · VTT · KU LEUVEN CiTiP · SystemX · SisTrade Software Consulting, S.A. · PAL ROBOTICS · FORESCOUT

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

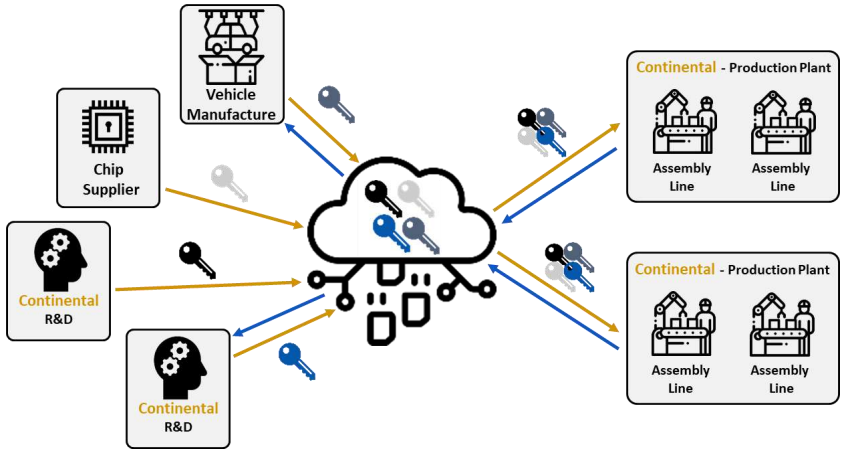
SeCoIIA

Challenging Pilots

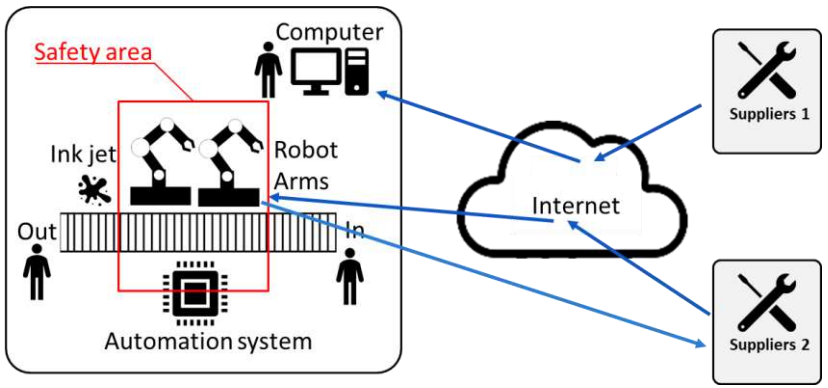
Aerospace



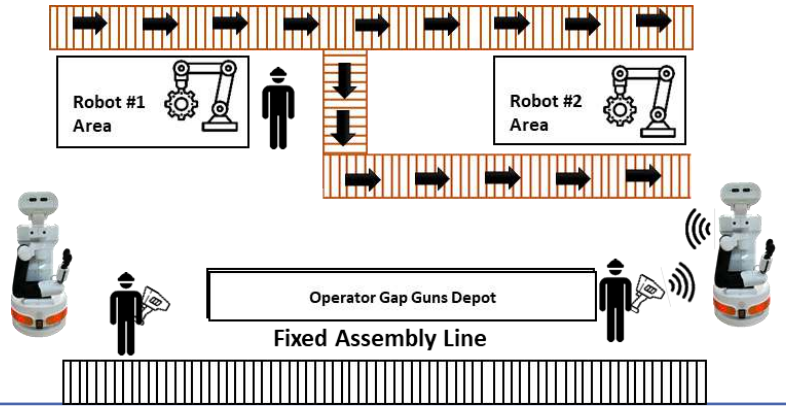
Automotive



Naval



Robotic



The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

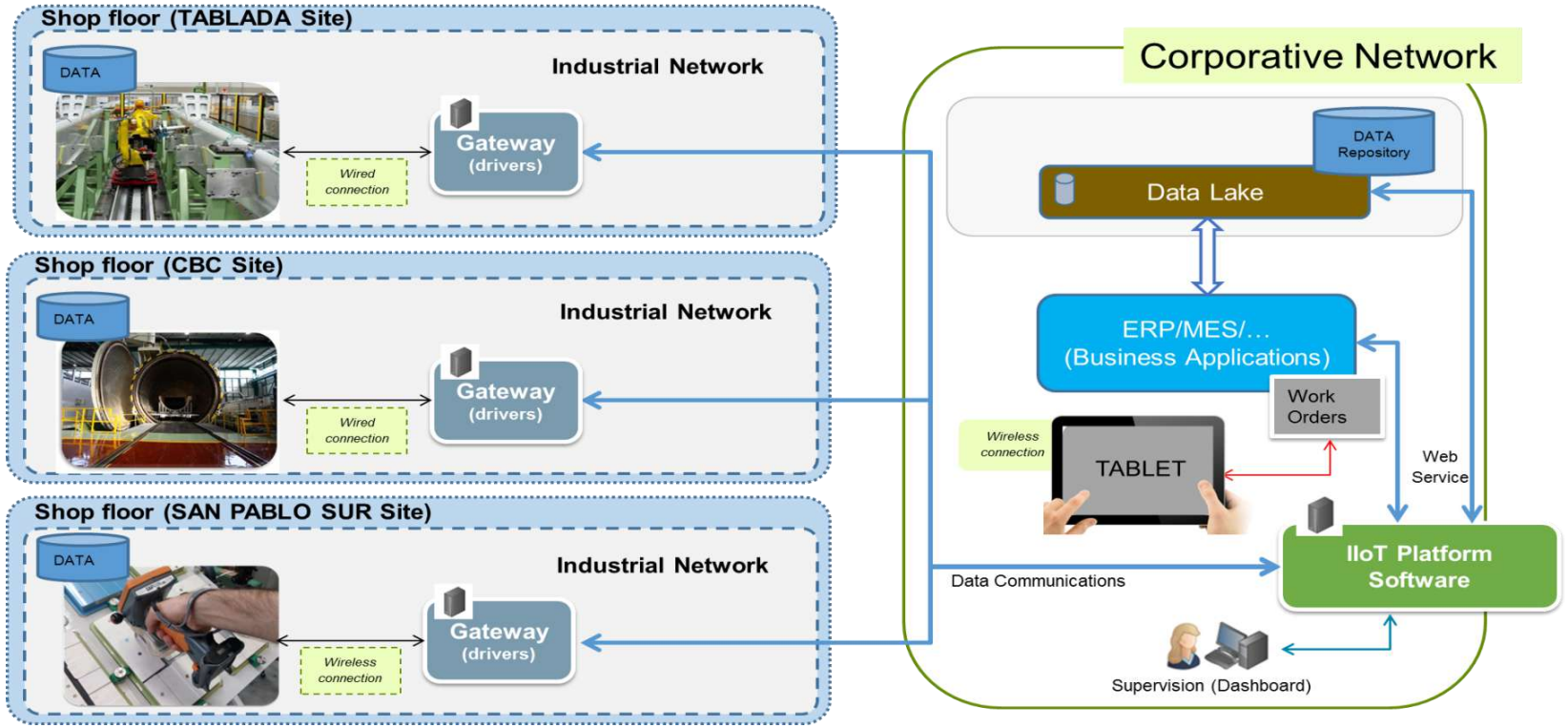
SeCoIIA

Aerospace Use-case

Aerospace

Secure Data Collection and Sharing across Manufacturing Factories

- Deployment of an Industrial IoT
  - Flexible management
  - Optimization of Manufacturing
- Analyse production data in near-real time
  - detect anomalies
  - raise meaningful alerts



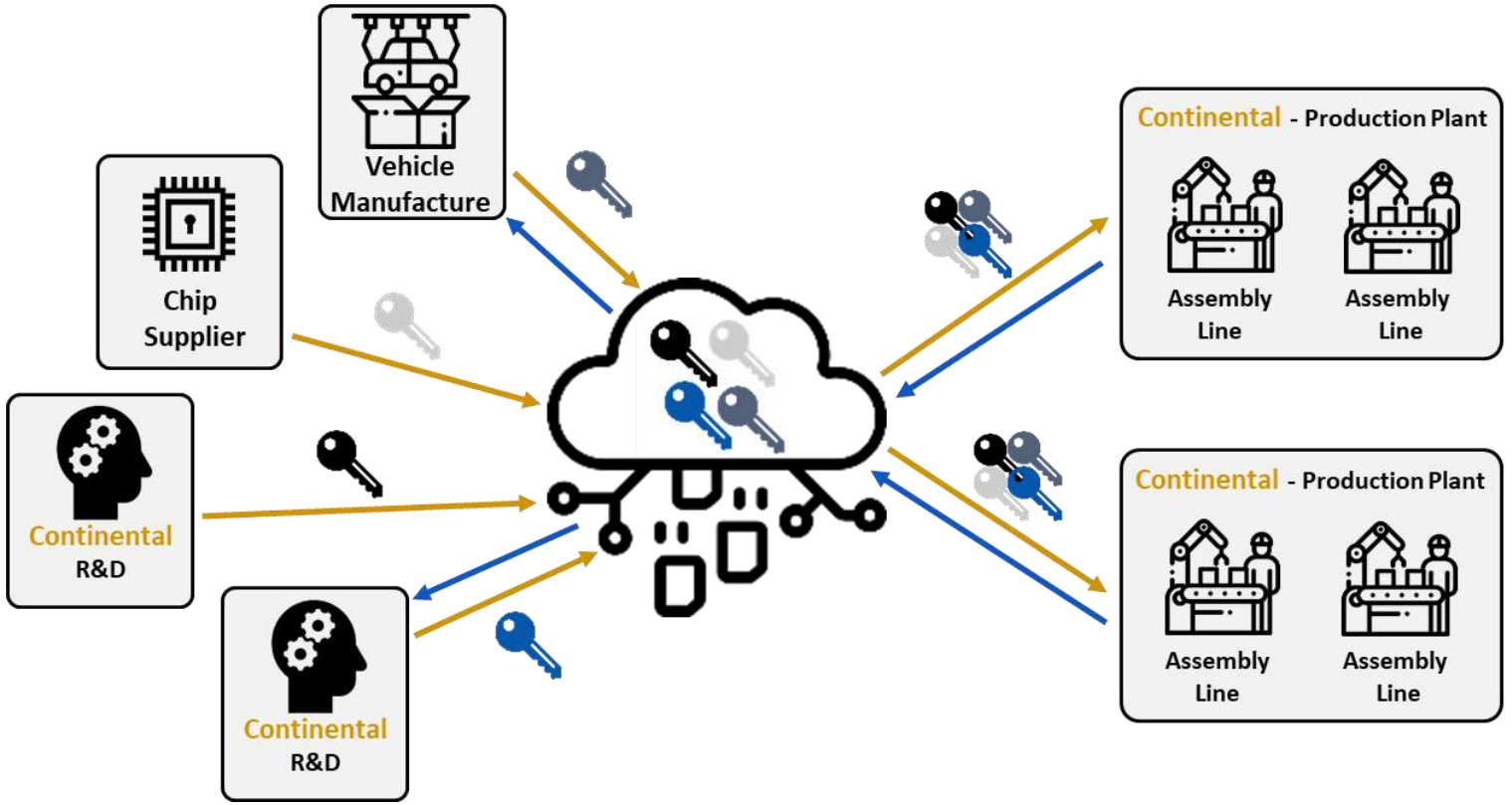
The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

Automotive Use-Case

Automotive

Multi-cloud environment for the sharing of product related security information

- Enable collaborative exchange of cryptographic materials across organizations
- Optimize productivity
- Enhance End2End security



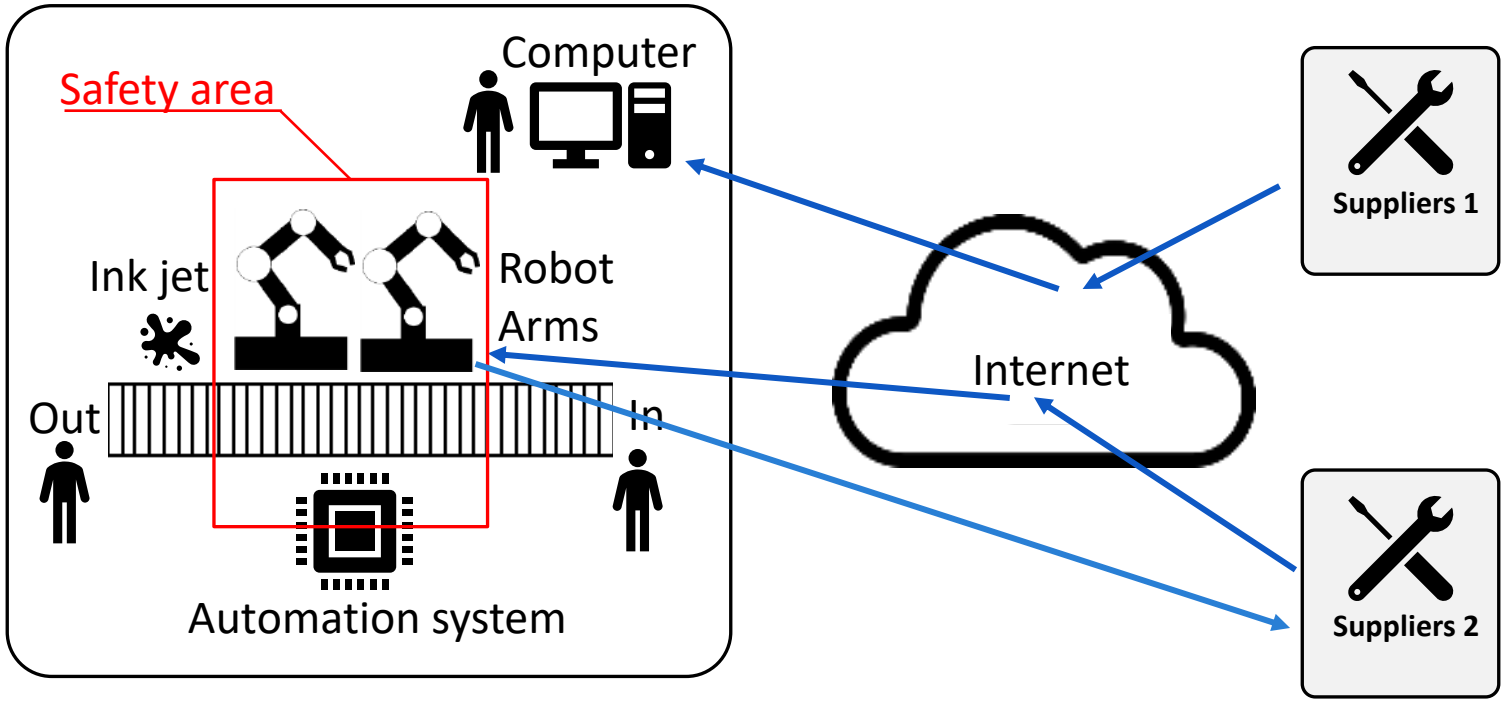
The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

Maritime Factories

Secure Remote Diagnosis and Maintenance of Critical Industrial Assets

Naval

- Decrease yearly maintenance cost
- Decrease production loss reduction
- Increase machine availability rate
- Guarantee the security of remote accesses for Diagnosis and Maintenance



The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

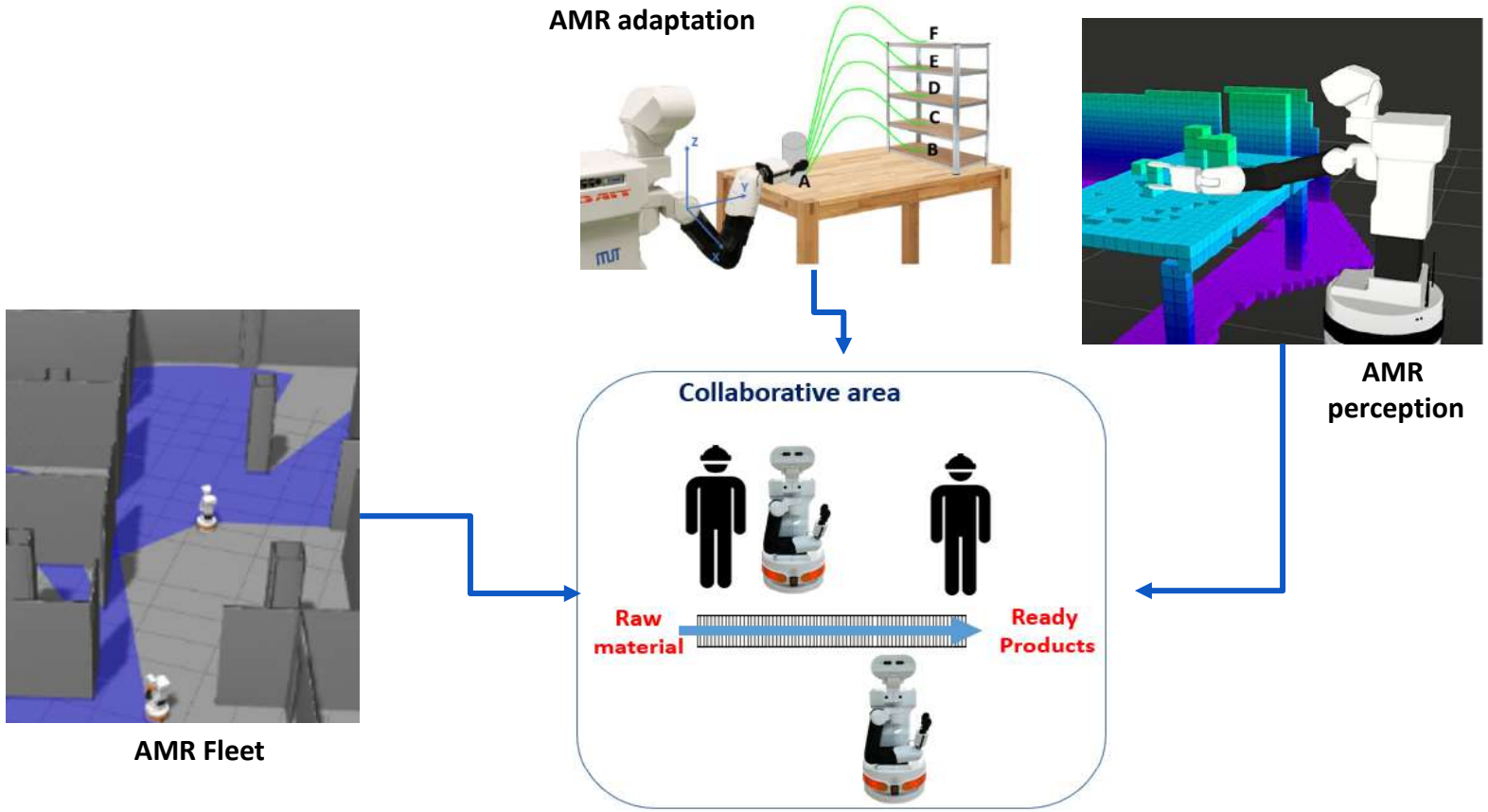
Cross-sectorial use case definition

Multi-robot human-machine collaboration in the shop floor

Robotic

Allow a safe and secure deployment of AMR

- Logistic automation
- Lone worker protection
- Learning by demonstration



The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

SeCoIIA

Project Key Capabilities

- **16 key capabilities to enforce security and Safety of FoF**
- **4 challenges dimensions:**
  - Human preparedness
  - Information security
  - Process safety
  - Social liability
- **4 collaboration levels:**
  - Organization to Organization (O2O)
  - Human to Human (H2H)
  - Machine to Human (M2H)
  - Machine to Machine (M2M)

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

H2020 SeCoIIA

Secure Collaborative Intelligent Industrial Assets

Cybersecurity workshop

Online - 20.01.2021

Feedback on Standardization activities

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

SeCoIIA

Our journey to standardization

Current State

- Screen relevant Standards

- Build a common understanding of standards ecosystem

280
Relevant Standards

Assessment

- Evaluate Alignment with Project Objectives

- Perform Gap analysis with respect to Pilots requirements

Target State

- Align project activities and development with current standards

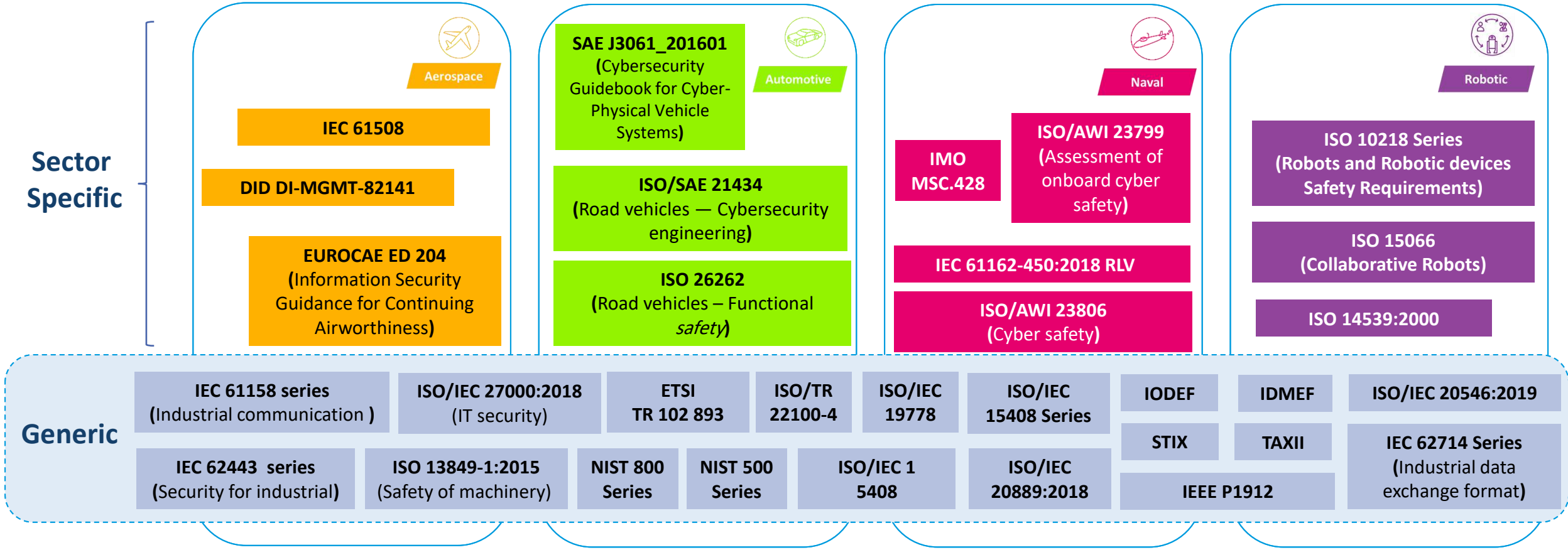
- Identify potential contributions to standardization activities

- Share Project results with Standardization Bodies

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

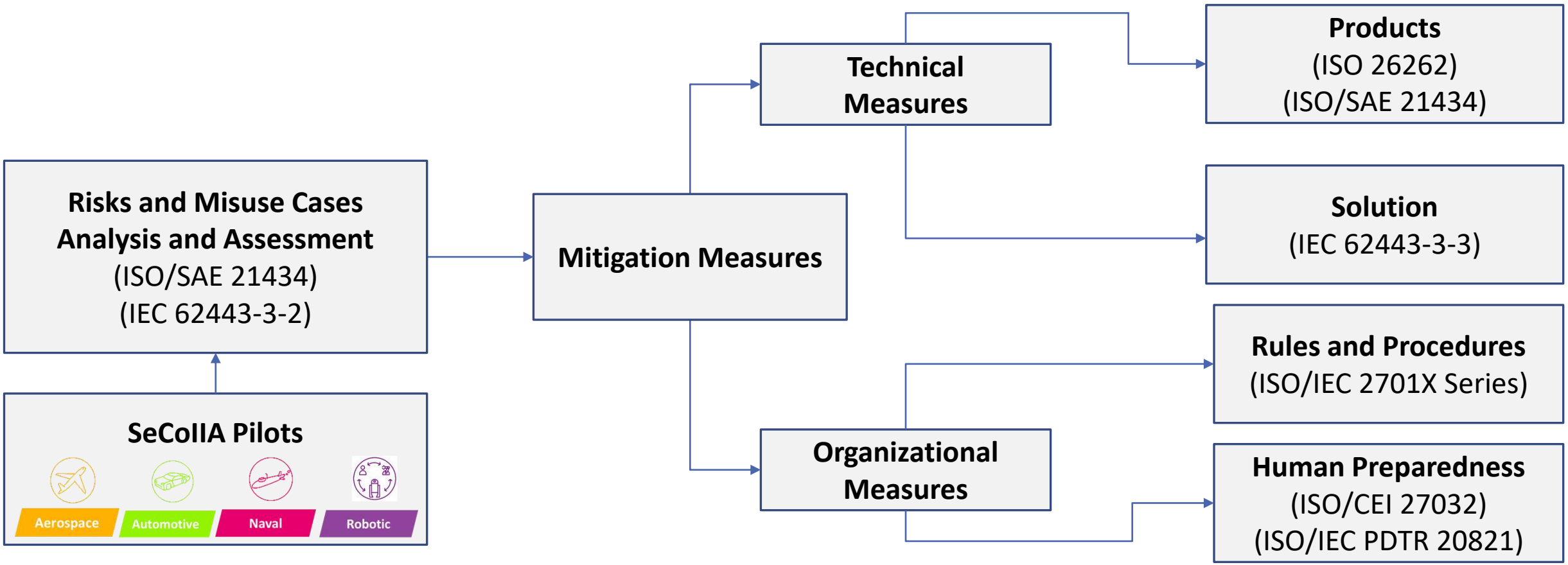
SeCoIIA

A rich and complex Standards Landscape

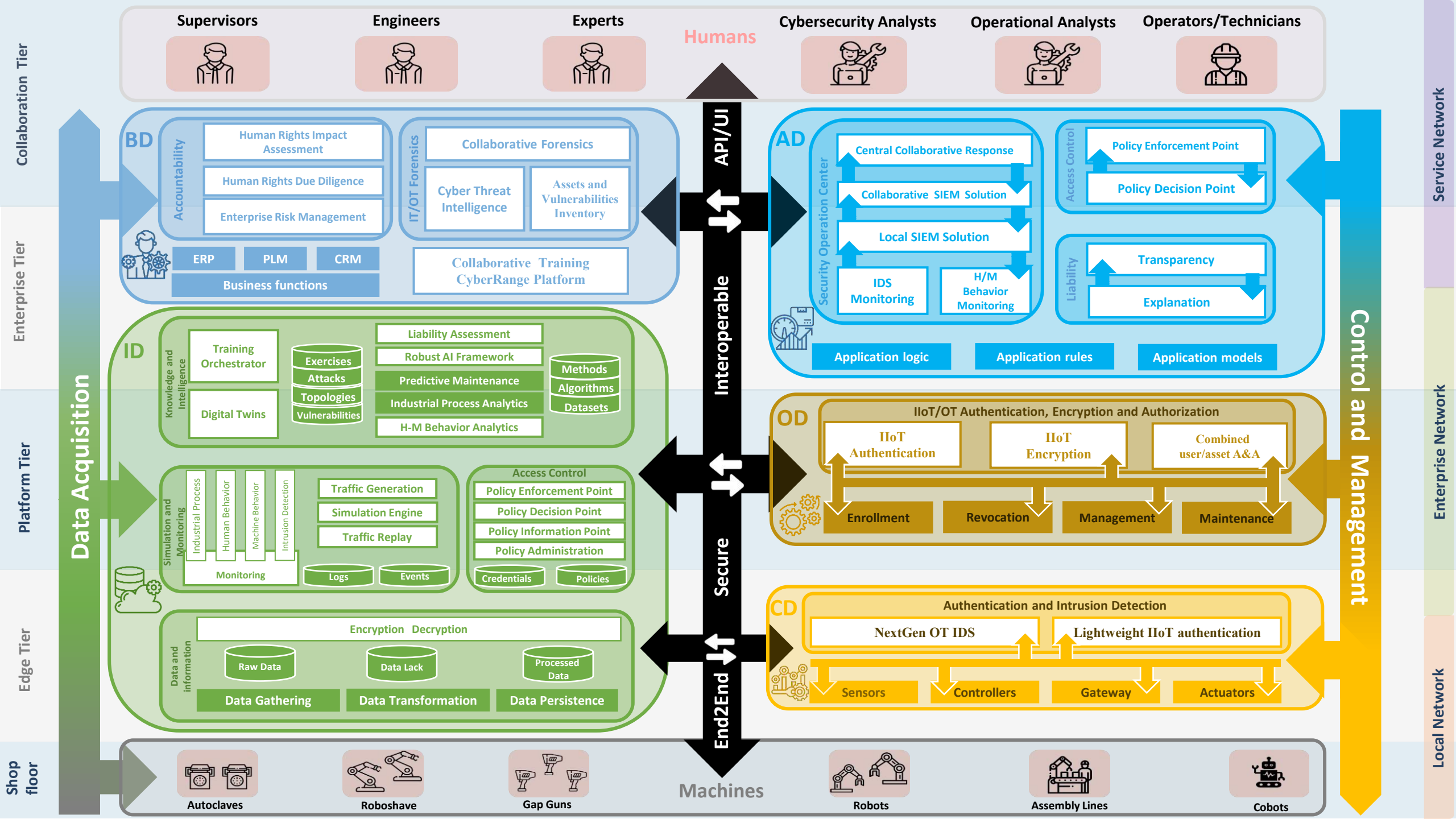


The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

Illustration:
Effective use of Standards in SeCoIIA



The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.


Collaboration Tier
Enterprise Tier
Platform Tier
Edge Tier
Shop floor
Service Network
Enterprise Network
Local Network
Humans
Supervisors
Engineers
Experts
Cybersecurity Analysts
Operational Analysts
Operators/Technicians
API/UI
Interoperable
Secure
End2End
Machines
Data Acquisition
Control and Management
BD
Accountability
Human Rights Impact Assessment
Human Rights Due Diligence
Enterprise Risk Management
IT/OT Forensics
Collaborative Forensics
Cyber Threat Intelligence
Assets and Vulnerabilities Inventory
ERP
PLM
CRM
Business functions
Collaborative Training CyberRange Platform
AD
Security Operation Center
Central Collaborative Response
Collaborative SIEM Solution
Local SIEM Solution
IDS Monitoring
H/M Behavior Monitoring
Access Control
Policy Enforcement Point
Policy Decision Point
Liability
Transparency
Explanation
Application logic
Application rules
Application models
ID
Knowledge and Intelligence
Training Orchestrator
Digital Twins
Exercises
Attacks
Topologies
Vulnerabilities
Liability Assessment
Robust AI Framework
Predictive Maintenance
Industrial Process Analytics
H-M Behavior Analytics
Methods
Algorithms
Datasets
Simulation and Monitoring
Industrial Process
Human Behavior
Machine Behavior
Intrusion Detection
Monitoring
Traffic Generation
Simulation Engine
Traffic Replay
Logs
Events
Access Control
Policy Enforcement Point
Policy Decision Point
Policy Information Point
Policy Administration
Credentials
Policies
Data and information
Encryption Decryption
Raw Data
Data Lack
Processed Data
Data Gathering
Data Transformation
Data Persistence
OD
IIoT/OT Authentication, Encryption and Authorization
IIoT Authentication
IIoT Encryption
Combined user/asset A&A
Enrollment
Revocation
Management
Maintenance
CD
Authentication and Intrusion Detection
NextGen OT IDS
Lightweight IIoT authentication
Sensors
Controllers
Gateway
Actuators
Autoclaves
Roboshave
Gap Guns
Robots
Assembly Lines
Cobots

SeCoIIA

Findings and lessons learnt

DRIVERS

- Rich and complete standards landscape
- High overlap between standards which provides a consensual protection level
- Constant evolution of existing standards

GAPS

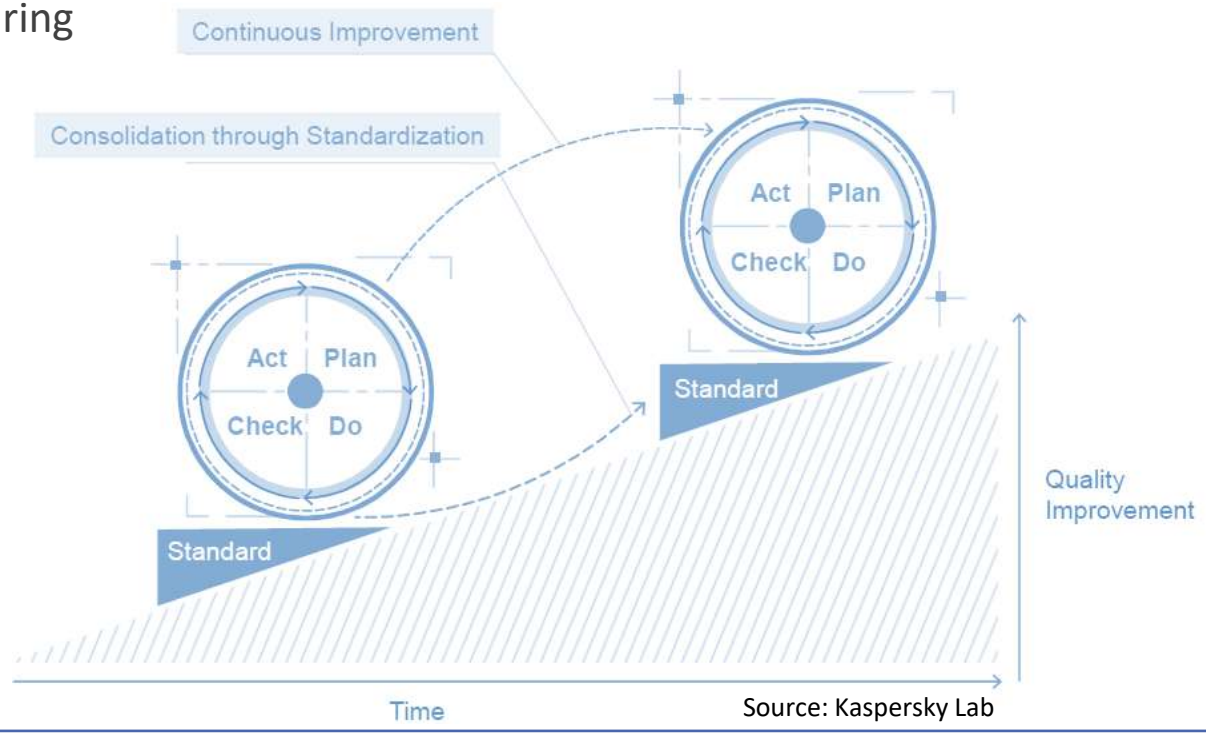
- Limited Interoperability
  - Focus: Technical and Semantic
- AI based (Zero-Touch) Manufacturing
  - Trustworthiness
  - Explanation
  - Certification
- Ethical and Legal dimensions are challenging
  - e.g. Collaborative Robotics
  - Accountability and due diligence
  - Collaborative forensics

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

SeCoIIA potential contribution to standardization activities

Ongoing identification of potential contribution

- Reference Architecture for Secure Smart Collaborative Manufacturing
- Industrial Cybersecurity Training & Simulation
- Secure Cloud and Edge Manufacturing Backbone
- Collaborative security operations center
- Human rights and/or accountability Modelling
- Operational technology forensics
- Security guidelines for human-robot collaboration capacity
- Baseline security requirements for IIoT capacity
- Trustworthy AI
  - ISO/IEC NP TR 24028 - trustworthiness in Artificial Intelligence
- …



Source: Kaspersky Lab

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

SeCoIIA

Concluding remarks

- Build a common understanding of standards ecosystem
  - Approaches, Concept, Challenges, Activities
- Accelerate and widen the adoption of cybersecurity standards in digital manufacturing
  - Align SeCoIIA project activities and developments with current standards
- Transfer relevant project results into standardization activities.
  - Ongoing identification of potential contributions.
  - Pave the way to new standards
    - Human rights, Accountability, Forensics, Artificial Intelligence, Cyber Training, etc.

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

Thank you!
Https://secoiia.eu

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nr. 871967.

CF Standards Analysis (see excel to complete)

Connected Factories 2 CS & Privacy Standardization & Industry Standards															
CS Standard Analysis															
		DT-ICT-07-2018-2019							DT-ICT-08-2018-2019		ECSEL		DT-ICT-02-2018-2019		
		CF2	Kyklos 4	DigiPrime	Qu4lity	EFPF	SHOP4CF	ZDMP	SeCoIIA	COLLABS	Industry4.E	Productive4.0	DIH2	TRINITY	
IEC62443		X				X		X	X	X					
NIST		X				X		X	X	X					
	NIST SP800-82	X				X									
	NIST CSF	X				X									
NISTIR8183	CS for Manufacturing	X													
NISTIR 8259	CS for IoT Device Manufacturers	X													
CSA CAIQ		X													
CSA GDPR COC		X													
CSA ICS		X													
ISO13849						X									
ISO27	27000:2018	X				X									
	JTC1/SC27	X				X									
	27017:2015	X				X									
ISO33052:2016	PRM					X									
CIS-ICS		X													
ETSI IoT		X													
ETSI TS103 457	Trusted Cross-Domain					X									
CISA		X													
NIS		X							X	X					
STRIDE		X													
CVE		X							X	X					
ATT&CK		X							X						
Industrie4.0		X													
GDPR		X							X						
SBOM		X													
RIM		X													
ENISA	IS & P standards for SME	X				X									
	Procure Secure	X				X									
OPC	IEC/TR 62541-2:2016	X				X									
ISO/TC 262															
TLS		X													
HTTPS		X													
IDSA		X		X											

Adding :

+ ID&AM : ISO 24760, UMA, XACML, SAML 2, OpenID,…
+ Identity Assurance : NIST 800-63
+ AAA : OAUTH, …

+ DIN27070 : security gateway for exchange of industry data

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 873086)

CF Impact Analysis

Connected Factories 2														
CS Impact Analysis														
	DT-ICT-07-2018-2019						DT-ICT-08-2018-2019		ECSEL	DT-ICT-02-2018-2019				
	CF2	Kyklos 4	DigiPrime	Qu4lity	EFPF	SHOP4CF	ZDMP	SeCoIIA	COLLABS	Industry4.E	Productive4.0	DIH2	TRINITY	RIMA
OT	X	X	X		X		X				X		X	
ICT	X	X	X	X	X		X				X		X	
Digital Platforms	X	X	X	X	X						X		X	
Data Platform	X	X	X	X	X		X						X	
System Integration			X	X	X		X						X	
Software Development			X	X	X		X				X		X	
Systems	X		X	X			X				X		X	
Connectivity	X		X	X			X	X					X	
ICS Systems	X		X					X					X	
PLC			X				X	X						
OPC/UA					X						X		X	
IIoT	X							X					X	
IoT					X								X	
Public Cloud	X			X			X							
Hybrid Cloud	X													
Private Cloud	X													
Edge				X										
Smart Sensors		X									X		X	
Smart Product	X													
Robotics	X							X			X	X	X	X
API	X				X									
Additive / 3D		X												
AI	X			X			X	X						
ML	X							X						
BA	X													
Incident Mgt	X													
Vulnerability Assessment	X													
Monitoring	X													
Digital Twin	X			X										
AR/VR														
5G	X			X										
Time Series							X							
DCS							X							
MES							X							
PLC							X							
ERP														

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 873086)

Identifying cross project collaboration

Key Security developments of our Digital PlatformRobust	Willing to Share – Use other experiences of Digital Platforms (Y/N)	Willing to Share – Use other experiences of Security Practitioners (Y/N)
Access management		
Privileged access management (admin)		
Identity management		
Authentication – Authorization	Yes	
White Listing		
Root Access		
Security management principles		
Control measures		
Audit capabilities	Yes	
Reporting	Yes	
Incident Management	Yes	
Event Monitoring – Incident Monitoring - Reporting	Yes	
Encryption		
Key Management		
Privacy Enhancing Technologies		
Denial of Service		
Patch Management		
Over the Air Updates		
Embedded Security		
Integration		
Firewalling - Proxying		
Cloud Security Mechanisms : please specify		
Isolation		
Virtualization		
End to End Security		
TTP (Trusted Third Party) : please specify		
DRM (Digital Rights Management)		
Robust AI based Security Solutions	Yes	
Other 2 : please specify		

Supported by the European Commission through the Factories of the Future PPP (Grant Agreement Number 873086)