CyberFactory#1: How to make the factory of the future efficient and secure

- Virtual Panel, Dec 9th 2020

CyberFactory#1: How to make the factory of the future efficient and secure

Adrien Bécue

Head of Innovation, Airbus CyberSecurity, France
Project Leader CyberFactory#1

İrem Hilavin

SW Design Architect, Vestel, Turkey
Work Package Leader Integration & Validation

Jari Partanen

Head of Quality, Environment and Technology Management, Bittium, Finland
Task Leader CyberResilience

Moderator: Tim Stuchtey,

Director at BIGS Potsdam

- The recording of the panel is available here:

https://attendee.gotowebinar.com/recording/1895911401043193858

Industrial cyber-risk - Today

31 May 2016 - Cyberattack on a German steel-mill Factory
Attack reports by BSI and SANS Institute

Attacker profile
-State sponsored
-Skilled in IT
-Skilled in ICS
-Aiming at physical damage

Attack story
-Spear phishing
-Credentials theft
-Hack into office network
-Infect Production mgmt SW
-Access industrial Ntwk
-Control Blast furnace
-Destroy HMIs
-Prevent safety shut down

Damages
-Plant damaged by molten metal heated to thousands °
-Production loss
-Reputational damage

Survey: www.menti.com Code: 35 64 55 0

Industrial cyber-risk – Tomorrow ?

Unmanned offshore station causes oil spill!
Valve control software compromised by malware…

Autonomous robot kills a worker!
Adversarial machine learning suspected…

Military secret stolen in weapon factory!
Rogue device placed by contractor leaked rocket warhead design data
…

Survey: www.menti.com Code: 35 64 55 0

Key enabling technologies

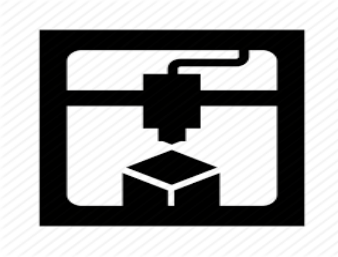
Cloud/edge technology
Big data

Artificial Intelligence
Machine-Learning

Virtual / Augm. reality
Simulation & modelling

Collaborative Robotics
Augmented Human

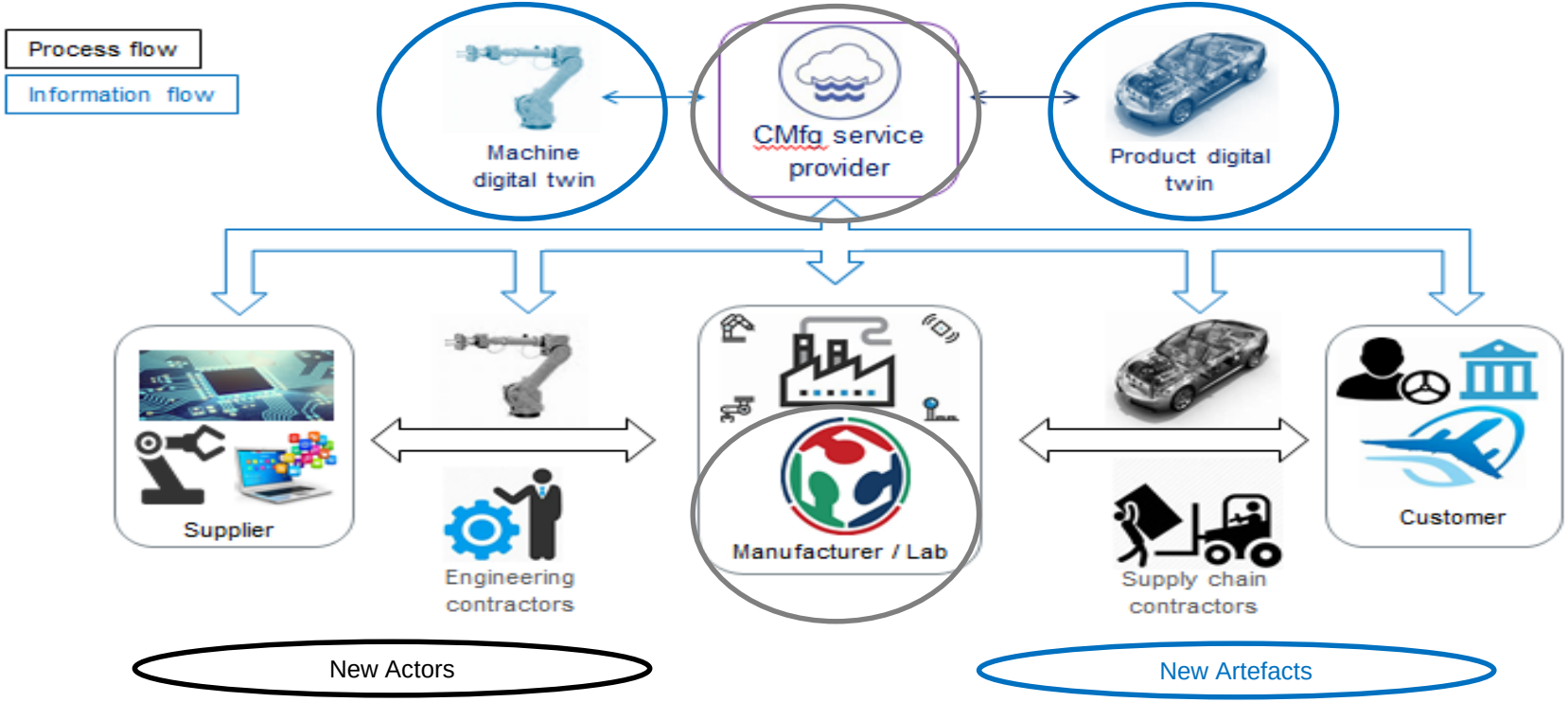
M2M Communication
IIoT & Self* networks



Additive Manuf.
3D printing

Survey: www.menti.com Code: 35 64 55 0

New actors and artefacts

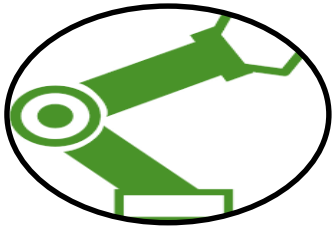


Survey: www.menti.com Code: 35 64 55 0

Project value chain

Users

- U1- Transportation systems
- U2- Textile industry
- U3- Consumer Electronics
- U4- Machine fabrication



Suppliers

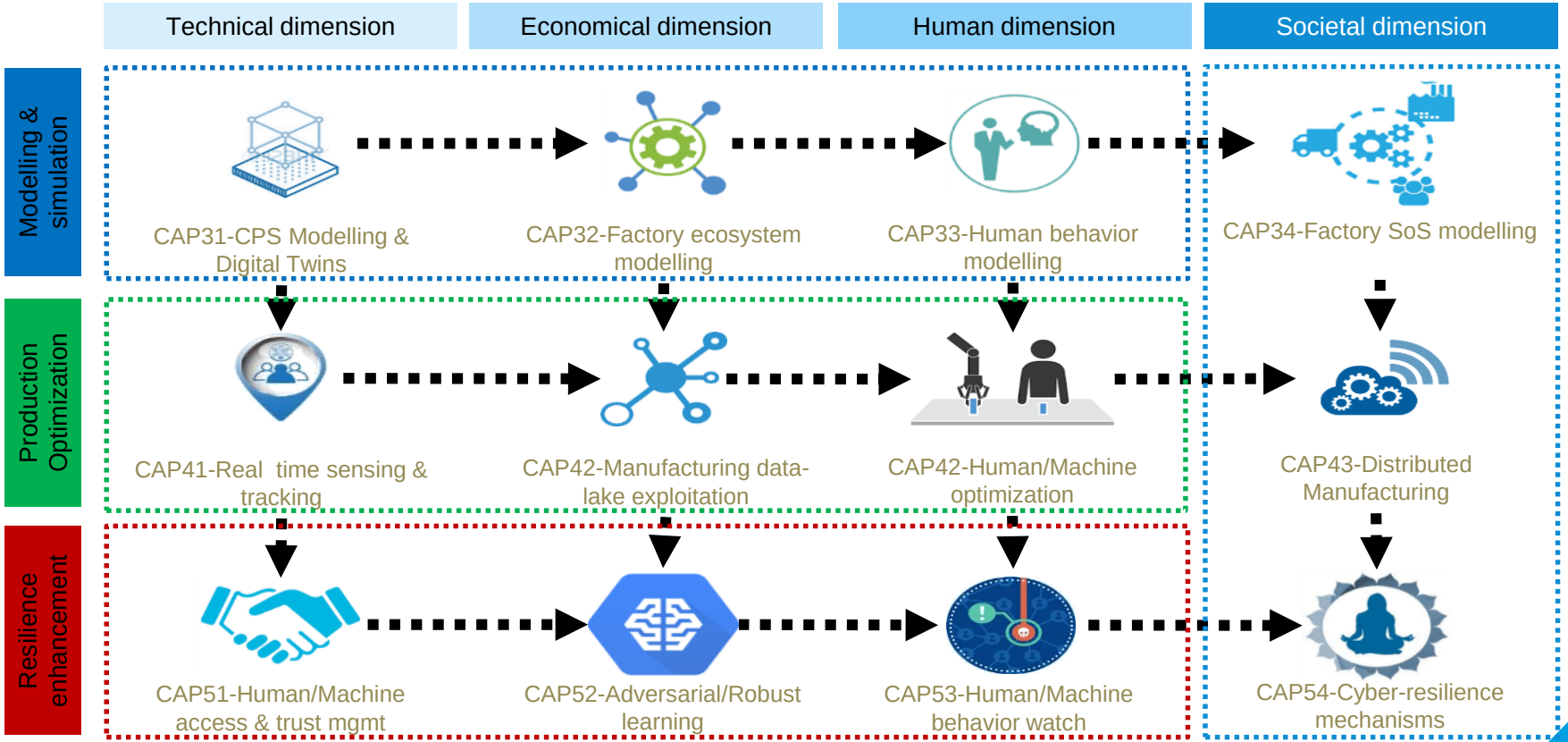
- S1- Robotics & Automation
- S2- IIoT & M2M Communication
- S3- SCADA, ERP & Supply Chain Mgmt
- S4- Security & Safety

Researchers

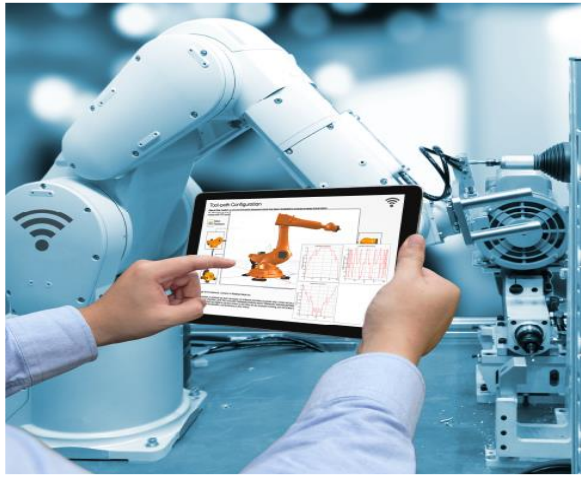
- R1- Cyber-physical system engineering
- R2- Data science & artificial intelligence
- R3- Economics & Social Sciences
- R4- Virtualization, Modelling & Simulation

Survey: www.menti.com Code: 35 64 55 0

Project key capabilities



Exploitation perspectives



Digital Twin Market
-USD 3.8 Billion in 2019
-USD 35 Billion by 2025
-CAGR of 37.8 %

Industry 4.0 Market
-USD 66.67 Billion in 2016
-USD 152.31 Billion by 2022
-CAGR of 14.72%

ICS Security Market
-USD 10.24 Billion in 2017
-USD 13.88 Billion by 2022
-CAGR of 6.3 %

Survey: www.menti.com Code: 35 64 55 0

Towards the Factory of the Future

CYBER FACTORY NO.1 CF#1

VESTEL 1.0
1994-1998

Vertical Integration

Implementation
- Plastic Injection
- PCBA
- Metal Pres
- LGP/DP

Methodology
- Quality Excellence
- CKD to CBU

VESTEL 2.0
1998-2003

Process Integration

Implementation
- PCBA Integrated Line
- Cefla Painting Line
- Metal Press Line
- Cell in TV out Assembly Line

Methodology
- Total Productive Maintenance

VESTEL 3.0
2003-2014

Automation Integration

Implementation
- Robotic Assembly
- Warehouse Automation
- AGV
- Test Automation

Methodology
- Supply Chain Management

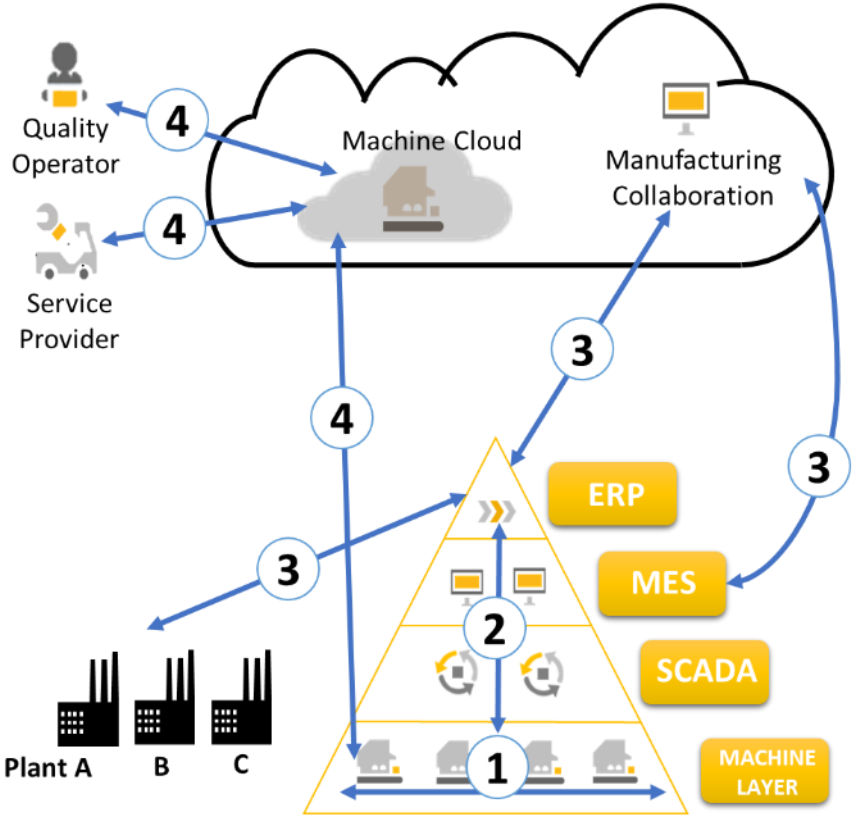
VESTEL 4.0
2014 - …

‘’Smart’’ Integration

Implementation
- Industrial Internet
- M2M Connectivity
- M2ERP Connectivity
- Cyber Physical Systems
- Artificial Intelligence

Methodology
- Industry 4.0

Towards the Factory of the Future



1. Machine to Machine
- Visibility
- Monitoring
- Optimization
- Kanban / Direct replenishment

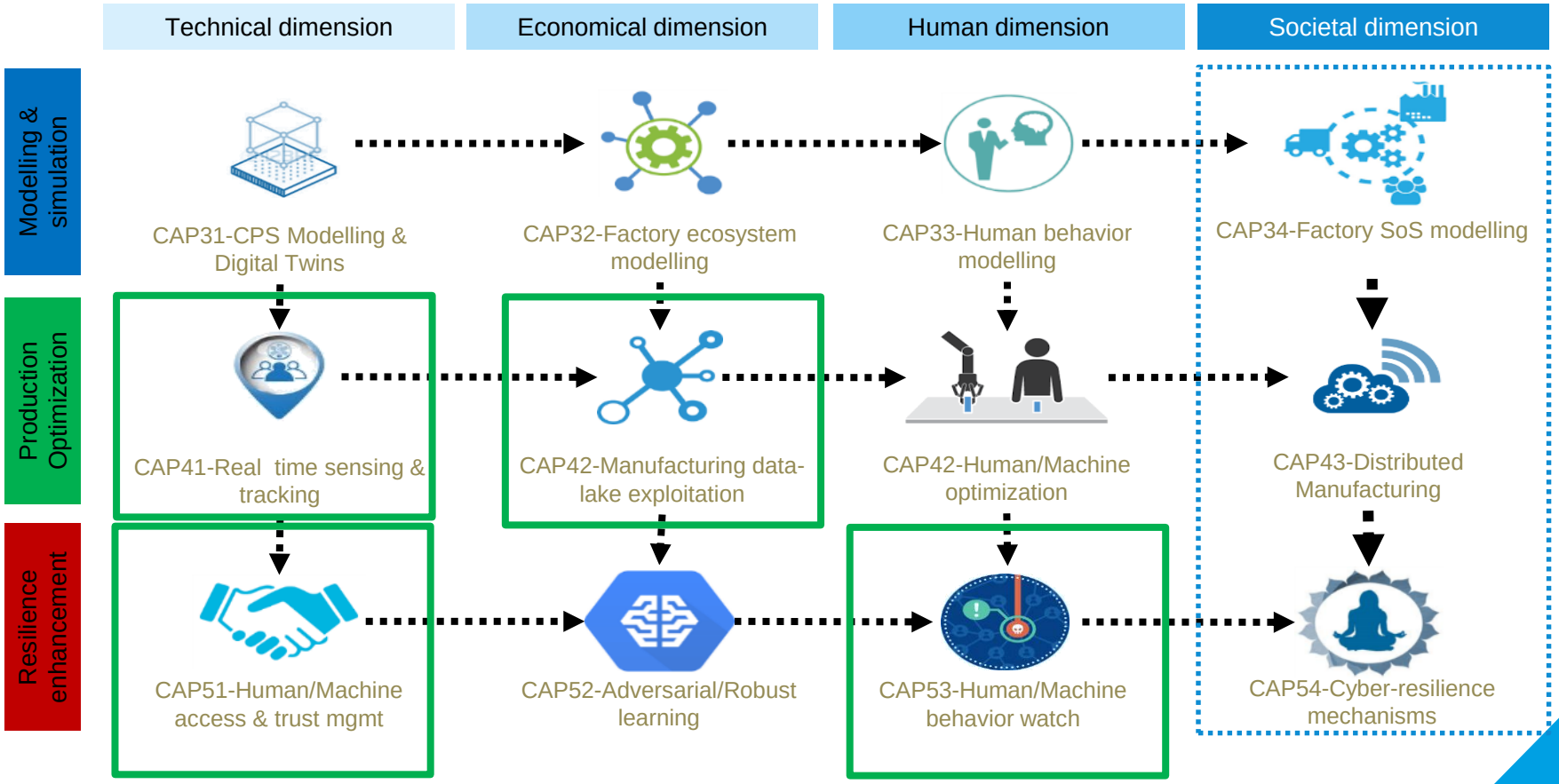
2. Machine to ERP
- Intra company vertical integration

3. Manufacturing Collaboration
- Supply chain horizontal integration

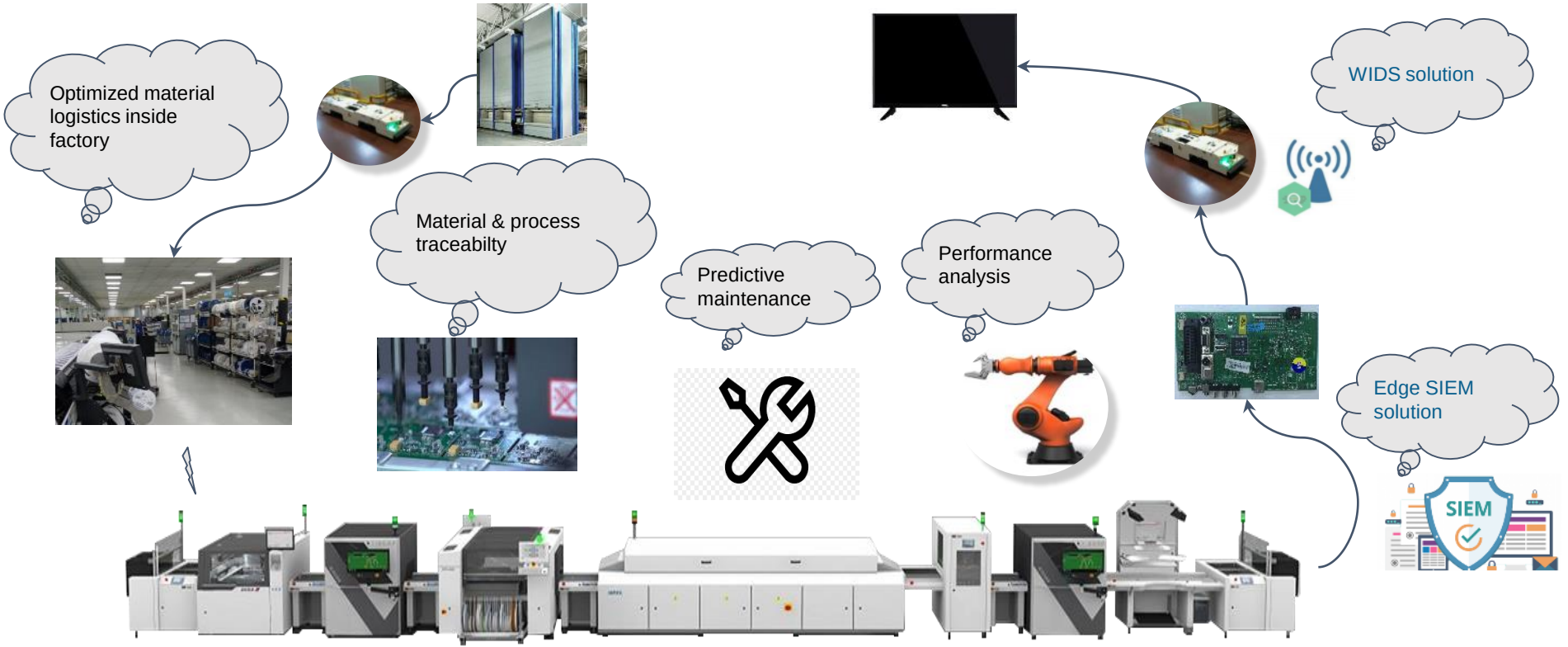
4. Machine Cloud
- Predictive maintenance
- Predictive quality

Survey: www.menti.com Code: 35 64 55 0

Key Capabilities Developed



Usecase Overview



Survey: www.menti.com Code: 35 64 55 0

CyberFactory#1 general objectives related to cyber-resilience

Manage access rights dynamically for humans and machines

Continuously watch for anomalies on factory assets regardless of their origin

INPUT
- **SotA,**
- **use cases,**
- **requirements**
- **etc.**

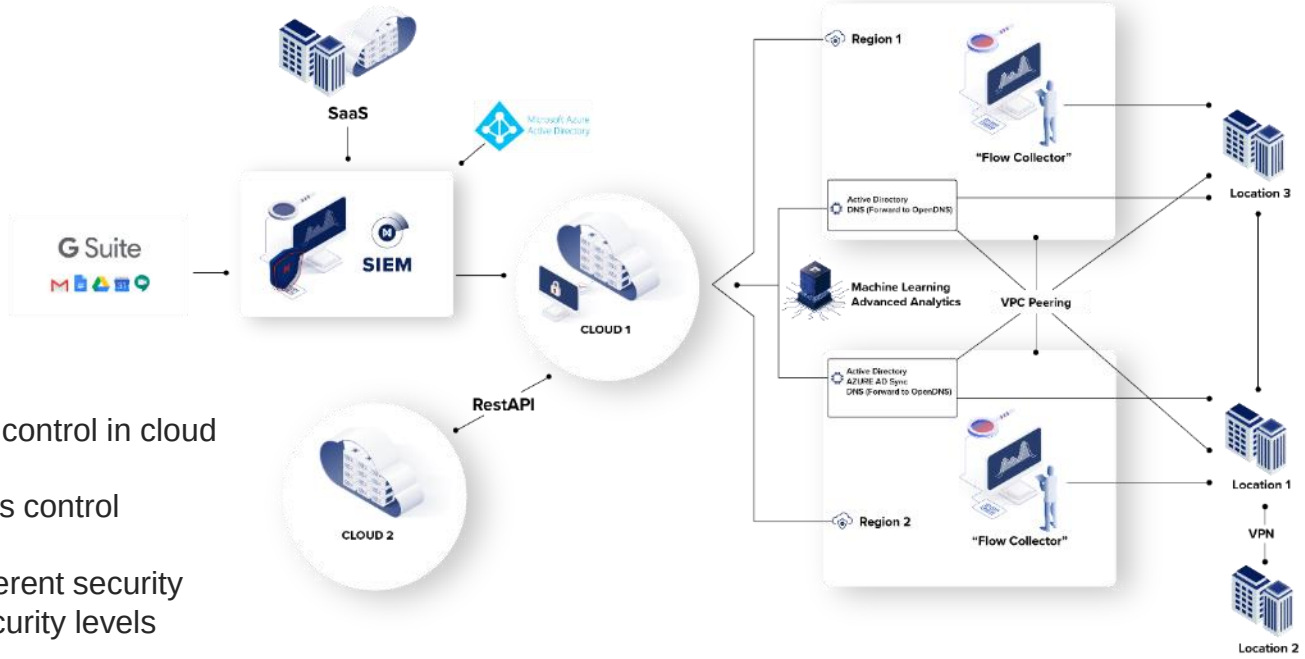
OUTPUT
- **Demonstrators**
- PoC

Prevent manipulation of manufacturing and product-embedded AI

Enable decision-aided or autonomous R&R of factory assets

Human/Machine access & trust management

The Identity and Access Management (IAM) solution in FoF requires scalable and dynamic model that can operate in hybrid cloud environment.



Monitoring and control in cloud

Dynamic access control

Support for different security models and security levels

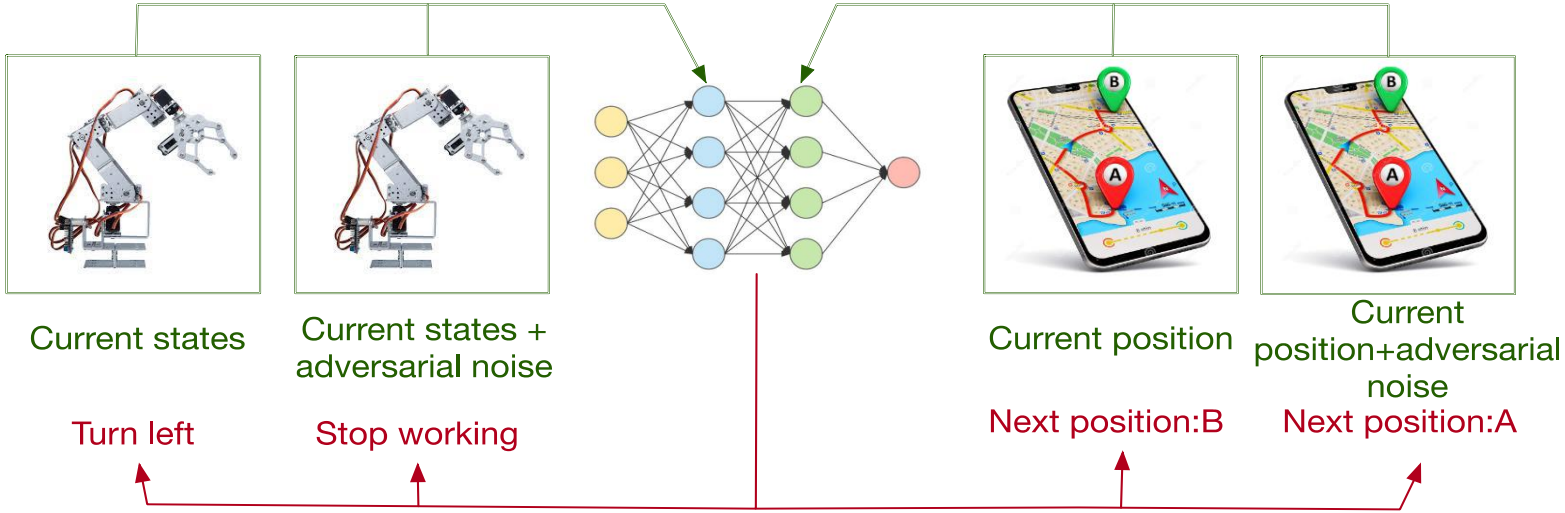
IT and OT environments

Utilizing Machine Learning (ML)

Survey: www.menti.com Code: 35 64 55 0

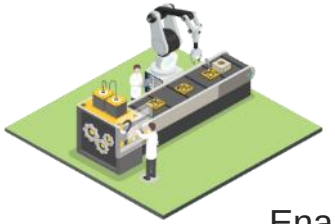
Robust machine learning ability

State-of-the-art DNNs can make correct prediction/decision with high confidence, But DNNs are also easily fooled, slightly feature changed that are unrecognisable to humans, but DNNs believe with high certainty are other decision.



To solve this issue, we can
1. Robust NN model
2. Detection of adversarial attacks

Human/Machine behaviour watch



Watch and analyse the behaviour of humans and machines in order to serve use-cases or detect misuse-cases (anomalies).

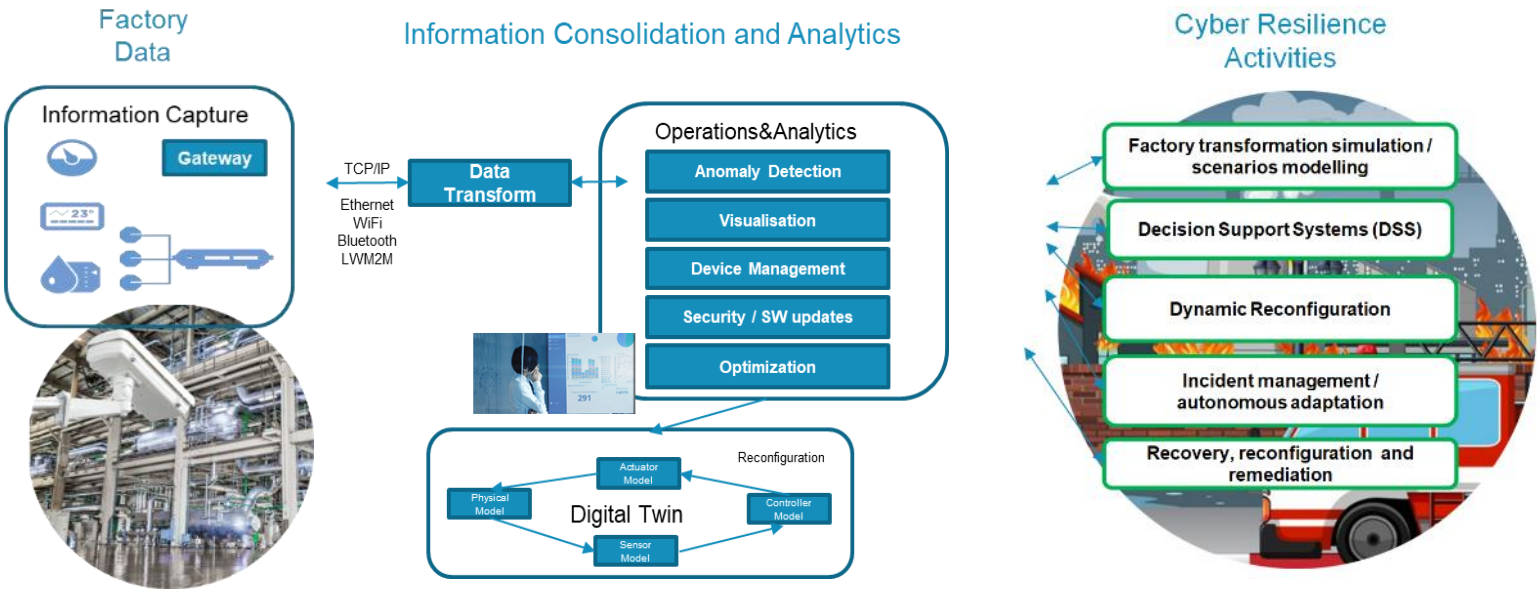
Enable data collection in identified monitoring areas (Human, Component, Process, Network) and monitoring layers (Edge, Platform, Enterprise).

Perform data correlation to facilitate the incident detection in shop floor and connected environments where humans and robots collaborate in their daily work.

Establish supervision techniques to provide situational awareness and security and safety related threat detection techniques.

Cyber-resilience capabilities

The development of Cyber-resilience capabilities goes beyond risk management and tactical technical solutions, requiring a holistic view of systems and processes to prepare for the reality of cyber incidents. These principles are applied in the FoF environment.



Survey: www.menti.com Code: 35 64 55 0