Attack Simulation on Manufacturing System Digital Twin

Adrien Bécue,
Airbus Cybersecurity

Presentation Plan

1. **Industrial Cyber-risk today and tomorrow**

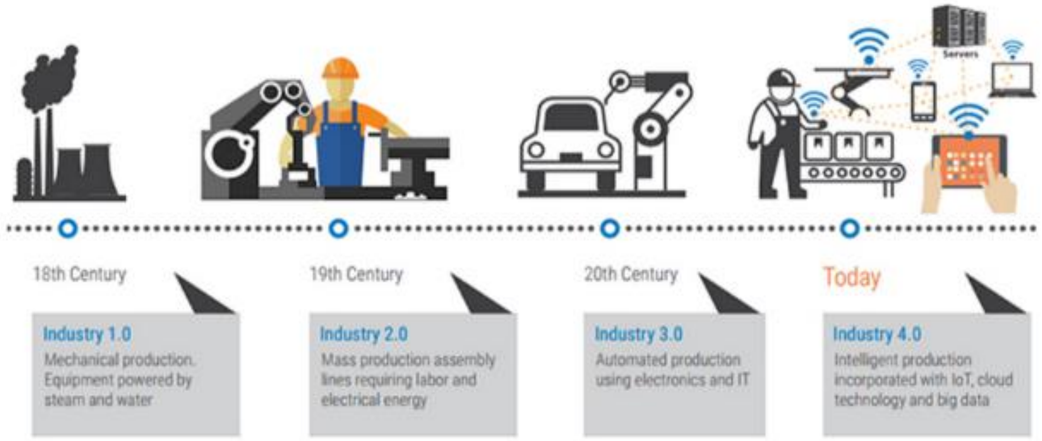
   > Introducing Industry 4.0 concept and security implications

2. **Simulation Challenge towards Industry 4.0**

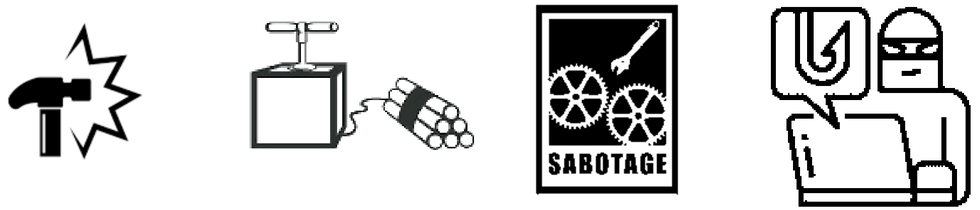
   > Defining the scope an challenges of Cyber-Physical Systems simulation

3. **Attack Simulation supporting security of Industry 4.0**

   > Leveraging CyberRanges and Digital Twins to secure Factories of the Future



Industrial Revolutions Timeline



Industrial Sabotage Techniques

Industrial Cyber-risk today and tomorrow

Adrien Bécue,
Airbus Cybersecurity

Industrial cyber-risk - Today

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

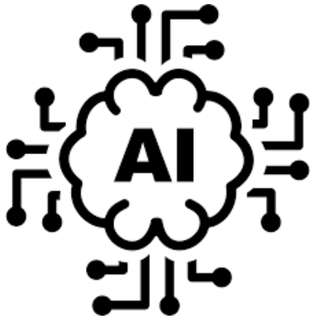
Attacker profile
-State sponsored
-Skilled in IT
-Skilled in ICS
-Aiming at physical damage

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

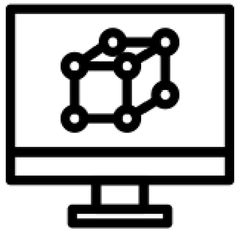
Damages
-Plant damaged by molten metal heated to thousands °
-Production loss
-Reputational damage

Industry 4.0: Key enabling technologies

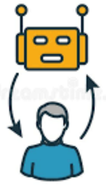
Cloud/edge technology
Big data



Artificial Intelligence
Machine-Learning



Simulation & modelling
Virtual / Augm. reality

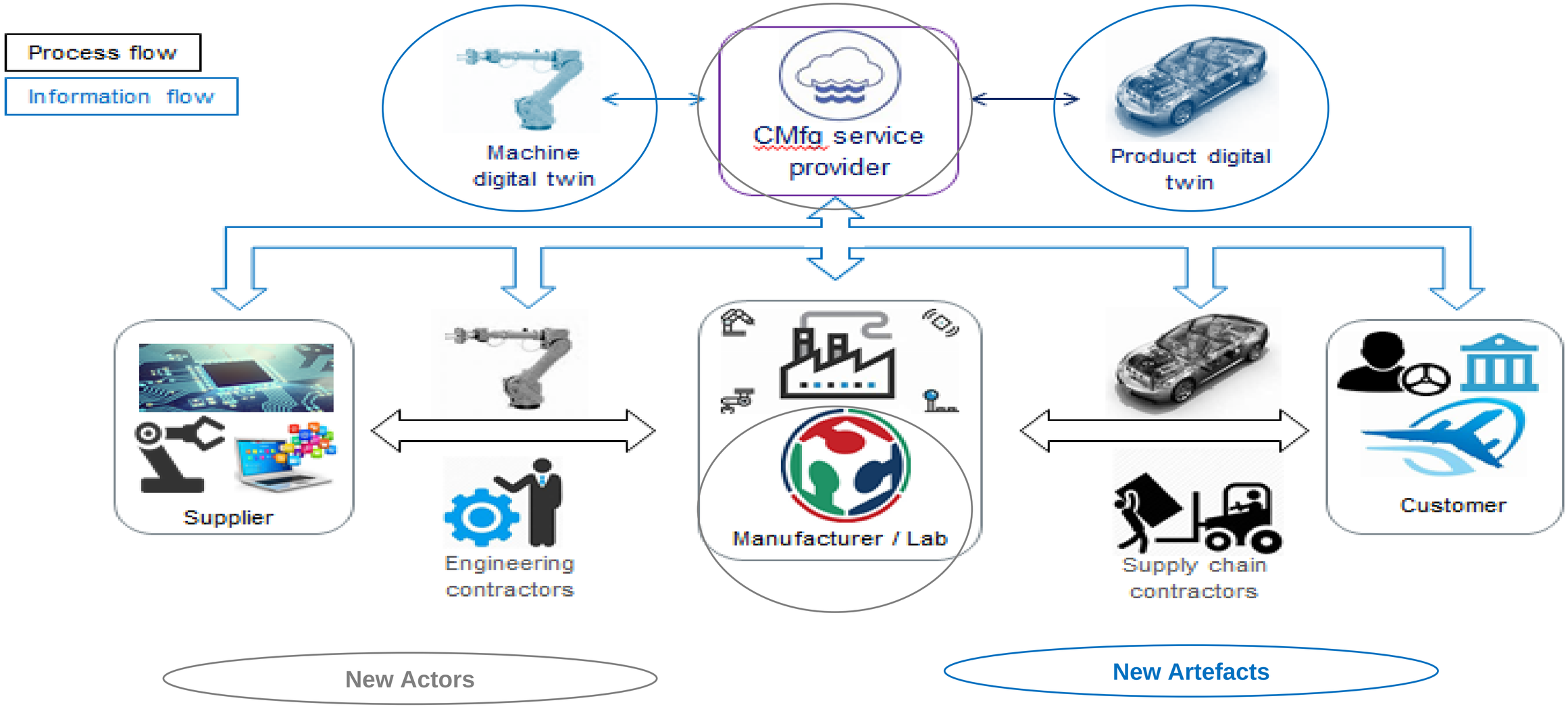


Collaborative Robotics
Augmented Human

M2M Communication
IIoT & Self* networks

Additive Manuf.
3D printing

Industry 4.0 Value Chain: New actors and artefacts



Industrial cyber-risk – Tomorrow ?

Automotive Assembly line hacked!
Attacker gained control through digital twin

Autonomous robot kills a worker!
Adversarial machine learning suspected…

Military secret stolen in weapon factory!
Rogue IoT device leaked rocket warhead design data …

Simulation Challenge towards Industry 4.0

Adrien Bécue,
Airbus Cybersecurity

Cyber-Physical System Properties

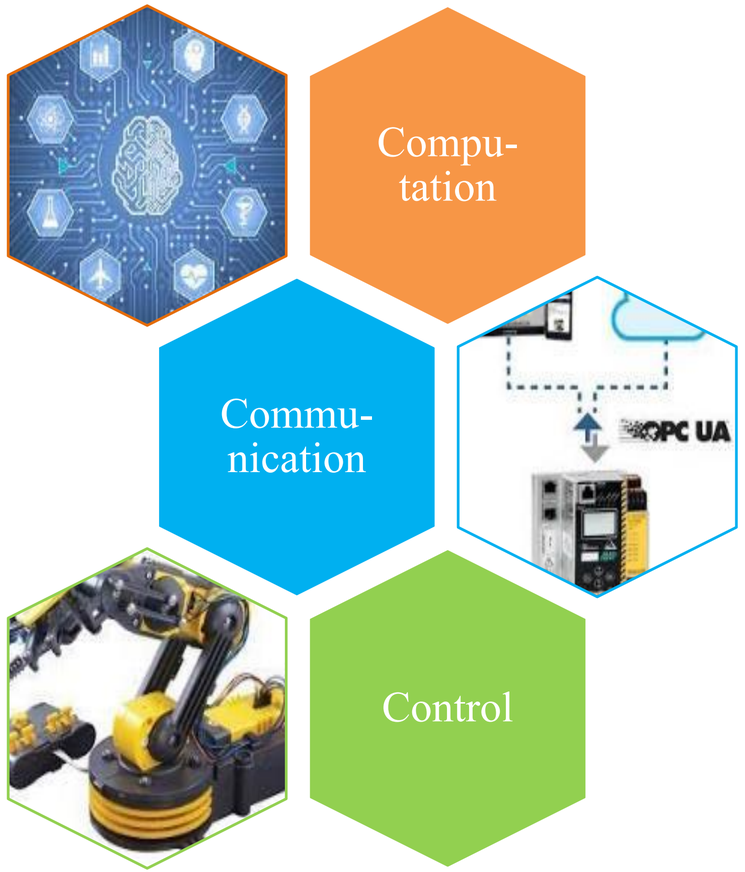
CPS: systems that integrate computing elements with the physical components and processes

Properties:

- Is made of 3 building blocks: Computation, Communication, and Control
- Includes a data acquisition and automation control flows (hopefully segregated)

Characteristics:

- Include feedback loops where physical processes affect computations and vice-versa
- Human is often in/on top of/underneath the loop, supervising or being supervised by the machine



CPS Modelling: Digital Twins

Definition: simulation model having the ability to connect to a physical entity and accurately reproduce its behavior and properties

Use-cases:

- Design: simulation-based design, requirement management and customization tool
- Operations: production monitoring, process optimization, quality control
- Maintenance: fault analysis, remote maintenance, predictive maintenance

Examples: General Electrics, PTC Windchill, Dassault Systems 3DS, MS Azure DT, Seebo, Anylogic, Ansys, IBM, Factory I/O, Siemens Digital Enterprise…

Cyber-Physical-Social System Properties

CPSS Space: a system which incorporates cyber space, physical space and social space

- Embraces the 3 layers of human response in any kind of interaction: behavioral, emotional, cognitive
- Social interaction: process whereby the behaviors of multiple individuals mutually influence each other

CPSS Object: a CPS that is enhanced with social attributes and able to somehow socialize.

- Requires specific characteristics of humans: consciousness, cognition, understanding, sentiment,
- Includes: Cyber-Physical System (CPS): eg a robot; Physical-Social System (PSS): eg a human ; Cyber-Social System (CSS): eg social network

CPSS Modelling Challenge

3 types of components: Cyber Components (C), Physical Components (P), Social Components (S)

3 types of systems: Cyber-Physical Systems (CPS), Physical Social Systems (PSS), Cyber-Social Systems (CSS)

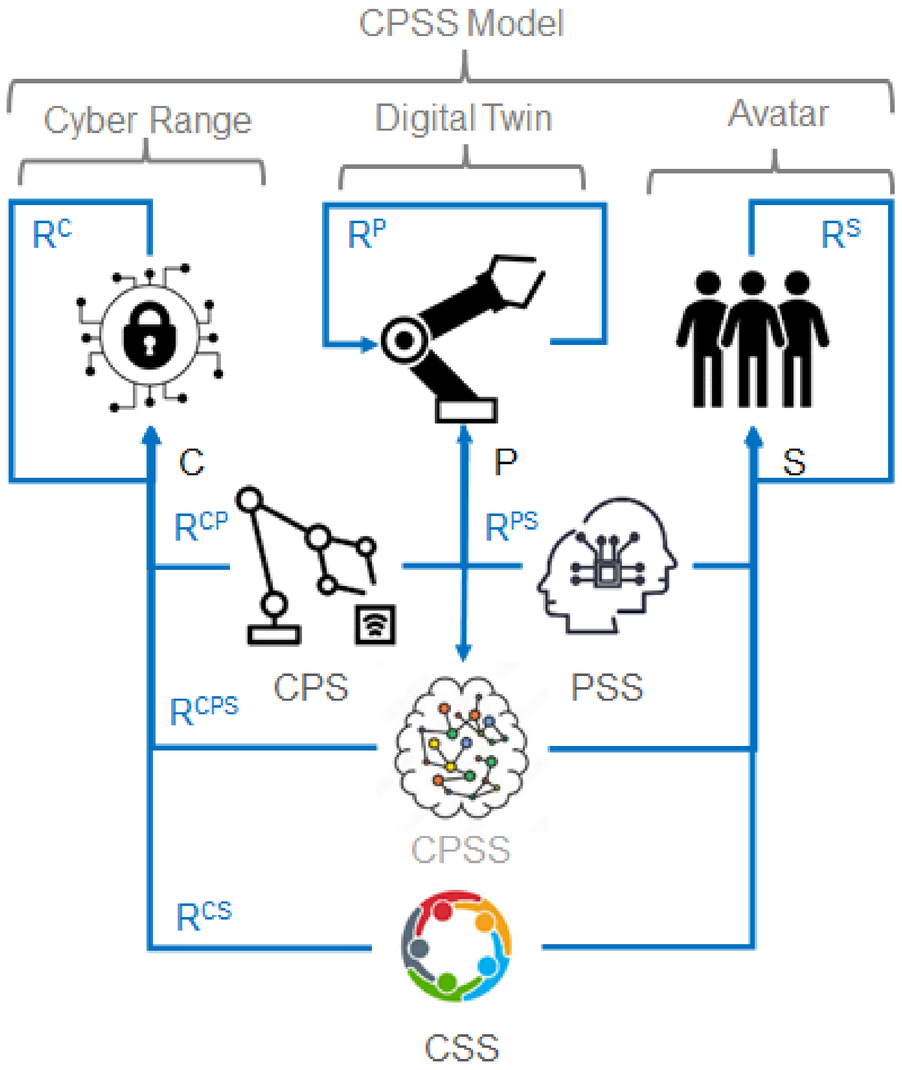
7 types of relations: R^{C}, R^{P}, R^{S} , R^{CP} , R^{CS} , R^{PS} , R^{CPS}

The social part is known to be the less predictable one which can lead to system instability

Application cases:

- CPSS Space: Smart Grids, Smart cities…
- CPSS Object: IoT, collaborative robotics

Simulation standard: Robot Operating System (ROS) - open-source robotics suite released by Willow Garage (2007) and maintained since 2013 by Open Robotics



Attack Simulation supporting security of Industry 4.0

Adrien Bécue,
Airbus Cybersecurity

Attack Simulation: leveraging Cyber-Ranges

- **Definition**: virtual environments used for cyberwarfare training and cybertechnology development.
- **Use-cases**:
- Testing: security testing in virtual / hybrid IT/OT network environments, validation of protective/defensive security solutions
- Training: applied cybersecurity exercises, blue team/red team exercises, ethical hacking exercises, capture the flag events
- Decision: simulation-based security design, attack prediction, situational awareness, response optimization
- **Examples**: Airbus Cyber-Range, Hynesim CR, Malice, CyberBit, Palo Alto, Ravello, Cisco …

Application Case: Airbus Roboshave System

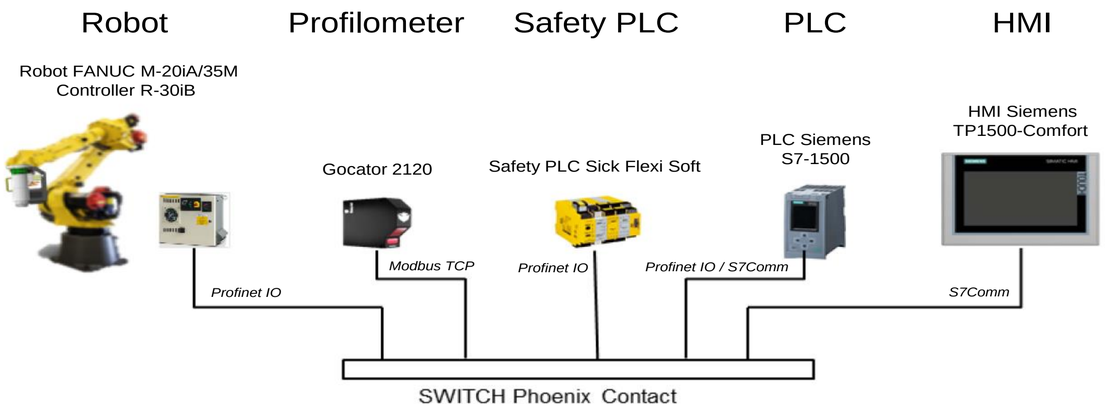
Roboshave automates rivet shaving operations on aircraft rudders to meet aerodynamics specifications

Components:

- Robot: FANUC M-20iA/35M;
- Profilometer: Gocator 2120;
- Safety PLC: Sick Flexi Soft;
- PLC: Siemens S7-1500;
- HMI: Siemens TP1500-Comfort

Protocols:

- 7Comm links to the HMI;
- Modbus TCP link between PLC & Profilometer;
- Profinet link between PLCs and Robot



Application Case: Airbus Roboshave Digital Twin

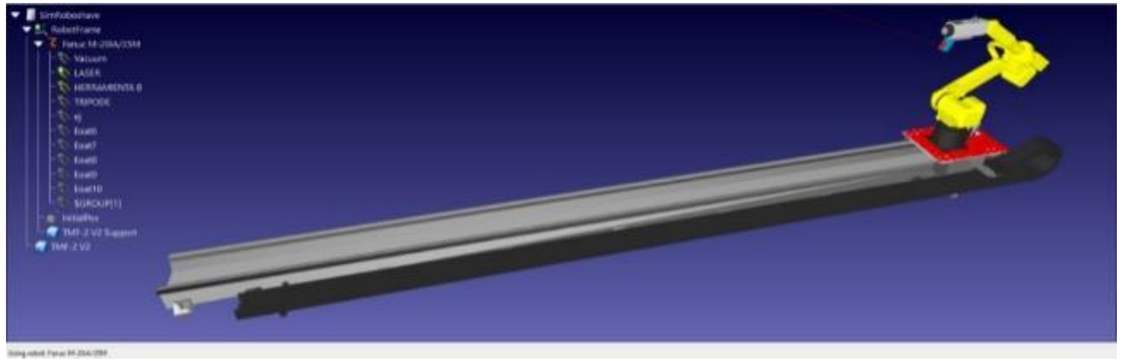
Roboshave Digital Twin is a result of Airbus CyberFactory#1 & SeCOIIA Projects

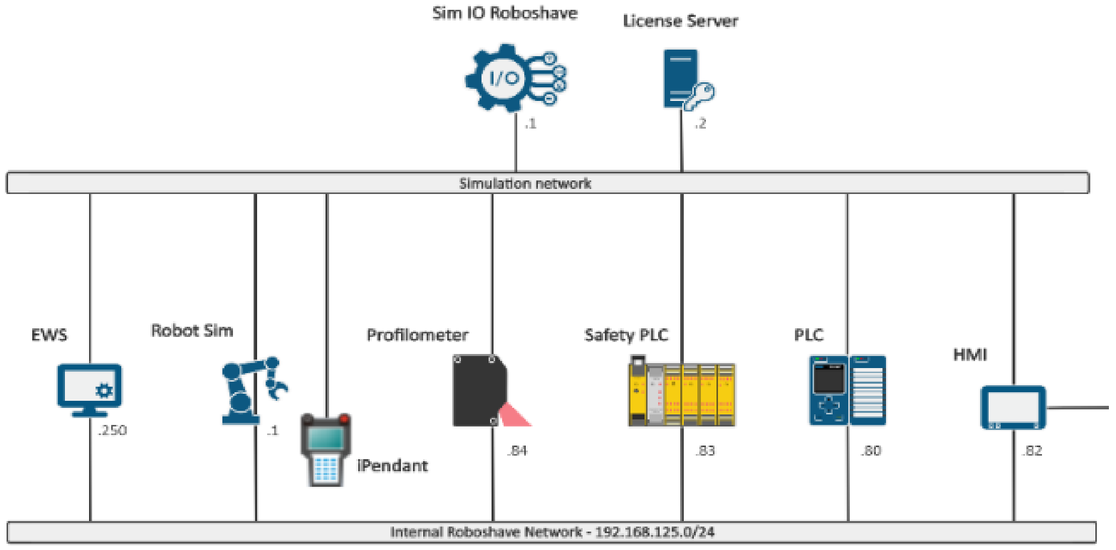
Simulators:

- Robot: RoboGuide from FANUC
- Profilometer: Airbus development
- Safety PLC: Airbus development
- PLC: PLCSim Advanced from Siemens
- HMI: WinCC Comfort from Siemens

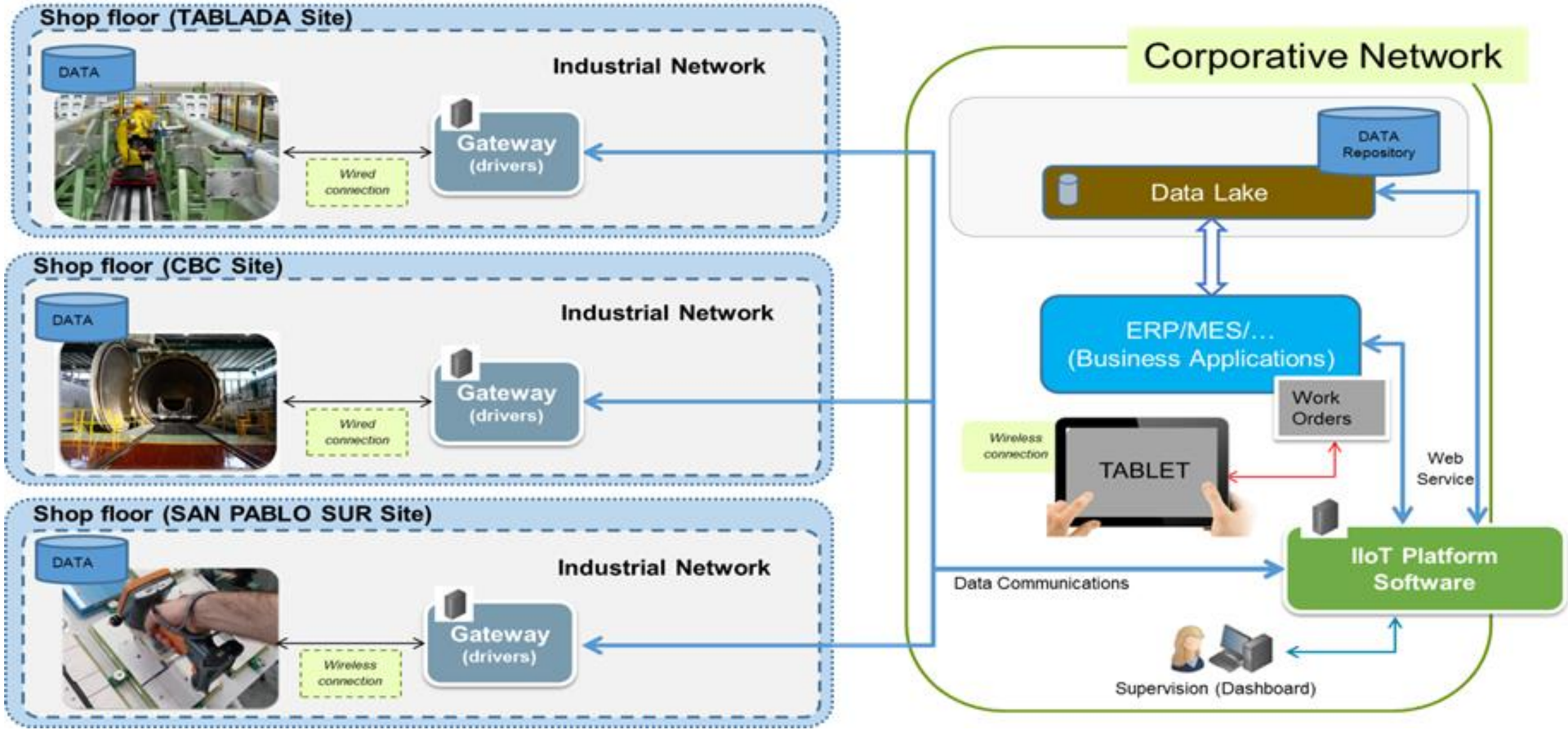
Attacks:

- MiM Address Resolution Protocol Poisoning
  > disables the cancel button
- Spoofing data over OPC UA
  > modifies rivet shaving stats on HMI





Upcoming work: Roboshave CPSS modelling



Administrator

Attacker

Worker

Cobot

Thank you!

https://www.cyberfactory-1.org/en/home/

adrien.becue@airbus.com