Developing the cybersecurity and resilience capabilities of Factories of the Future (FoF)

FIIF: CyberFactory#1 dissemination event, 9.6.2022 Helsinki

Jarno Salonen, VTT Technical Research Centre of Finland

Agenda

CyberFactory#1 basics

FoF Resilience

R&D work done by the Finnish consortium

CyberFactory#1 fact sheet
ITEA#17032 (2018-2022)

CyberFactory#1 (CF#1) aims at designing, developing, integrating and demonstrating a set of key enabling capabilities to foster optimization and resilience of the **Factory of the Future (FoF)**.

CF#1 is a catalyst project supplementing and developing current enabling technologies of the **Industry 4.0**, more specifically in the areas of:

1. Factory System of Systems modelling
2. FoF Optimization
3. FoF Resilience

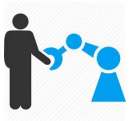
CF#1 is an ITEA3 project with 28 partners from seven countries (Canada, Finland, France, Germany, Portugal, Spain and Turkey) embracing technical, economic, human and societal dimensions at once. The project started in 12/2018 and ends in 06/2022.

Cloud/edge technology
Big data

Virtual/Augmented reality
Next generation HMIs

IIoT and M2M
Communication

Artificial Intelligence
Machine-Learning



Collaborative Robotics
Augmented Human

Additive Manufacturing
3D printing

Industrial cyber-risk – basis for the project

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 OT

Attack story
-Spear phishing
-Credentials theft
-Hack into office network
-Access to industrial Ntwk
-Control Blast furnace
-Prevent safety shut down

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

Industrial cyber-risk – Future?

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

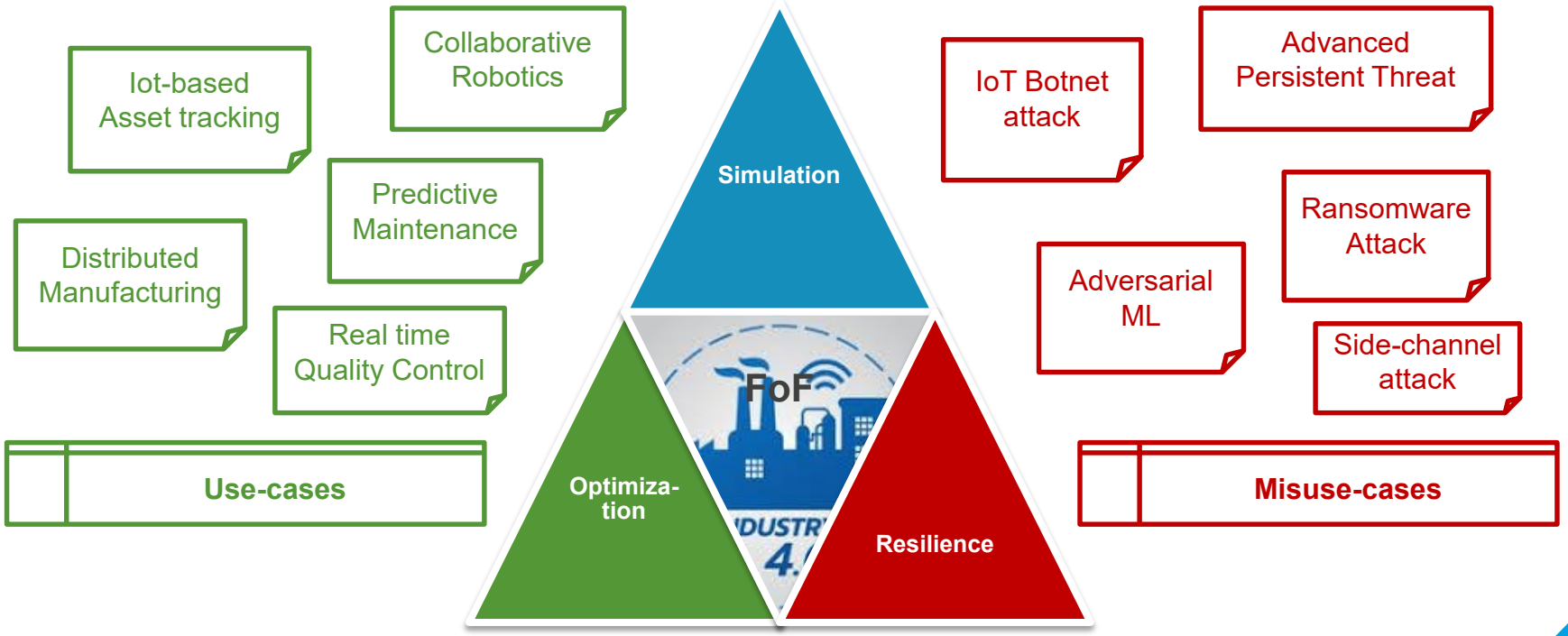
Autonomous robot kills a worker!
Adversarial machine learning suspected…

Affecting industrial processes…

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

Project ambition

Addressing opportunities and threats for the Factory of the Future:



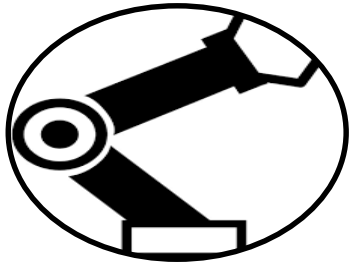
Project key capabilities

	Technical dimension	Economical dimension	Human dimension	Societal dimension
Modelling & simulation	CAP31-CPS Modelling & Digital Twins	CAP32-Factory ecosystem modelling	CAP33-Human behavior modelling	CAP34-Factory SoS modelling
Production Optimization	CAP41-Real time sensing & tracking	CAP42-Manufacturing data-lake exploitation	CAP43-Human/Machine optimization	CAP44-Distributed Manufacturing
Resilience enhancement	CAP51-Human/Machine access & trust mgmt	CAP52-Adversarial/Robust learning	CAP53-Human/Machine behavior watch	CAP54-Cyber-resilience mechanisms

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

Partners in the value chain (12 from 28)

6 presenting today

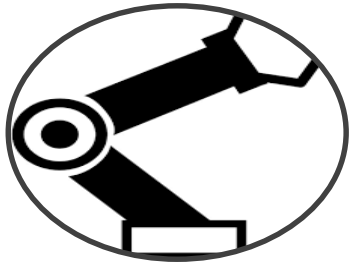
Users

AIRBUS

idepa THE ACCESSORY IS ESSENTIAL

VESTEL

HIGH METAL



Suppliers

PAL ROBOTICS

Bittium

SisTrade Software Consulting, S.A.

Lostar

Researchers

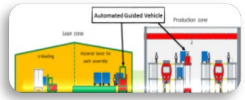
VTT

isep Instituto Superior de Engenharia do Porto

BIGS BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

OFFIS INSTITUT FÜR INFORMATIK

10 Use Cases



Optimization of Material Supply for Rail Vehicle Production
(BOMBARDIER Tr. UC)

Secure and optimized factory information and logistic management
(VESTEL UC)

InSystems proANT transport robot fleet optimization in factories
(INSYSTEMS UC)

Roboshave: Optimization of Robotic Manuf. System based on IIoT technologies
(ADS UC)

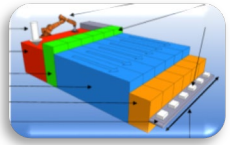
Autoclaves: Cyber-physical Jigs Monitoring across Industrial IoT deployment
(ADS UC)

GapGun: Advanced control of smart tools using Industrial IoT
(ADS UC)

Cyberfactory#1
10 Use Cases / Misuse cases

Secure CPS-based Manufacturing on auxiliary automotive industry
(S21SEC UC)

Textile production line increased digitalization for the automotive industry
(IDEPA UC)



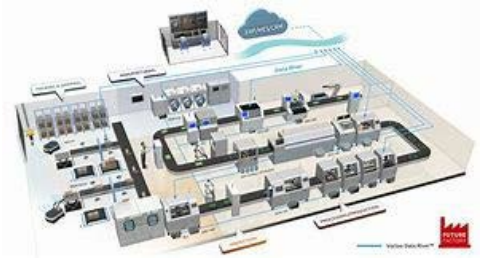
Highly automated cheese making by IoT process lines and machinery
(HIGH METAL UC)

Cyber-secure networked supply chain and information architecture
(BITTIUM UC)

Project target market areas

Digital Twin Market

- Fastest growing market
- Lack of open standards



Industry 4.0 Market

- Largest market potential
- Saturation, adoption lagging behind

IIoT Security Market

- Fast growing market, medium size
- Highly competitive

FoF Resilience

Overview of the FoF resilience work package

Manage access rights dynamically for humans and machines

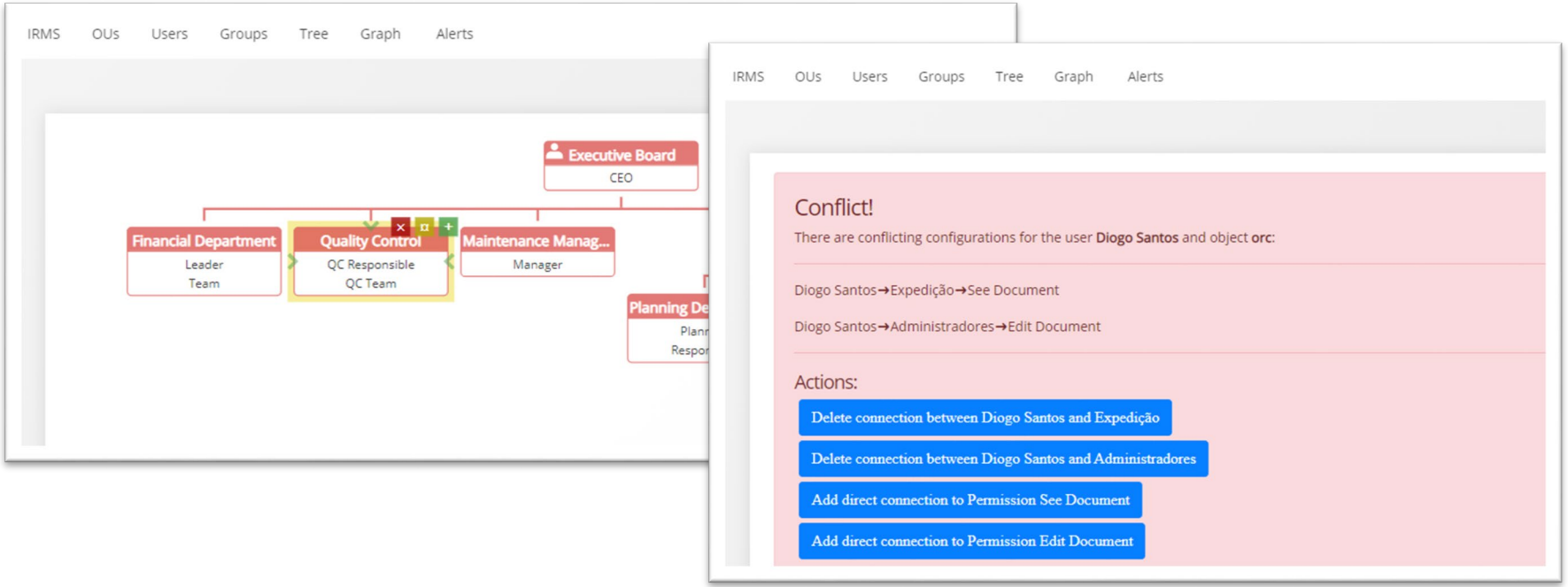
Continuously watch for anomalies on factory assets regardless of their origin

Prevent manipulation of manufacturing and product-embedded AI

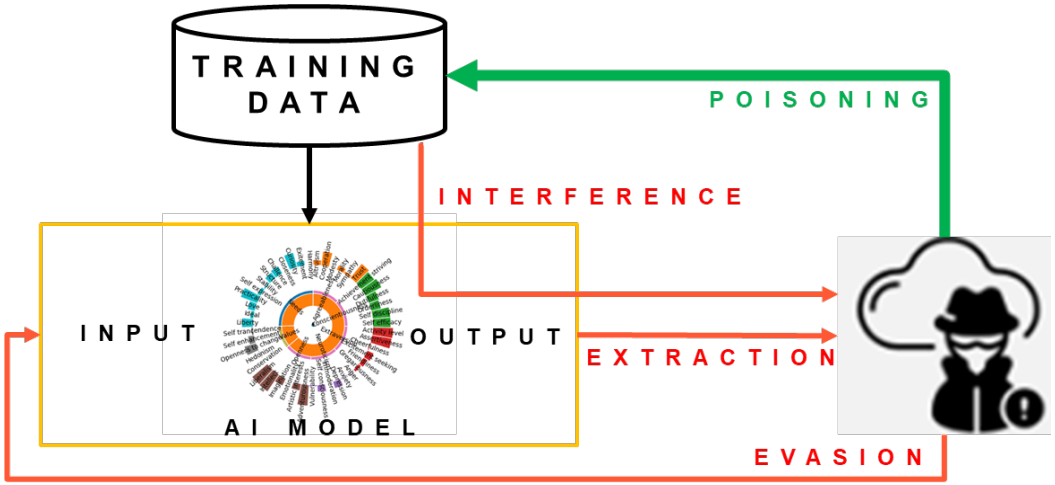
Enable decision-aided or autonomous Remediation & Recovery of factory assets

Establishing trust within the factory IT and OT systems
Intelligent Role Management System (IRMS)

- Organizational (Organogram) mapping and Position Definitions (left)
- Conflict Detection and Resolution (right)



Preventing the manipulation of AI
Ways of fooling the AI to propose wrong actions

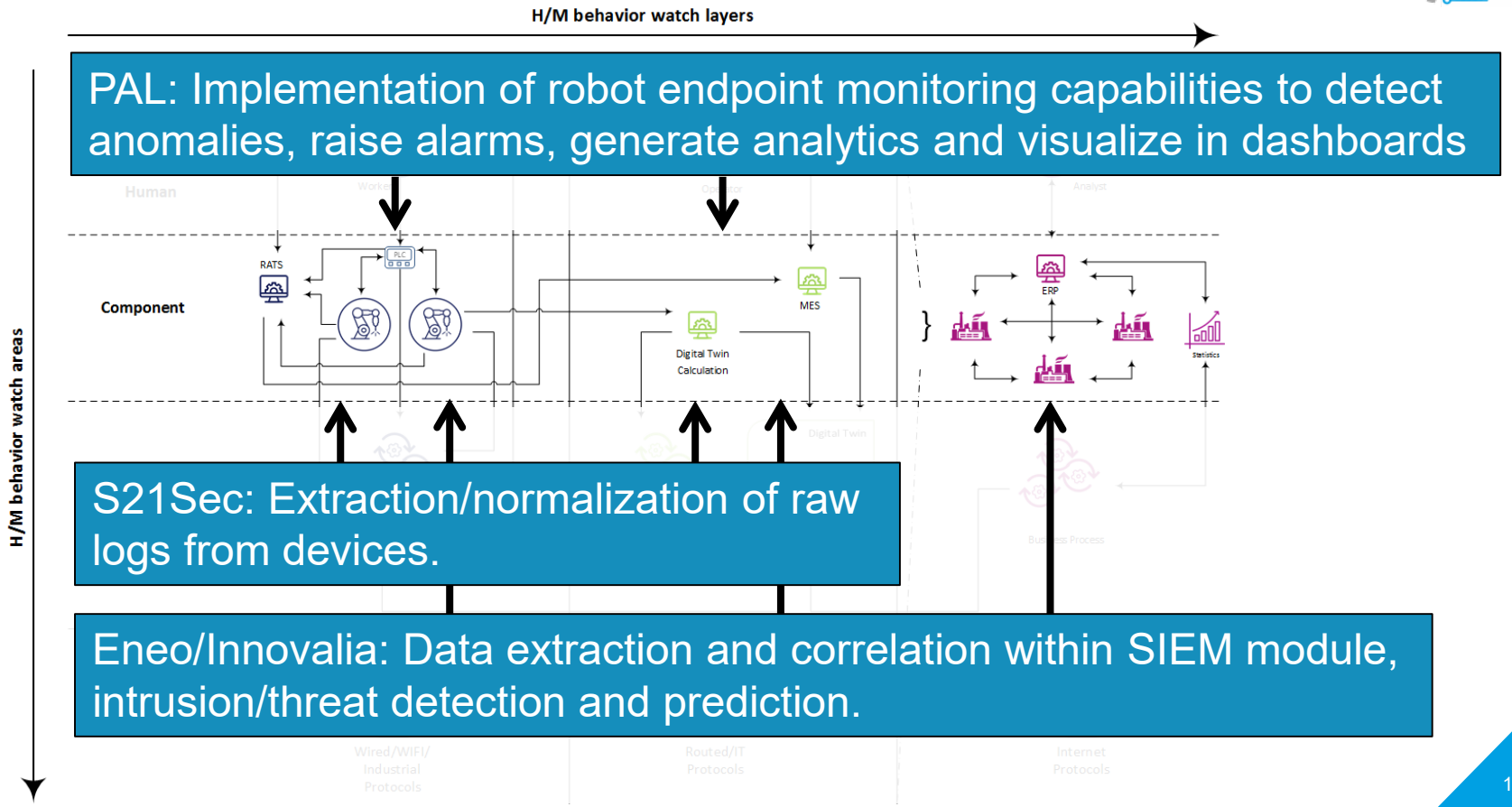


Poisoning attack: adversarial **contamination of the training data**. This will ruin retrained new model and make it behave as desired by attacker.

This can be achieved **by injecting malicious samples** during operation that subsequently disrupt retraining of in example intrusion detection system

Clean and analyze the training data carefully before utilizing it

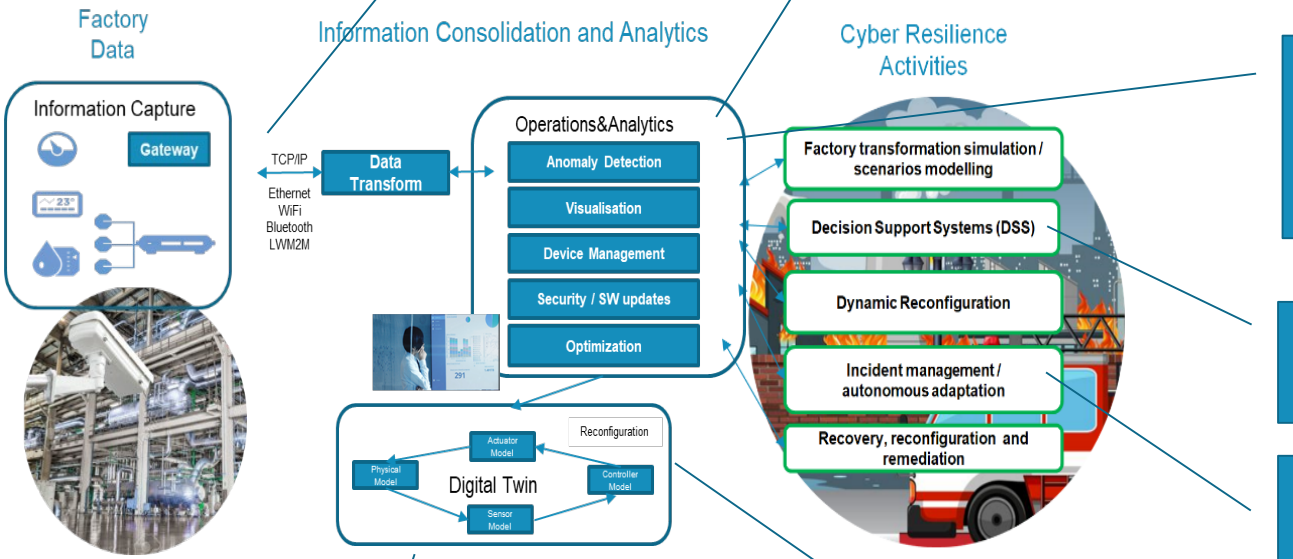
Real-time monitoring of the factory
Spotlight: component behaviour watch



FoF resilience
Cyber resilience planning and practicing

Addition of Extra Layer of Security for Wireless Communications **(GOHM, Vestel)**

OT systems to report to Security operations system (SoC) Capability to collect, process, filter and forward information to SoC **(Lostar) Architecture with Vestel, GOHM**



Include to the "Virtual Assistant Agent" a module with notifications to different users **(Sistrade)**

Secure architecture for **implementation of Incident Management DSS Tool (Airbus DE)**

Description of a reconfiguration approach which is able to adjust individual robot behaviour at run time **(HTW)**
Show what reconfiguration concept shall prevent (OFFIS)

Simulation of Use Case Security Architecture with help of digital twin and Airbus CyberRange Tool **(Airbus FR, Bittium, VTT, Netox, Rugged Tooling, Houston)**

Secure Cheese Making Architecture (HighMetal, VTT, Houston Analytics)

Research and development done by the Finnish consortium

Finnish partners involved

Bittium (supplier/end-user, https://www.bittium.com/), development of a secure information architecture along with applicable processes and information tools that support their digital partnered manufacturing and deliveries.

High Metal (end-user, https://highmetal.fi/en/), optimisation of the cheese manufacturing process in their machines as well as improving the overall cybersecurity.

Houston Analytics (supplier, https://www.houston-analytics.com/), prediction of faults and failures, predicting and addressing quality issues, automated root cause analysis, and optimisation of equipment usage and processes.

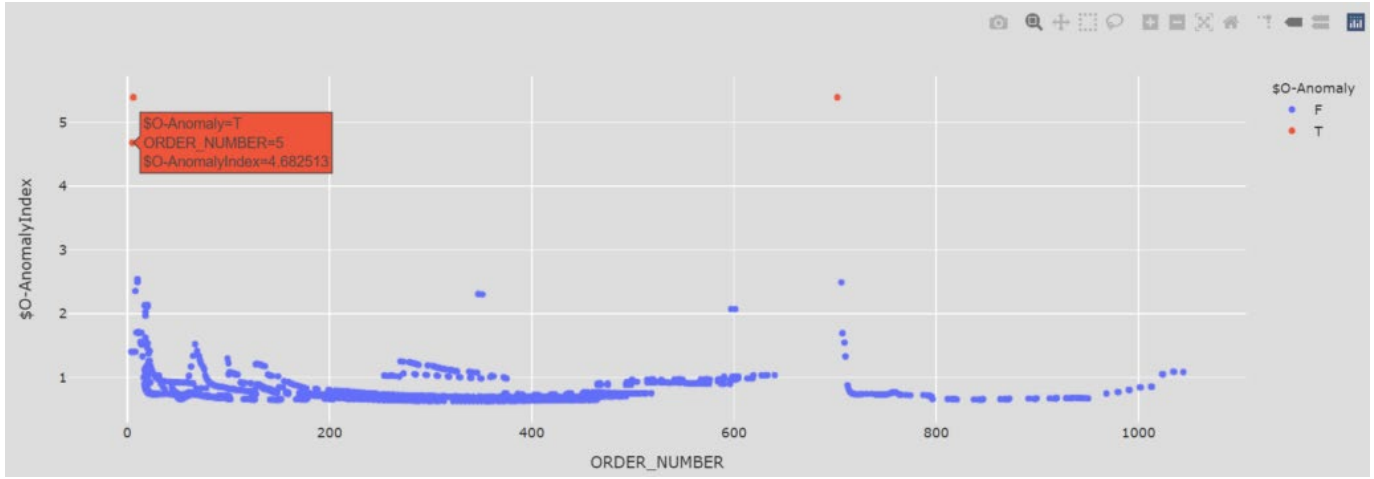
Rugged Tooling (supplier, https://ruggedtooling.com/), developing quality assurance and monitoring solutions for the functional safety and resilience of systems in demanding IP networks.

Netox (supplier, https://netox.fi/), developing on premise and cloud IAM solutions for their manufacturing industry customers with the focus on operational technology (OT).

VTT (research, https://www.vttresearch.com), Developing solutions for modelling and simulation (digital twin), cybersecurity and resilience.

Some examples by the Finnish consortium

Using AI for anomaly detection with visualisation for the human aid



VTT

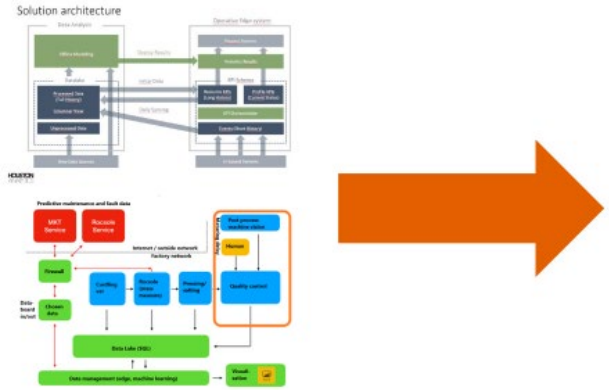
HOUSTON ANALYTICS

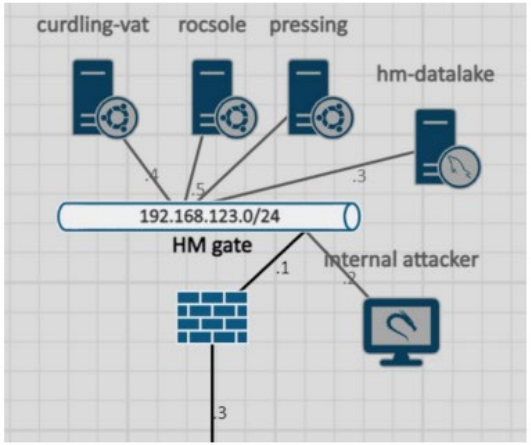
Bittium

Interested? Check the blogpost
https://www.cyberfactory-1.org/blog/tackling-anomalies-in-factory-of-the-future-networks-with-ai-and-visualization/

Some examples by the Finnish consortium

Building the cyber digital twin for industrial cybersecurity simulations





VTT

HIGH METAL

RUGGED TOOLING

Interested? Check https://www.cyberfactory-1.org/ for the forthcoming blogtext + video next week

Thanks!

The presentation slides will be shared on the FIIF member page as well as the project webpage

https://www.cyberfactory-1.org/blog/fiif-event-cyberfactory1/

If you have any questions related to the project, don’t hesitate to contact us.

Jarno Salonen

Safe and connected society / Applied cybersecurity

VTT Technical Research Centre of Finland

jarno.salonen (at) vtt.fi