CyberFactory#1 - Increasing the FoF resilience with modelling and simulation tools

Jarno Salonen
VTT Technical Research Centre of Finland

Agenda

Setting the scene

Cybersecurity vs. Cyber resilience

Primary tools

CyberFactory#1 - Our R&D efforts increasing FoF cyber resilience

How to benefit from simulation and modelling

- Designing an Intelligent Role Management System (IRMS)
- Creating trust towards AI technologies
- Monitoring the FoF
- Preparing for cyber Incidents with the help of cyber resilience capabilities
- Simulation of cyber attacks with the help of Airbus CyberRange

Setting the scene again

Setting the scene

Image derived from PwC US – Factory of the Future, https://www.youtube.com/watch?v=JsjIMNRcRf4

Cybersecurity vs. Cyber resilience

Cybersecurity

“the process of protecting information by preventing, detecting, and responding to attacks”

- NIST

“the protection of internet-connected systems, such as hardware, software and data from cyberthreats”

- TechTarget

(Cyber) resilience

“the capacity to recover quickly from difficulties, toughness”

“the ability of a substance or subject to spring back into shape, elasticity” *- Oxford languages*

“the psychological quality that allows some people to be knocked down by the adversities of life and come back at least as strong as before” *- Psychology today*

“you make people resilient by exposing them to things that they are afraid of and make them uncomfortable voluntarily and use exposure” *- Jordan B. Peterson*

“entity’s ability to continuously deliver the intended outcome, despite adverse cyber-events”

- Björck et al. (2015)

Primary tools
Digital Twin and Cyber Range

Digital twins (DT) are representations of physical systems or devices that can be connected to a training environment.*

- Global DT market: $3.2B (2020) → $48.2B (2026) – *MarketsandMarkets 2020*

Cyber ranges (CR) are dedicated environments for cybersecurity testing and training...and make use of DTs.*

- Global CS market: $165.78B (2021) → $366.10B (2028) AND
- CIP market: $96.30B (2019) → $154.59B (2027) – *Fortune Business Insights 2021*

Benefits of CR and DT for resilience

- Security by design
- Data collection for e.g. anomaly detection, behaviour analysis
- Incident management and situational awareness
- Security testing
- Simulating disaster scenarios and planning/testing recovery, reconfiguration and remediation measures
- Training personnel to prepare for the worst (including awareness)

The aforementioned activities cover the entire lifecycle of FoF

* Noponen et al. (accepted). Review on Cybersecurity Threats Related to Cyber Ranges. International Conference for Internet Technology and Secured Transactions, 7-9 December 2021, London, UK

CyberFactory#1

Our R&D efforts increasing FoF cyber resilience

Manage access rights dynamically for humans and machines

Prevent manipulation of manufacturing and product-embedded AI

Continuously watch for anomalies on factory assets regardless of their origin

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

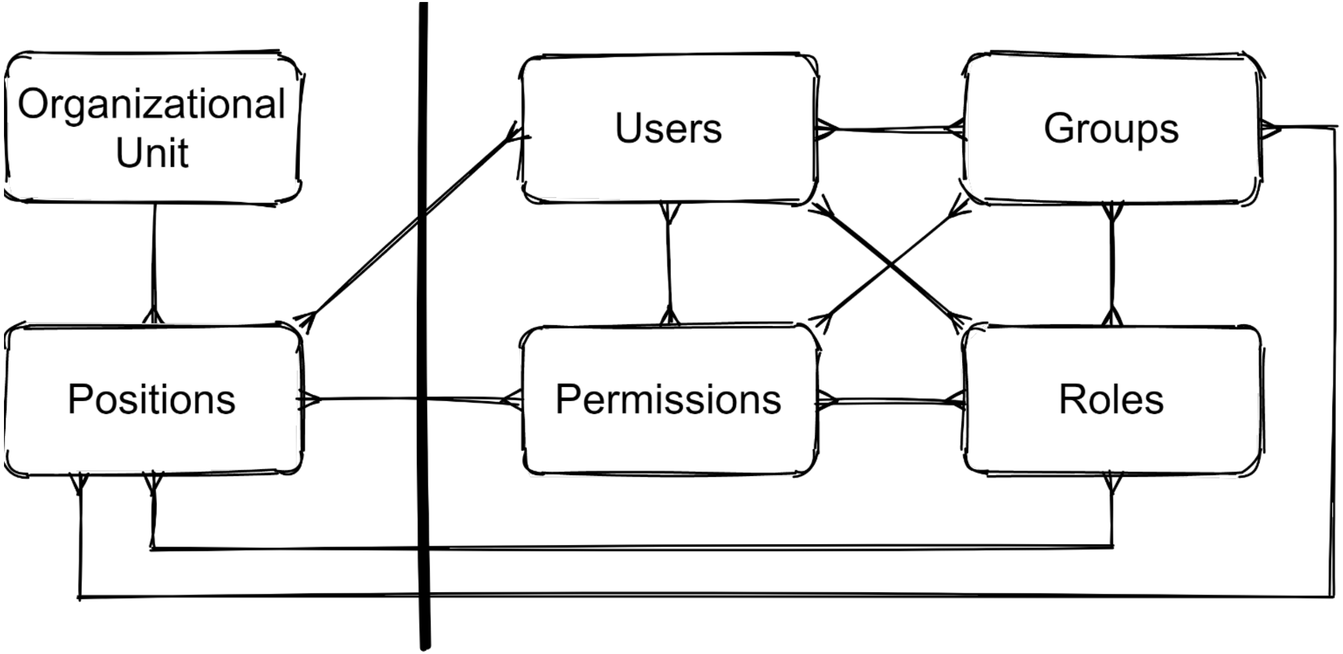
How to benefit from simulation and modelling?

CyberFactory#1 | ESM Conference, 27 October 2021

How to benefit from simulation and modelling

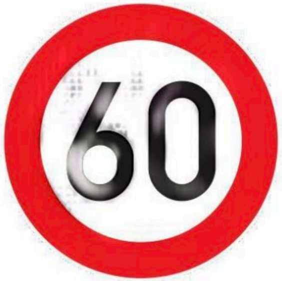
Designing an Intelligent Role Management System (IRMS)

- IRMS Model and its Flexibility:



How to benefit from simulation and modelling

Creating trust towards AI technologies



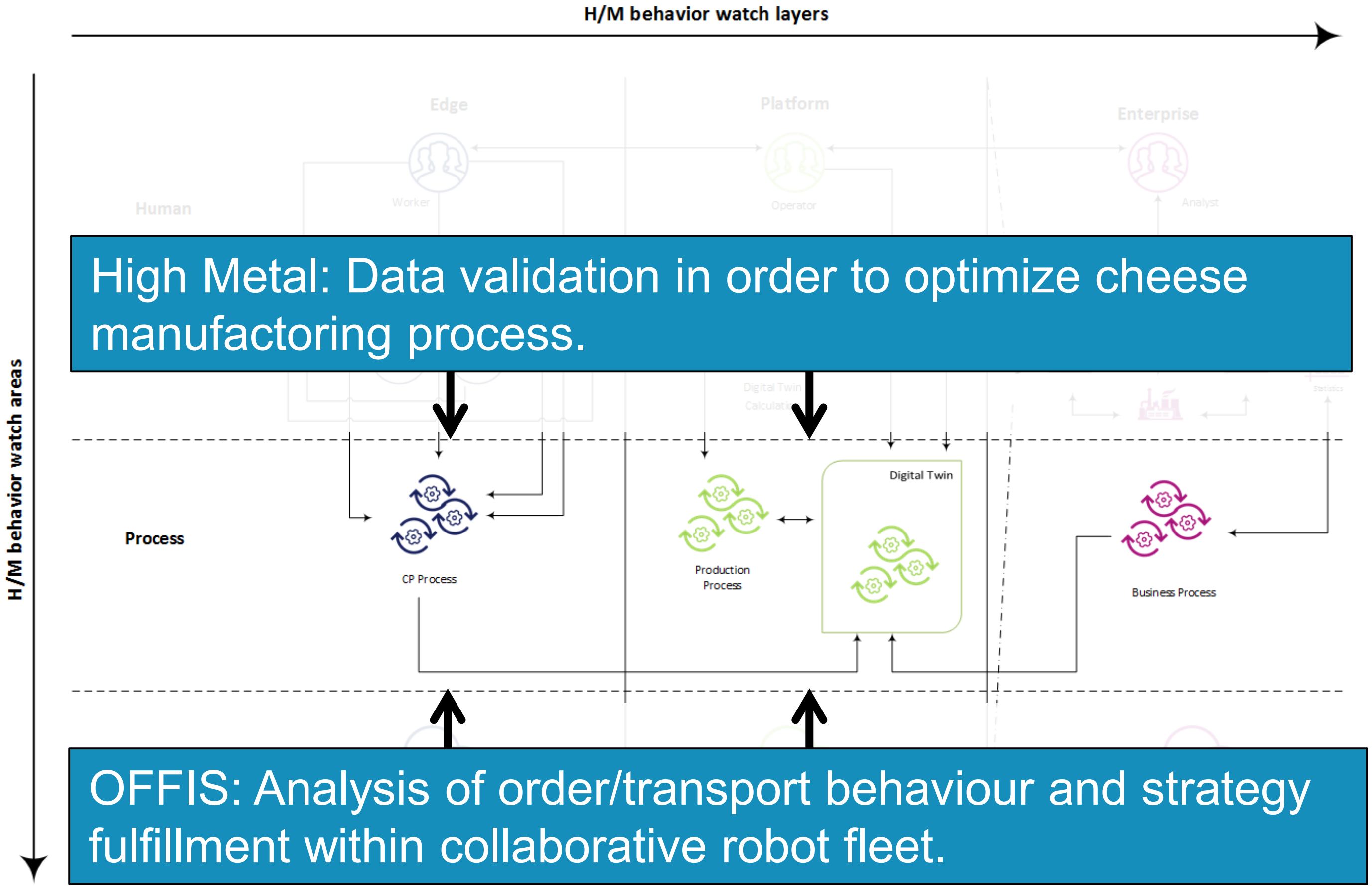
Traffic sign
with adversarial noises

Real label is 60 km/h

Max. speed is 100 km/h

Image derived from https://emerj.com/partner-content/self-driving-cars-simulations/

How to benefit from simulation and modelling
Monitoring the FoF



High Metal: Data validation in order to optimize cheese manufactoring process.

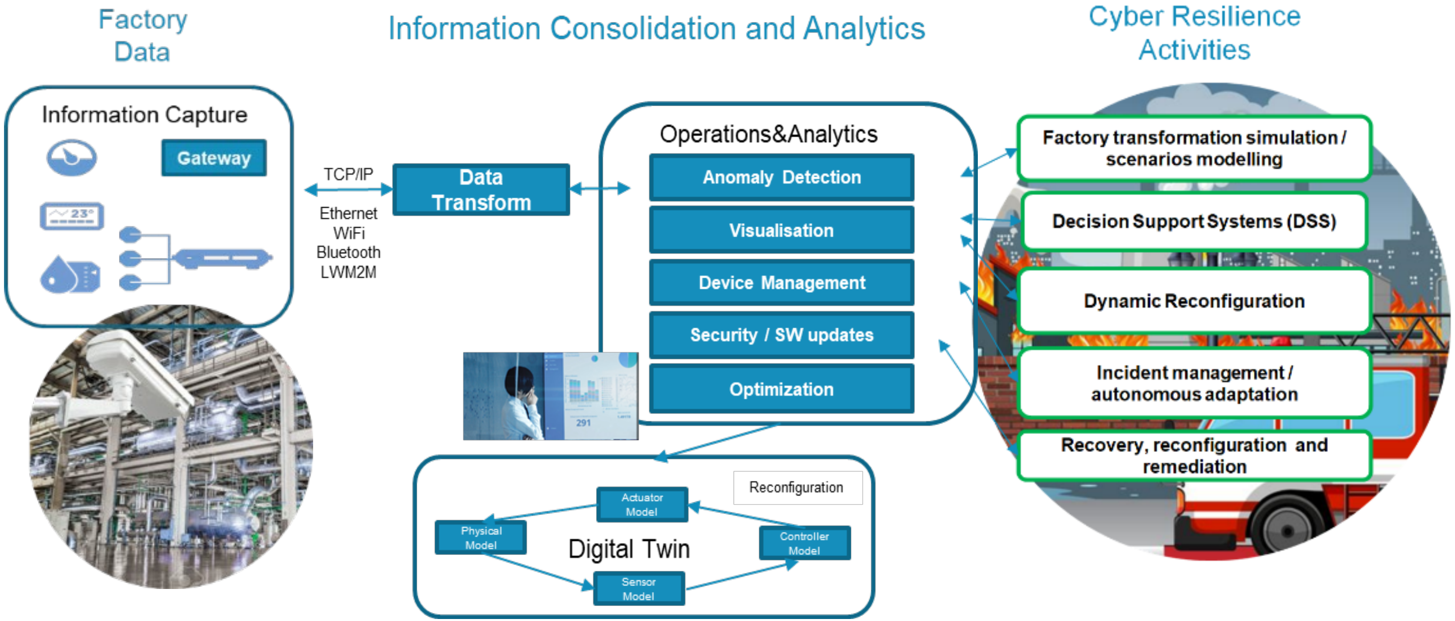
OFFIS: Analysis of order/transport behaviour and strategy fulfillment within collaborative robot fleet.

How to benefit from simulation and modelling

Preparing for cyber Incidents with the help of cyber resilience capabilities

The development of Cyber-resilience capabilities goes beyond risk management and 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.



Factory Data

Information Consolidation and Analytics

Cyber Resilience Activities

Information Capture

Gateway

TCP/IP

Ethernet
WiFi
Bluetooth
LWM2M

Data Transform

Operations&Analytics

- Anomaly Detection
- Visualisation
- Device Management
- Security / SW updates
- Optimization

Digital Twin

Actuator Model

Physical Model

Controller Model

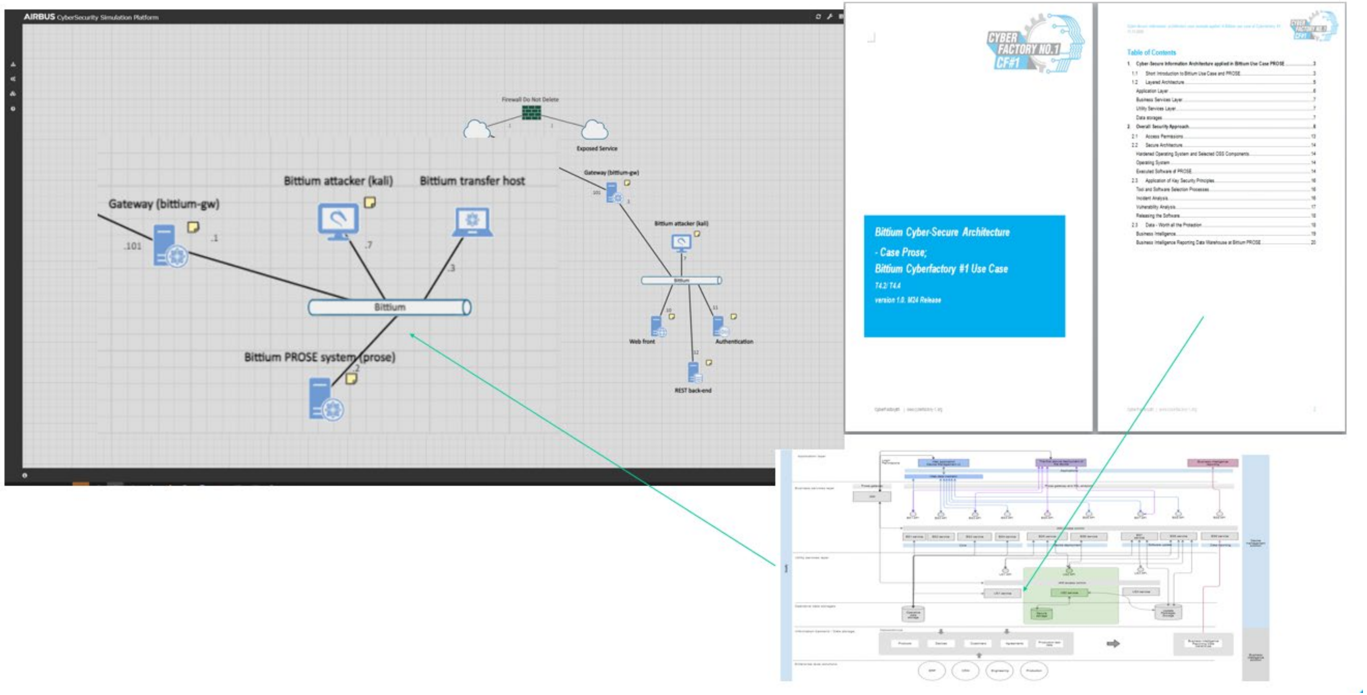
Sensor Model

Reconfiguration

- Factory transformation simulation / scenarios modelling
- Decision Support Systems (DSS)
- Dynamic Reconfiguration
- Incident management / autonomous adaptation
- Recovery, reconfiguration and remediation

How to benefit from simulation and modelling

Simulation of Cyber Attacks with the help of Airbus CyberRange



Bittium Cyber-Secure Architecture

- Case Prose;

Bittium Cyberfactory #1 Use Case

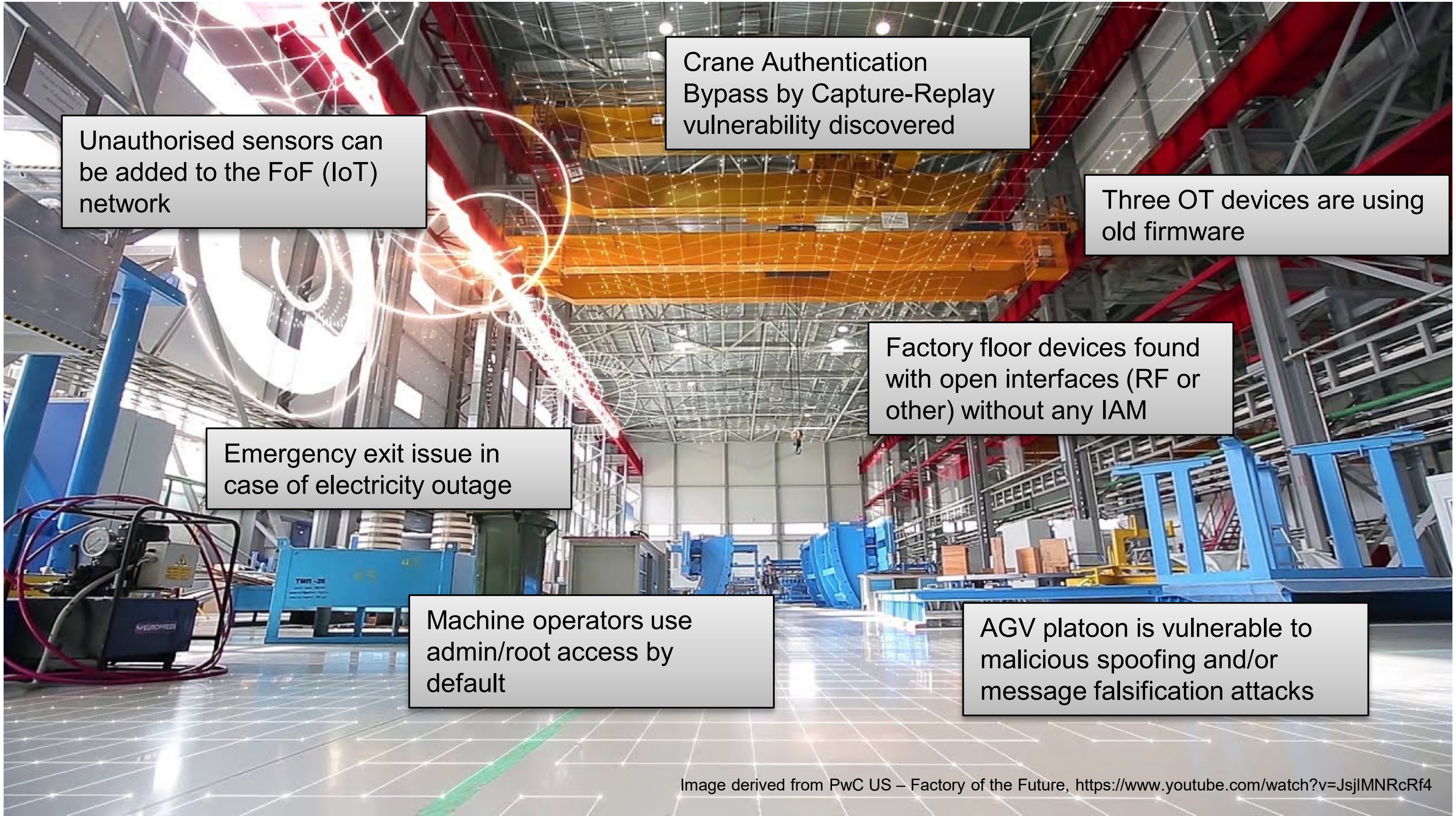
T4.2/ T4.4

version 1.0. M24 Release

Table of Contents

Connection of the use case architecture, digital twin of the use case and simulation environment.

Setting the scene again



Crane Authentication Bypass by Capture-Replay vulnerability discovered

Unauthorised sensors can be added to the FoF (IoT) network

Three OT devices are using old firmware

Factory floor devices found with open interfaces (RF or other) without any IAM

Emergency exit issue in case of electricity outage

Machine operators use admin/root access by default

AGV platoon is vulnerable to malicious spoofing and/or message falsification attacks

Image derived from PwC US – Factory of the Future, https://www.youtube.com/watch?v=JsjIMNRcRf4

Thank you!

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

Jarno.Salonen (at) vtt.fi