Developing and Using a Digital Twin of a Decentralized Robot Fleet

- FIIF 09.06.2022, Helsinki
- Linda Feeken (DLR), Matthias Glawe (Airbus)

Modeling and Simulation for the Factory of the Future (FoF)

Project Work Package Introduction

Model & simulate components of the FoF

CAP31

Model & analyze behavior of human workers in the FoF

CAP33

CAP32

Understand the ecosystem of the FoF

CAP34

Understand the FoF as one holistic system of systems

Collaborating Automated Guided Vehicles (AGVs)

Use Case Introduction

- Fleet of Autonomous Guided Vehicles (AGV) on the production floor of the Factory of the Future
- AGVs that load and unload boxes or trays via conveyor belts
- Load transfer to/from active/passive conveyor stations

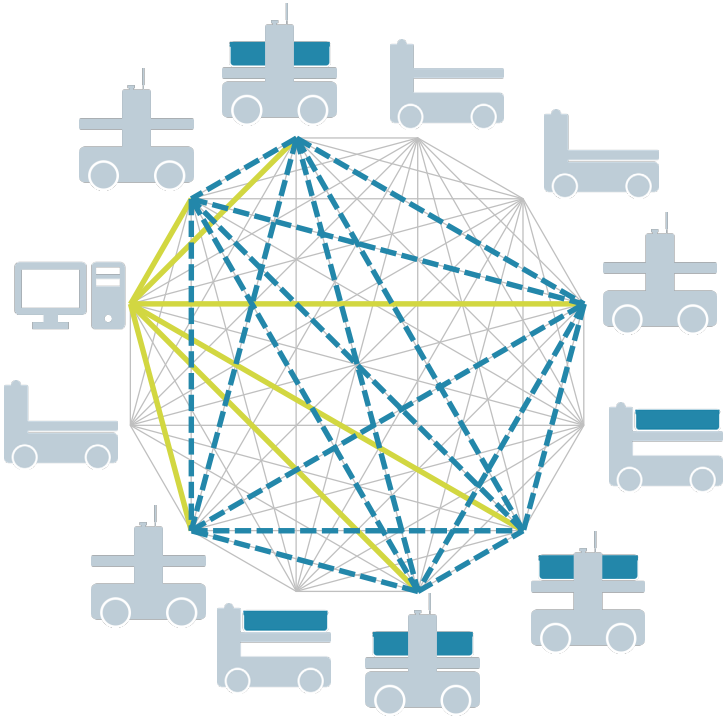
source: ASTI Mobile Robotics GmbH

source: ASTI Mobile Robotics GmbH

Collaborating Automated Guided Vehicles (AGVs)

Decentralized Orchestration

- AGV fleet is orchestrated decentralized
- Each AGV has its own control unit (CAC)
- Communication via Coaty Framework
- Transport Distribution influenced by Strategy
  - Self organization
  - Who takes over which transport
  - Who can drive where
  - Who charges battery when
- Strategy can be (manually) changed at runtime

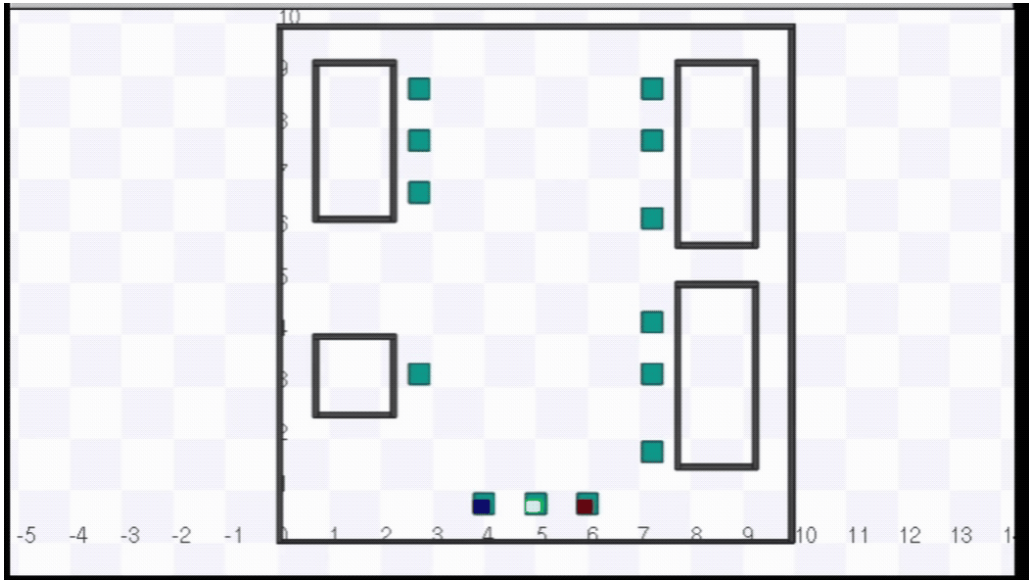


source: ASTI Mobile Robotics GmbH

AGV Fleet on the Factory Floor

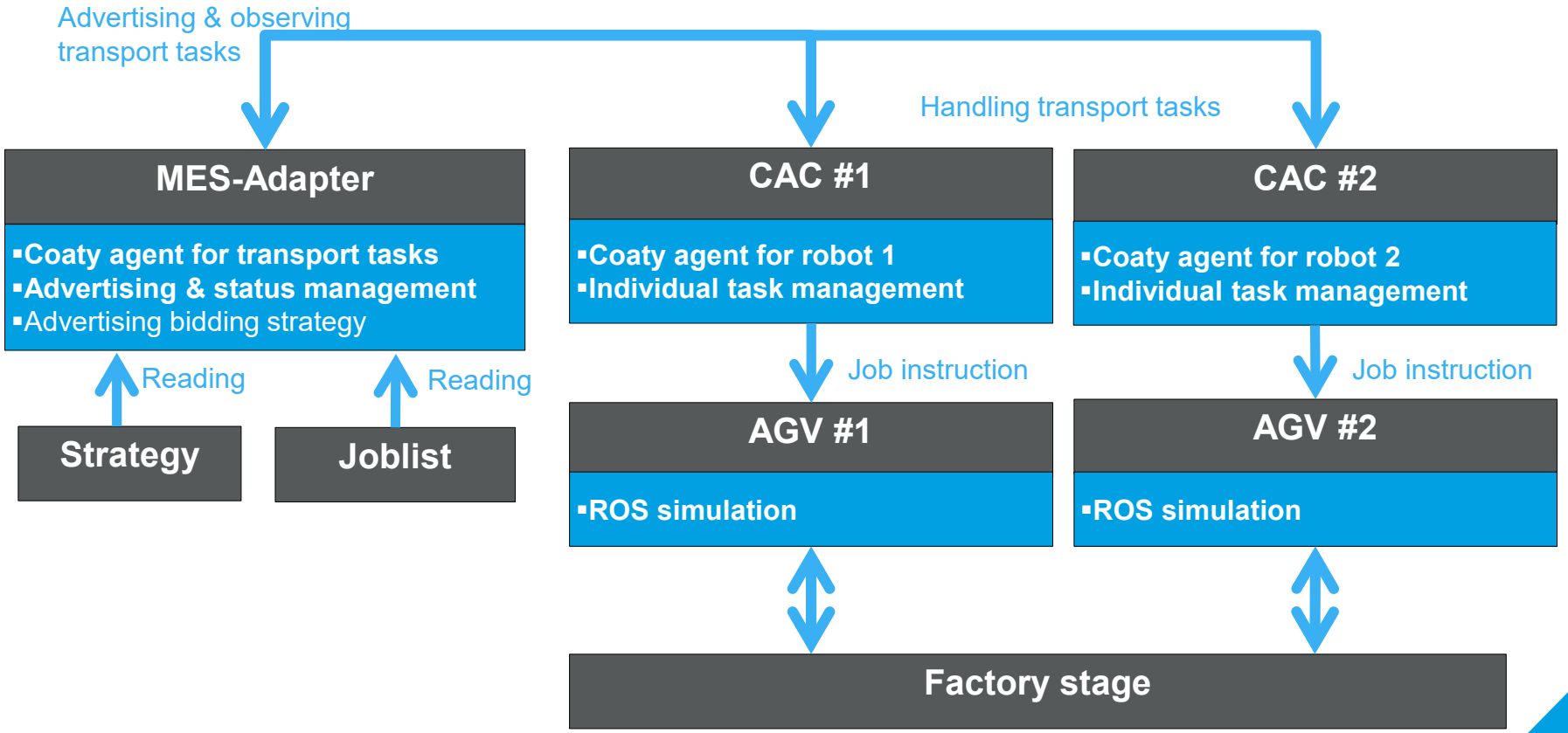
Digital Twin

- Simulation of AGV models
- Simulation of factory environment
- Fast forward capability
  - With simplified AGV Models
- Configuration via Config Files
  - Robot speed
  - Starting battery level
  - Battery drain rate
  - Battery charge rate



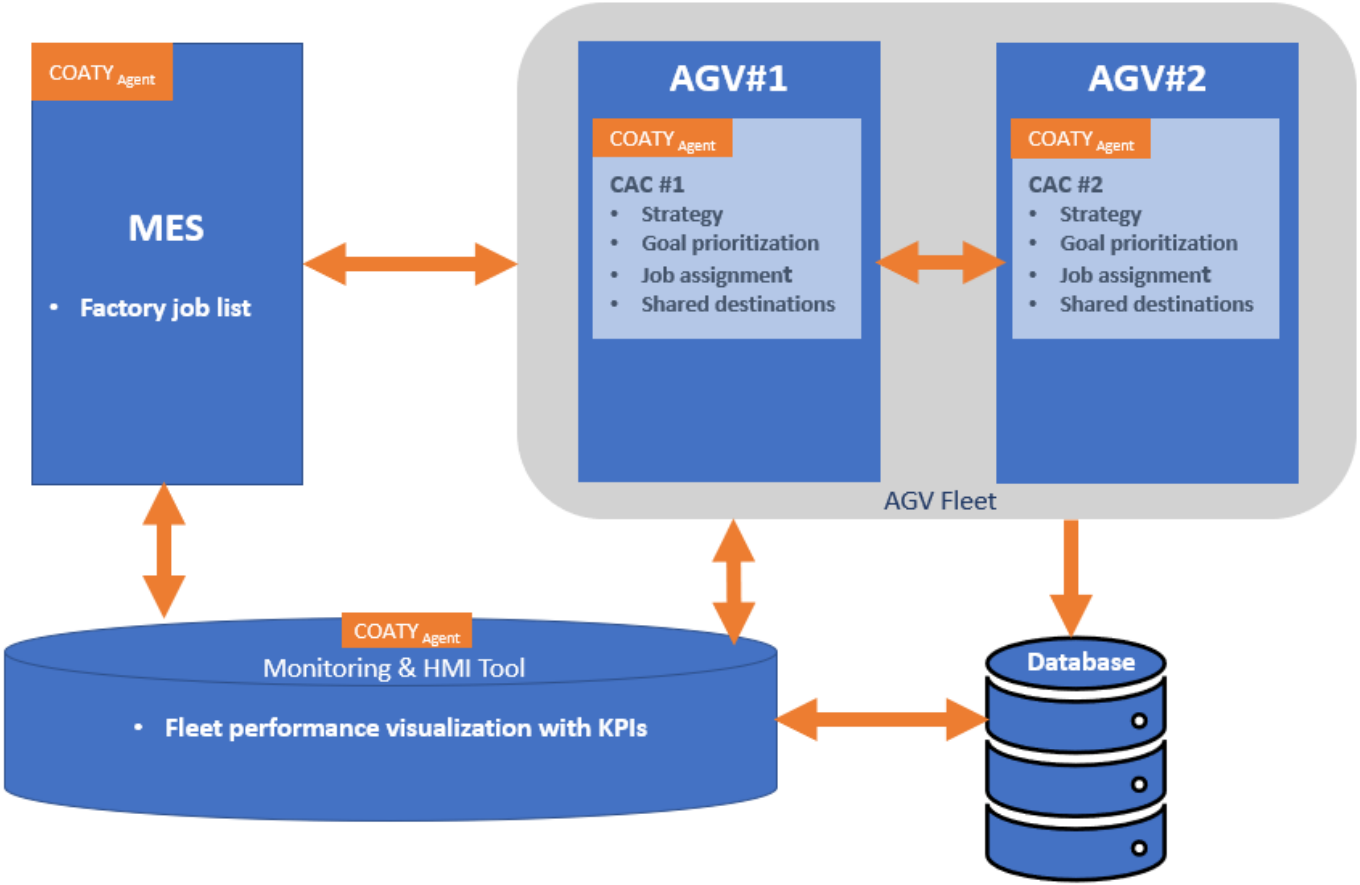
AGV Fleet on the Factory Floor

Achievements: Working System



AGV Fleet on the Factory Floor

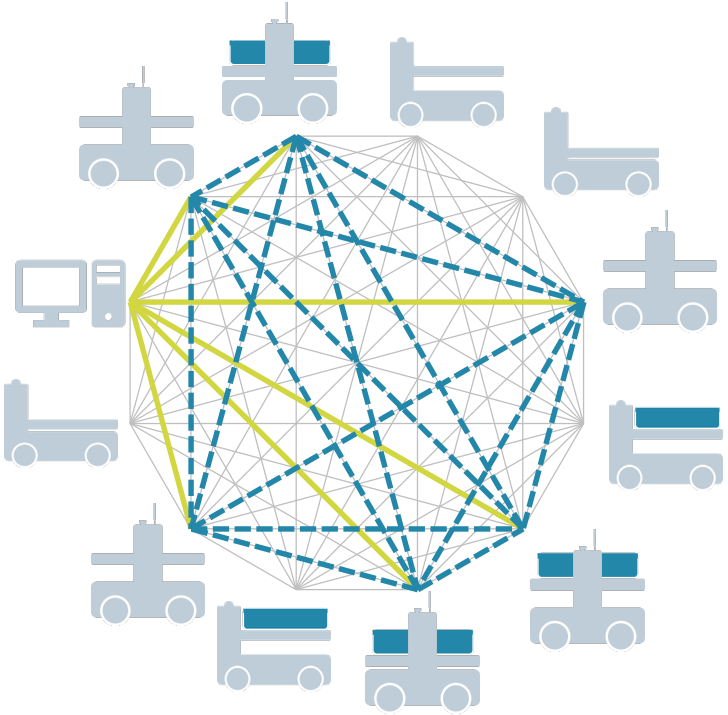
Achievements: Data Collection Architecture



AGV Fleet on the Factory Floor

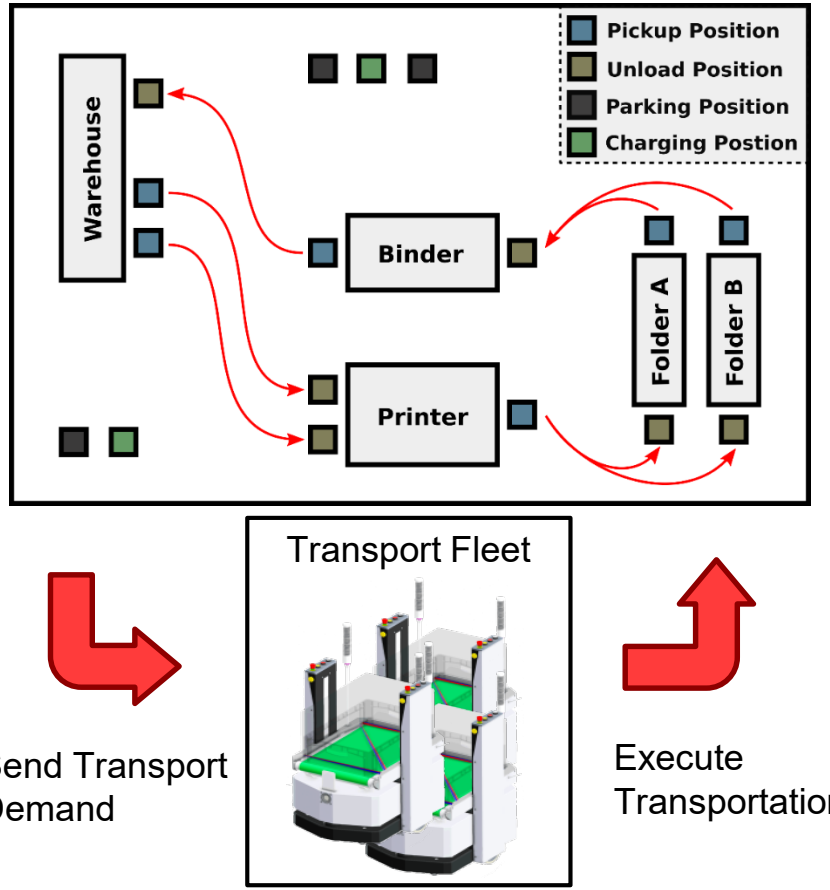
- **Implementation of Interface for real world Traces & other Simulator input**

- Coaty
  - Publish/Subscribe
  - Loose coupling of Agents
  - Communication via Coaty Objects



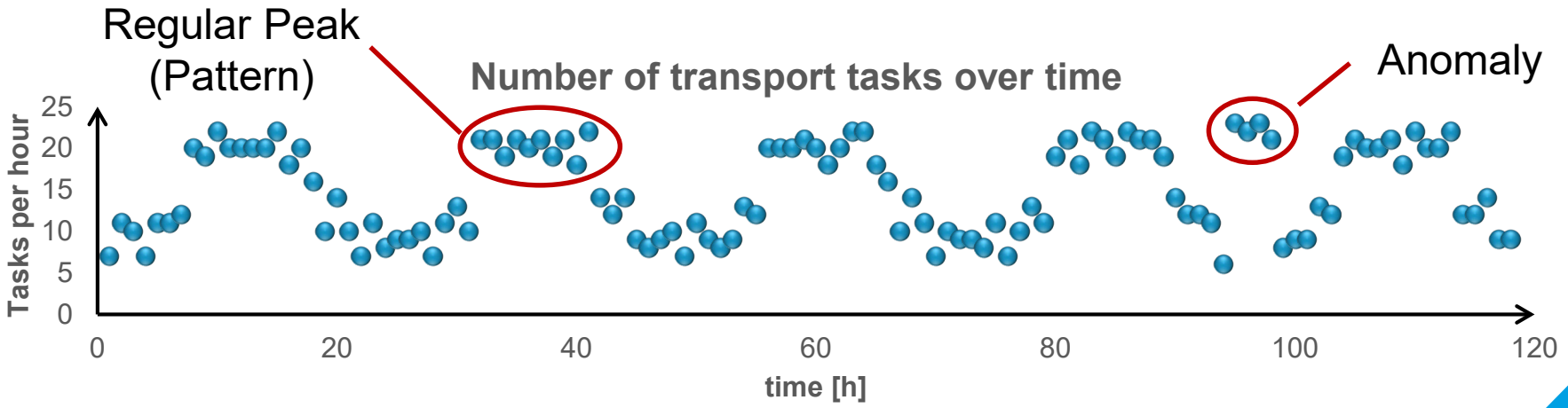
Optimization of Fleet Behaviour

AGVs on the Factory Floor



- Usage of the before presented simulation to support the optimization and resilience of the AGV fleet
- Fleet context assumption:
  - Fleet is responsible for ongoing product delivery in factory supply chain
  - Fleet receives transport demands from factory to execute

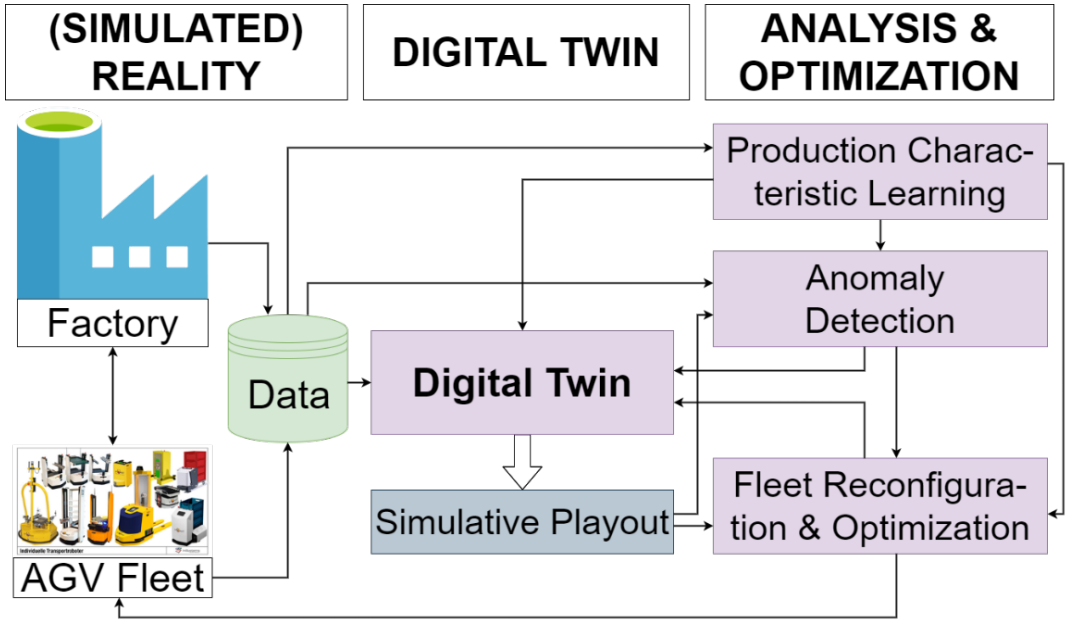
- Machines adhere to a regular production plan
  → Observed transport tasks follows some patterns
- Currently: AGVs are missing the capability to
  - Identify such patterns
  - Identify anomalies as pattern deviations
  - React and prepare accordingly



Optimization of Fleet Behaviour

Approach

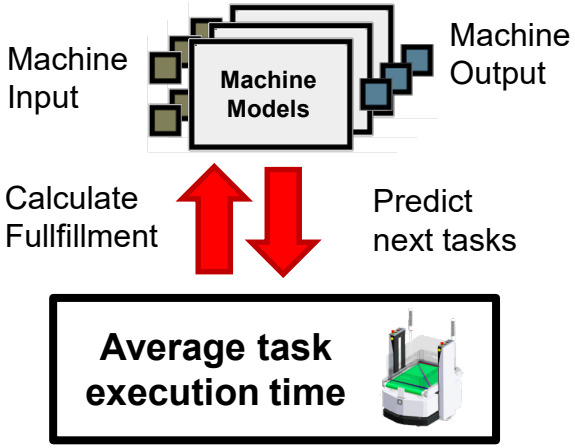
GOAL: Optimization of fleet behavior by adaption of the AGV fleet strategy (task assignment) to production dynamics and anomalies in the factory

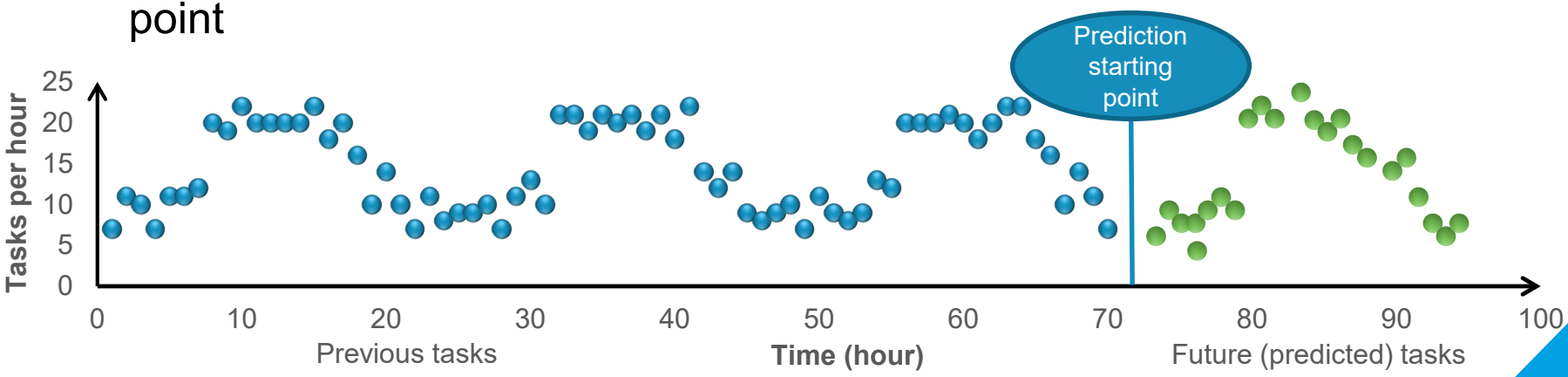


- PCL: Learn patterns of production dynamics in order to proactively adapt fleet configuration.
- AD: Detect deviation from (learned) regular patterns.
- FRO: Takes input from PCL & AD and uses DT to explore the best fitting fleet configuration as preparation for rollout.

Prediction Approach

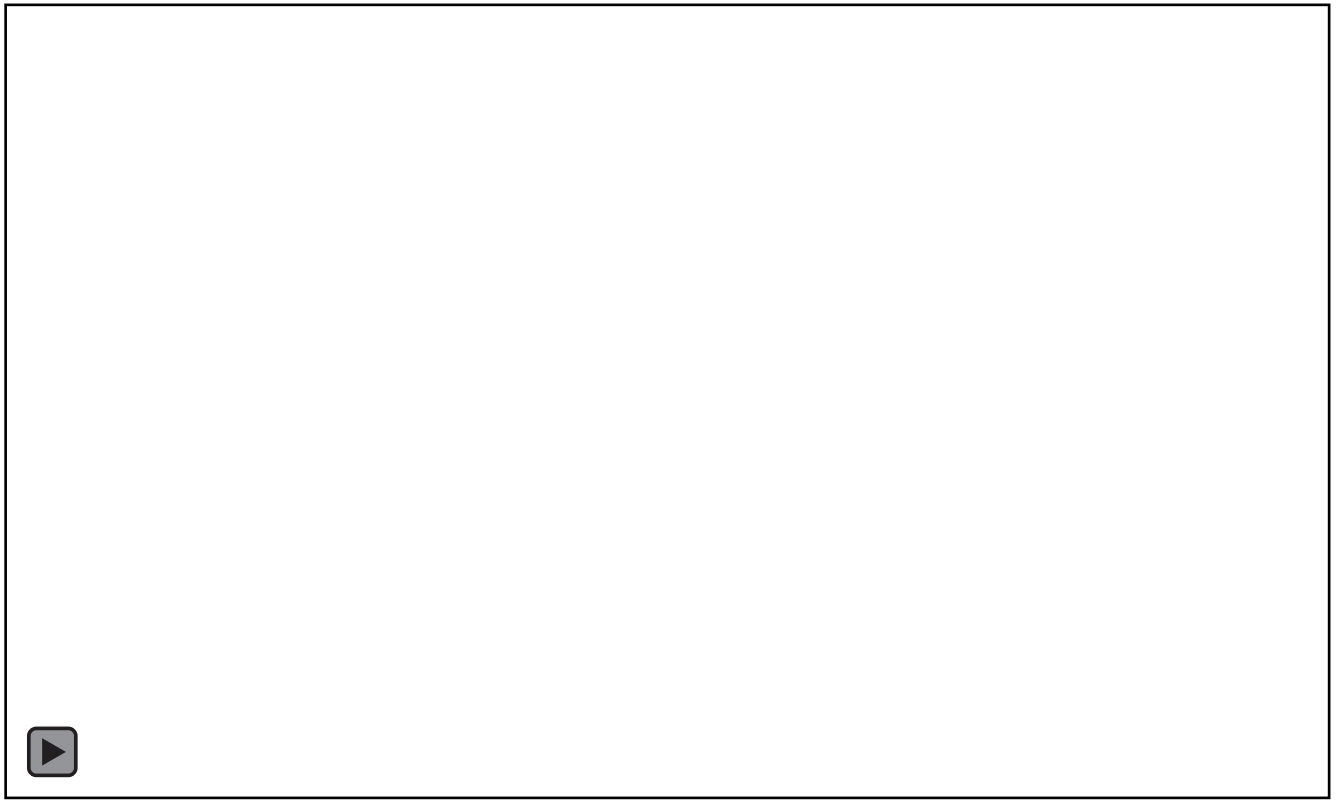
- Focus on I/O Behavior of Machines & Warehouses
- Train model for each machine that predicts requested tasks depending on machines inputs
- Predict future tasks at a dedicated starting point





Optimization of Fleet Behaviour

Process Anomaly Detection



Anomaly Detection:

- Predict future tasks for one day
- Use prediction as expected task amount (green line in animation)
- Identify anomalies as exceeding of warning limit

Optimization of Fleet Behaviour

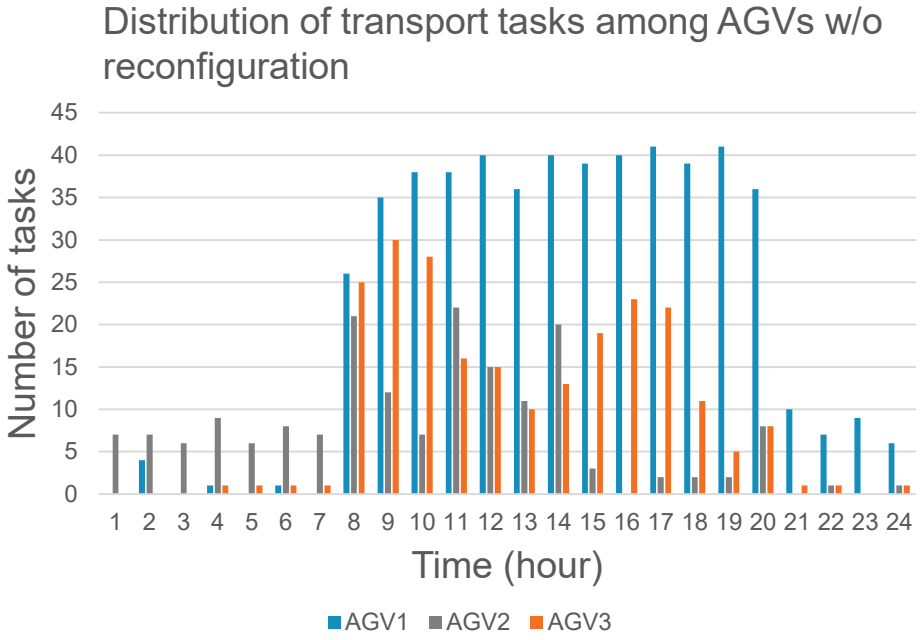
Reconfiguration Challenge

- Hazardous situations, e.g.
  - Regular events (predictable task peaks)
  - Irregular events (transport anomalies)
- Optimization fleet and improve resilience
  - Adapt fleet behavior – but how?

Challenge:

Which configuration optimizes fleet behavior in task assignment?

Example: Uneven Task Assignment!

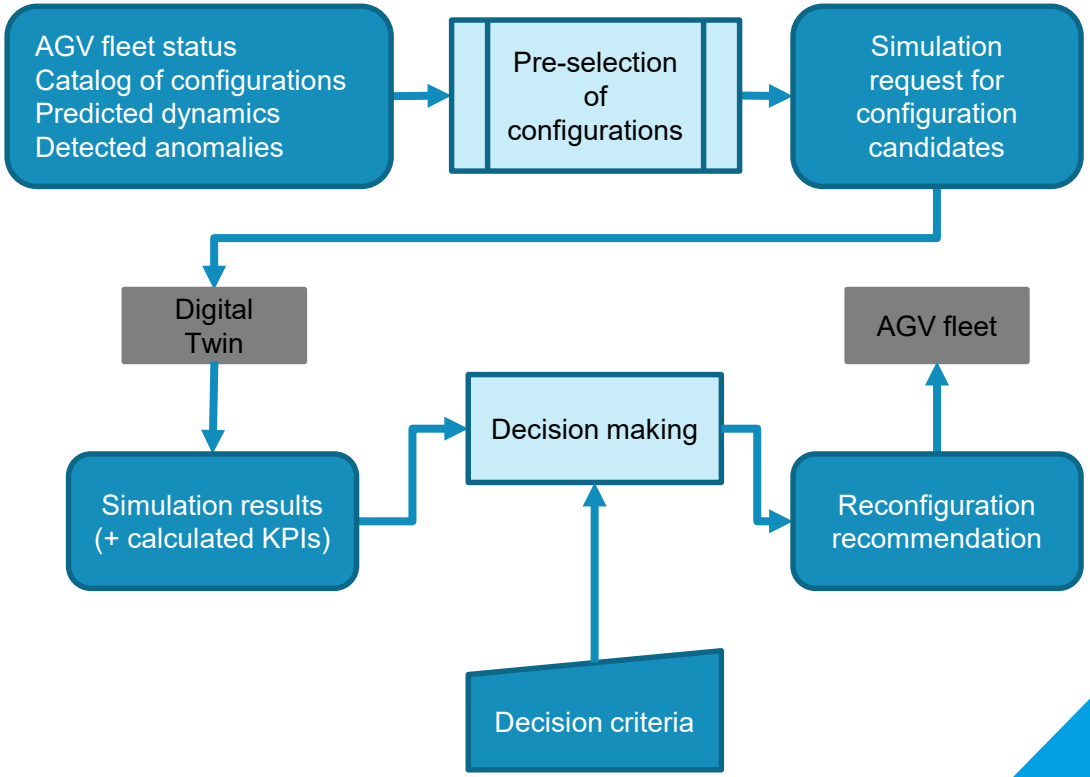


Optimization of Fleet Behaviour

Global Reconfiguration - Overview

- Pre-selection
  - Assessment of irregular causes
  - Constrain the candidates for task assignment strategies
- Simulate with DT
  - DT is faster than real time
  - Selected configuration candidates are applied
  - Get Fleet KPIs for every configuration
- Decision making
  - Calculation of weighted sum of KPIs
  - Weights are decided by experts
  - Multi-objective optimization
- Combination of configurations for time intervals

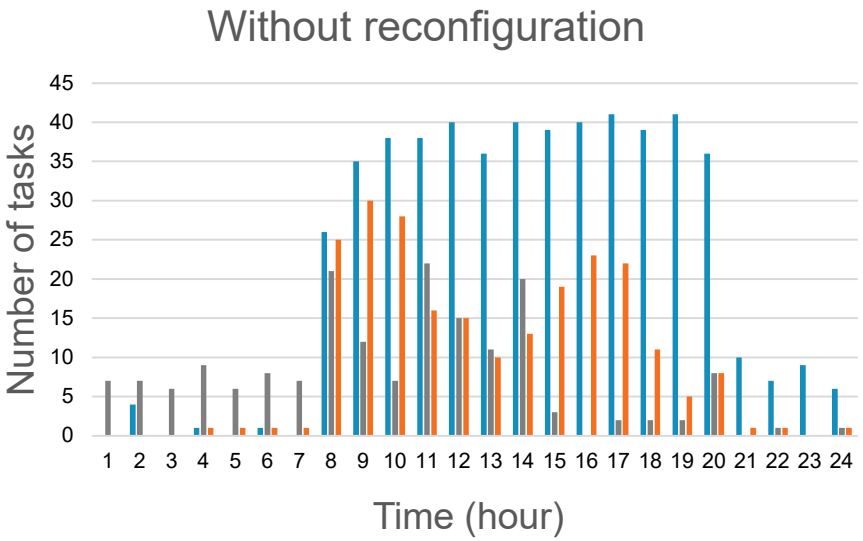
Best reconfiguration is played out to AGV fleet.

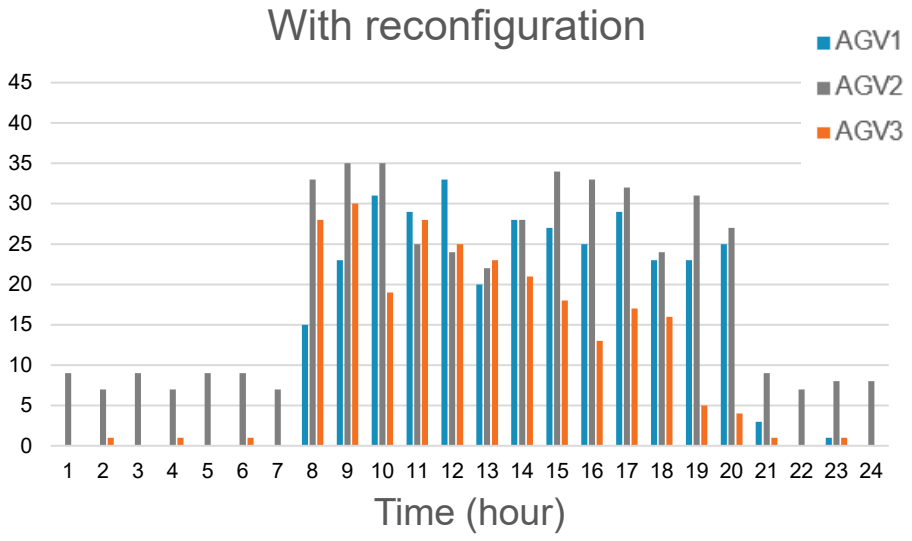


Example: KPIs valuation from simulation of AGVs as Digital Twin with pre-selected configurations

Optimization of Fleet Behaviour

Global Reconfiguration - Results





- Resulted improvements
  - 31.8% decrease in maximal difference in amount of driven distance
  - 43% decrease in maximal difference in length of local queues of robots
  - 42% decrease in maximal difference in finalized transport tasks

FoF resilience
Requirements

“Enable security analysis and Misuse-Case execution”

→ Capabilities in CPS Modelling

→ Representation in Cloud based Cyberrange

→ Modelling Attack scenarios

“Have the ability to detect and react on Misuse-Cases”

→ Capabilities in H/M Behavior Watch & FoF Resillience

→ Development of Detection methods

→ Demonstration of Detection, incident handling and reaction

CYBER FACTORY NO.1 CF#1

CPS Modelling & Digital Twins

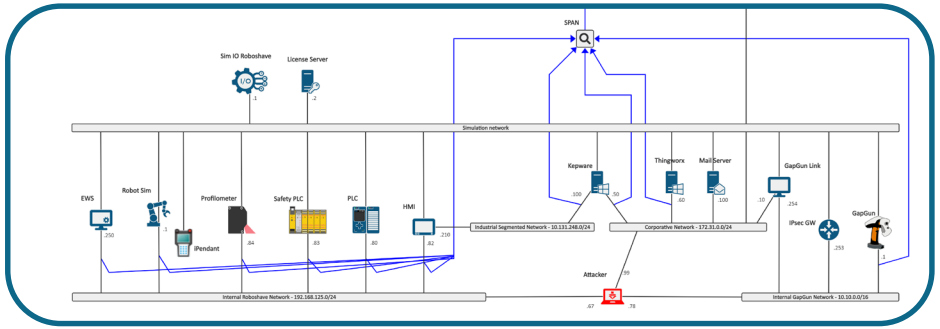
- Improve process quality
- Training area for operators
- Predictive maintenance
- Pre-production test area for updates
- Waste reduction and energy efficiency
- Cybersecurity assessment

Safety Security Sustainability

CyberRange
An Airbus tool to simulate IT/OT environments

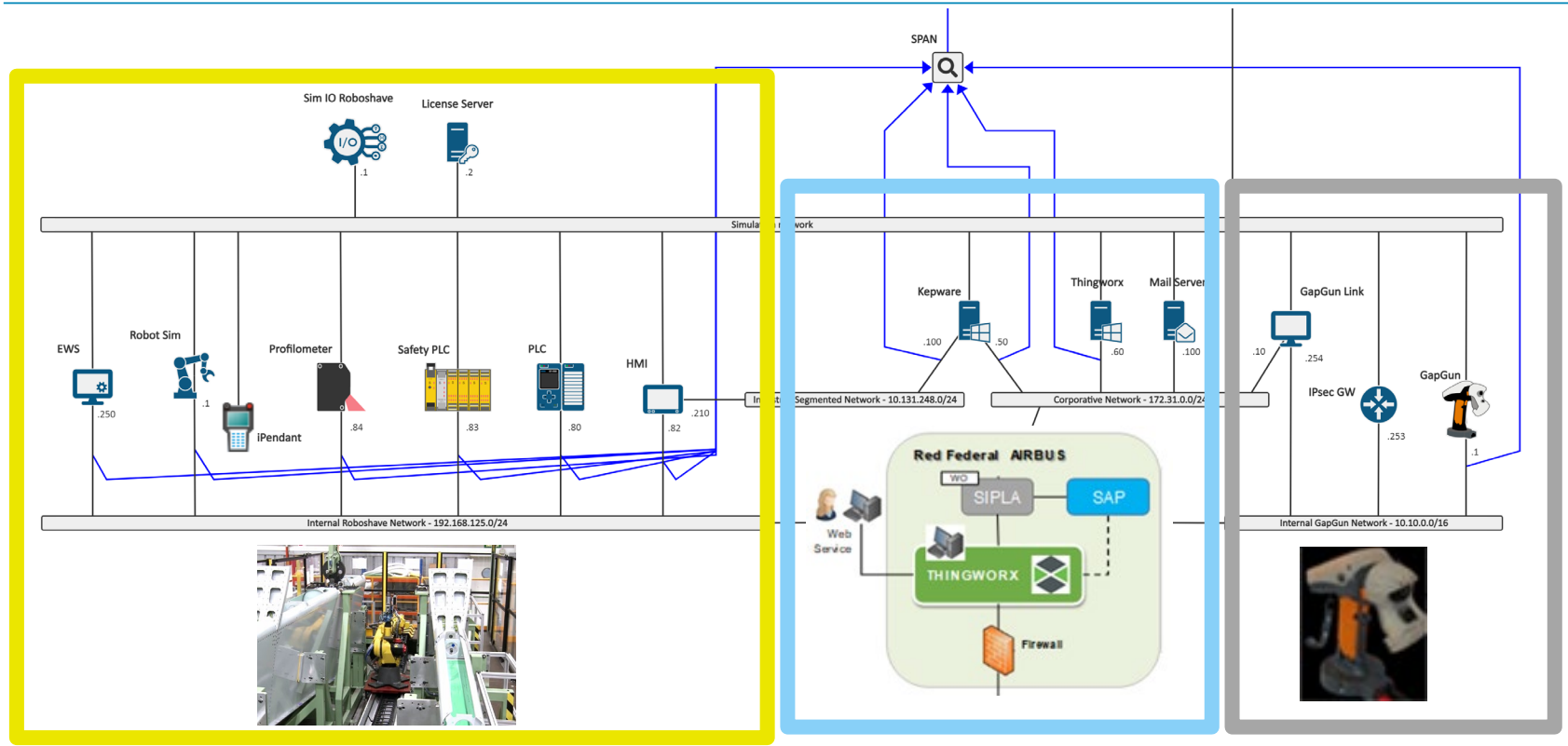
CPS Modelling & Digital Twins

AIRBUS Cyber Range

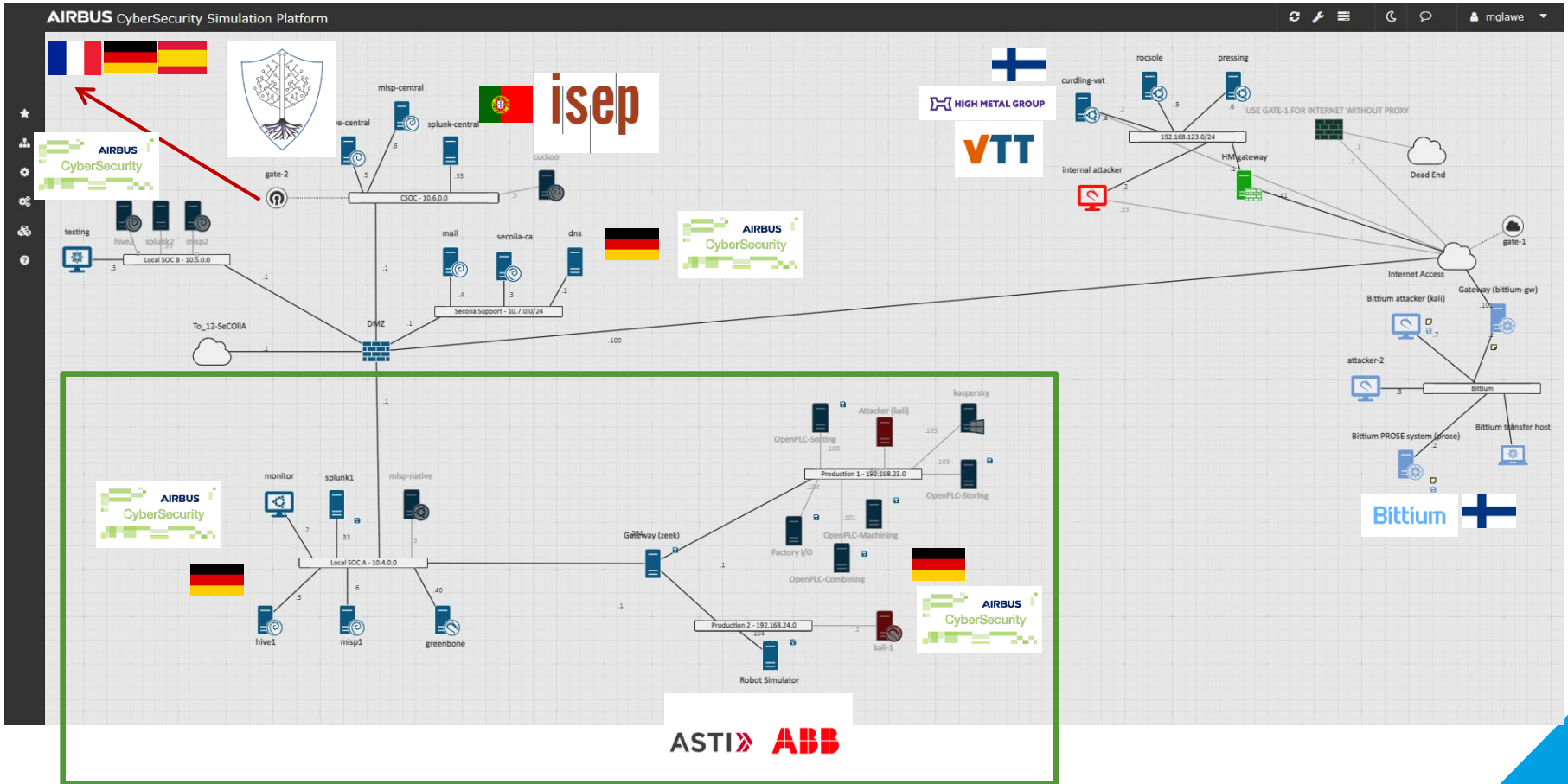


Digital Twin in CyberRange

CPS Modelling & Digital Twins



Digital Twin in CyberRange
Using the Cloud Platform



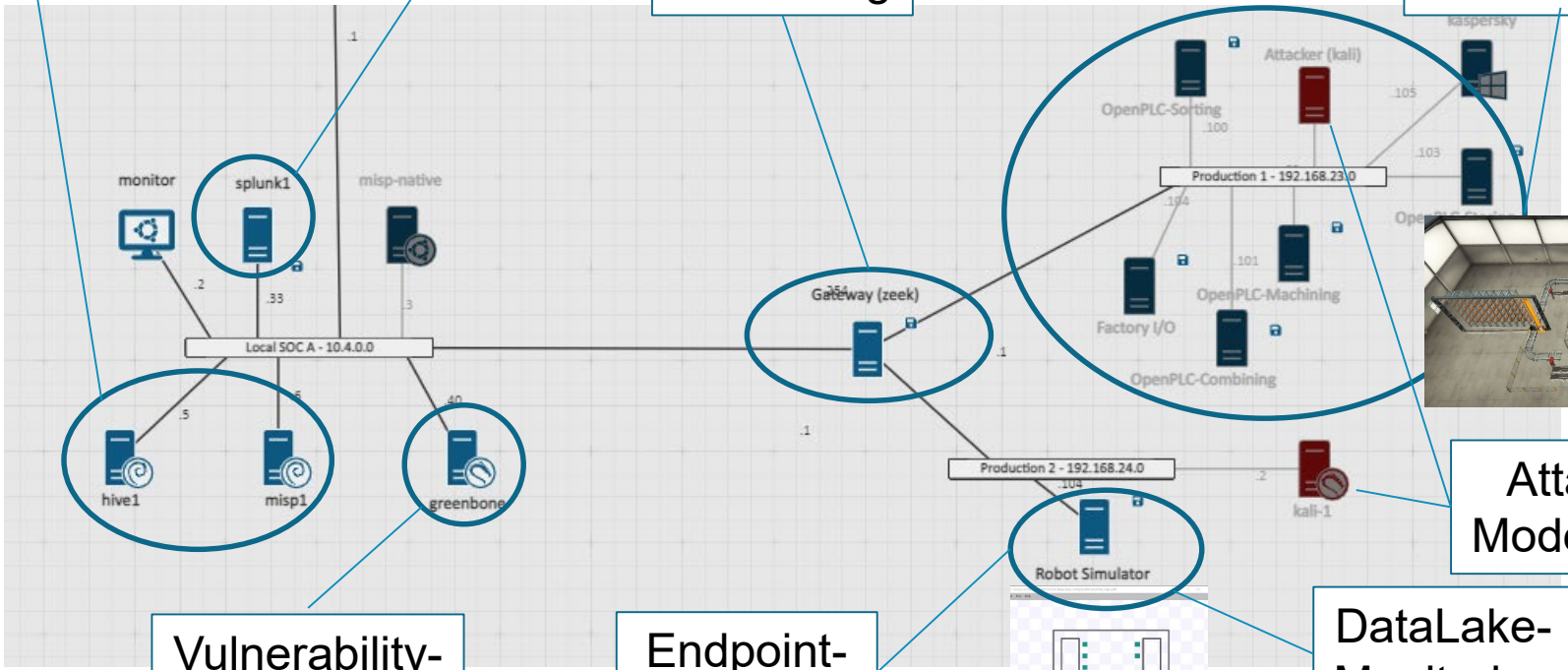
FoF resilience
Digital Twin in CyberRange

SOC

SIEM

NW-Monitoring

Factory Environment



Attack Modelling

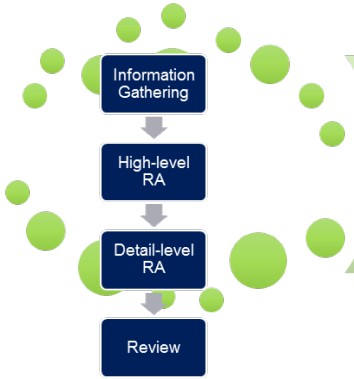
Vulnerability-Scanner

Endpoint-Monitoring

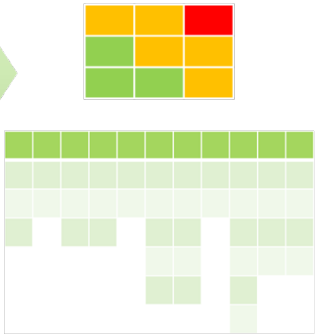
DataLake-Monitoring

"A misuse case is simply a use case from the point of view of an actor hostile to the system under design."

Risk Assessment to UC



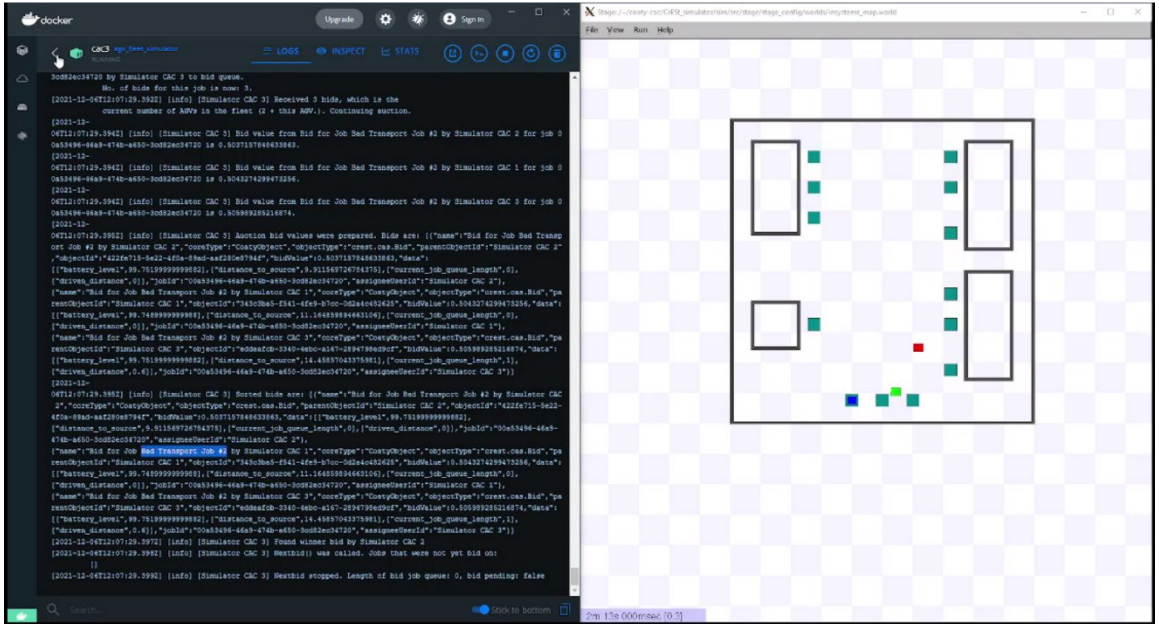
Attacker definition and staging



Find Mitigations and Limitations

Complete definition

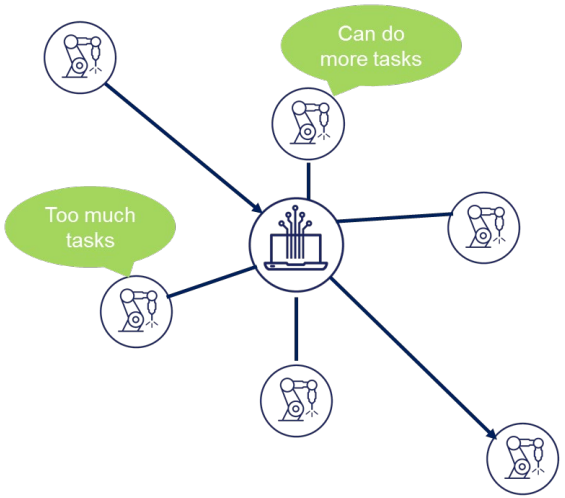
- Assumptions:
  - Attacker gained acces to the robot network
  - Attacker corrupted one robot or deployed a rogue device



“Enable security analysis and Misuse-Case execution”
→ Capabilities in CPS Modelling
→ Representation in Cloud based Cyberrange
→ Modelling Attack scenarios

“Have the ability to detect and react on Misuse-Cases”
→ Capabilities in H/M Behavior Watch & FoF Resillience
→ Development of Detection methods
→ Demonstration of Detection, incident handling and reaction

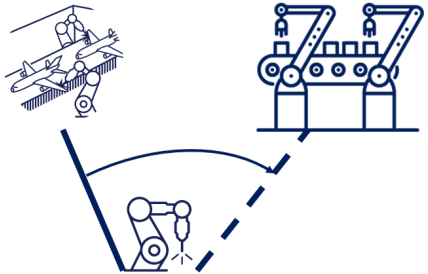
Dynamic Systems



Interconnection

Cobotics

Modular Production



FoF resilience

CAP53
Human/Machine Behavior Watch

All inter-machine communication at the platform tier (relevant for covering the Use Cases or detecting the Misuse Cases) shall be monitored.

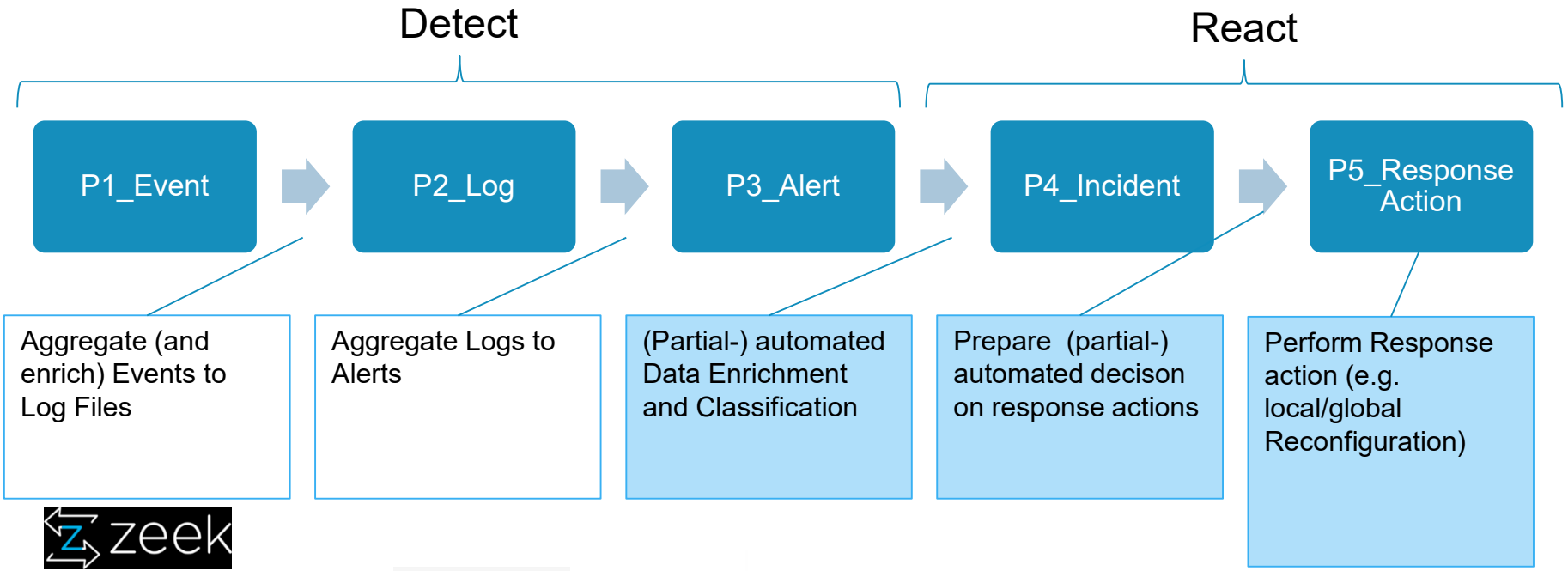
The deployed data acquisition mechanisms shall ensure a full coverage of all data sources (relevant for covering the Use Cases or detecting the Misuse Cases).

CAP54
Cyber-resilience mechanisms

Seamless integration of the monitoring services with state-of-the-art SIEM solutions shall be ensured.

It shall be ensured that the deployed monitoring services (relevant for covering the Use Cases or detecting the Misuse Cases) are able to understand and work with all present communication protocols, especially the ones used at the edge tier.

FoF resilience
Conceptual Process



zeek
OpenVAS
Open Vulnerability Assessment Scanner
MySQL
ROS
splunk>
TheHive

monitor - Google Chrome

heracles.cyberrange.cloud/console.html#id=2ca01ffa-4f28-423a-9603-2af88e59d967&wz=wz-04

Remote console - monitor

Clipboard | Fullscreen | 2133 x 1036 | Shortcut Keys | English (en-US)

Activities | Firefox Web Browser | Thu 12:29

Intrusion detection | Search | Splunk 7.3.0 | Search | Splunk 7.3.0 | TheHive - Organisati | Cortex | Request error: from | github.com/TheHive- | DNS-RPZ - Cortex Ne | /registry-1.docker.io/ | Greenbone Security

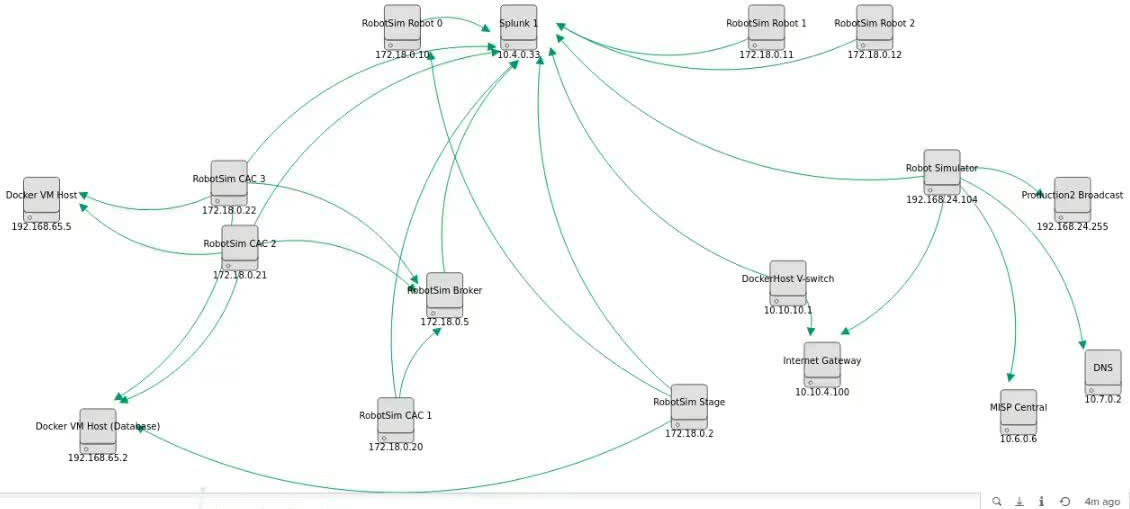
splunk1.secoiia.corp:8000/en-US/app/airbus_app_demo/zeek

SOC A | SOC B | SOC C | Central SOC | Triggered Alerts - Spl... | Other Bookmarks

Communicating endpoints

Highlight node

whitelisted connection



Communicating endpoints

Device IP address	Classification
10.10.10.1	DockerHost V-switch
172.18.0.2	RobotSim Stage
172.18.0.5	RobotSim Broker

Connections by volume

4m ago

Videos | Research & Innovatio... | Robot Simulator - Go... | monitor - Google Chr... | C:\Users\Christian\D... | Settings

U: 0.02 Mbit/s D: 0.66 Mbit/s | Desktop | 12:29 12.05.2022

- Partially automated data aggregation
  - Reduce time until detection
  - Reduce necessary resources especially in data aggregation
- Utilization of Non-Security Data Sources in anomaly detection
  - Gain Holistic view
  - Necessary to define whether anomalies are malicious
- Testing and development of detection capabilities based on a Digital Twin and simulates Misuse-Cases
  - Development of detection capabilities in parallel to Use-Case development
  - Adopted detection patterns using Use-Case Know-How

SUMMARY & Questions

Digital Twins can support Development, Resilience and Operation

Open Interfaces and Adoptability are core for multi-purpose usage