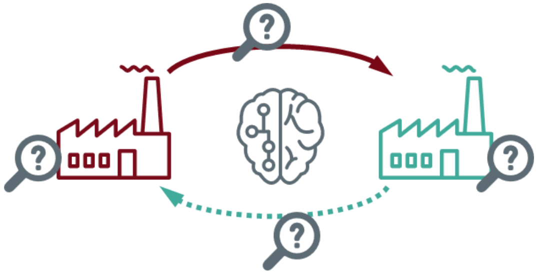
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

COMPUTER SECURITY APPLICATIONS OF IIOT DIGITAL TWINS FOR THE NUCLEAR SECTOR



David Allison and Paul Smith
{firstname.lastname}@ait.ac.at

Centre for Digital Safety and Security

BMK

1.400 employees

7 Centers

Austria's largest RTO

Infrastructure Systems

System Competence

Applied Research

Federation of Austrian Industries (through VFFI)

Next Generation Solutions

4 Subsidiary Enterprises

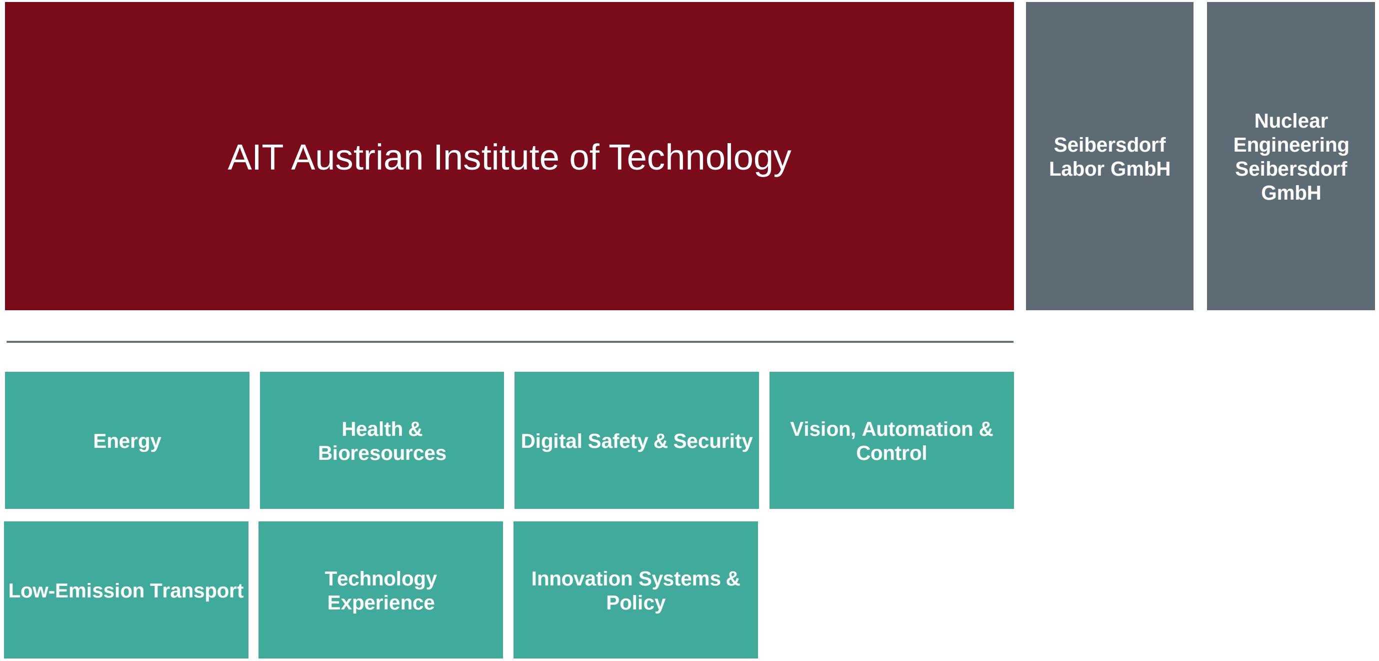
LKR, NES, SL, Profactor 51%

165 m EUR total revenue

Tomorrow Today

as of YE 2020

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



AIT Austrian Institute of Technology

Seibersdorf Labor GmbH

Nuclear Engineering Seibersdorf GmbH

Energy

Health & Bioresources

Digital Safety & Security

Vision, Automation & Control

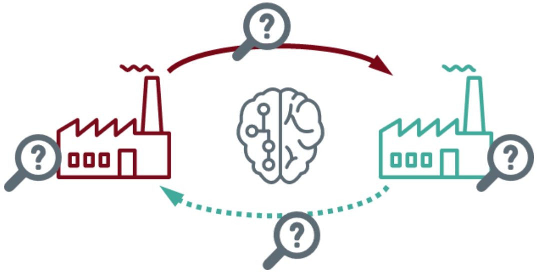
Low-Emission Transport

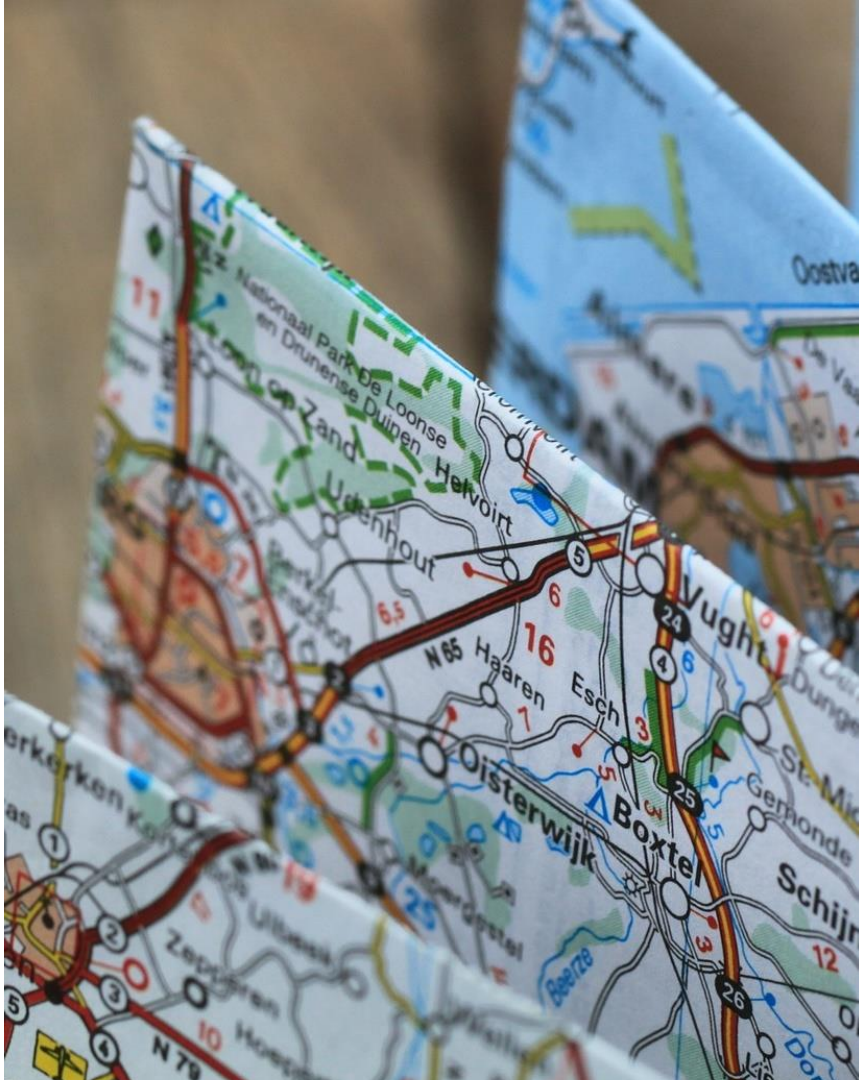
Technology Experience

Innovation Systems & Policy

TALK OUTLINE

- What is a digital twin, including common applications?
- A word on the computer security *of* digital twins
- Applications of digital twins to computer security activities

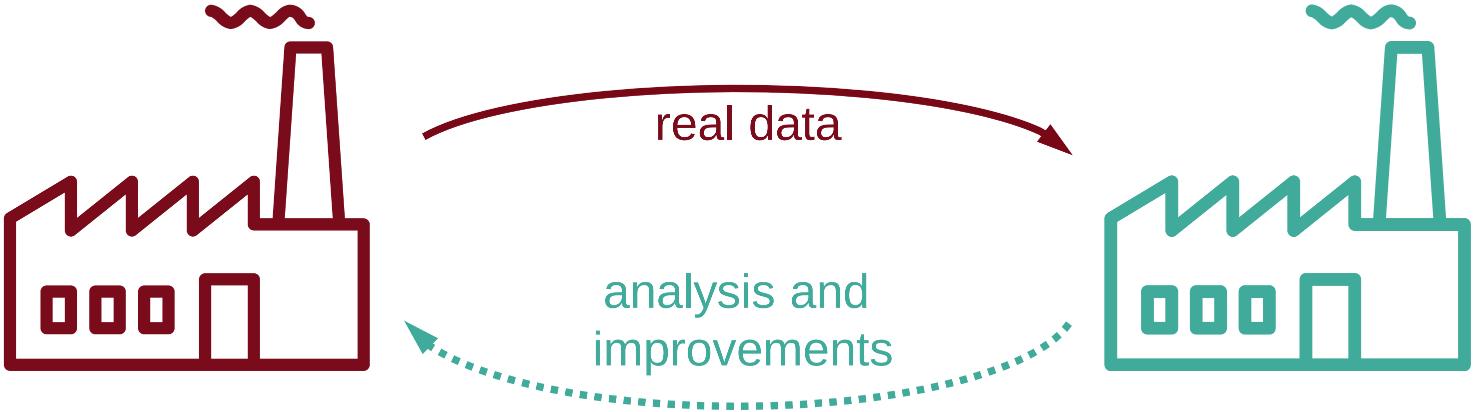




WHAT IS A DIGITAL TWIN

The definition of a **digital twin** has not yet been standardised

Generally speaking, a digital twin is a **virtual representation** of a **real-world system** that uses **real data** for **analysis and improvements**



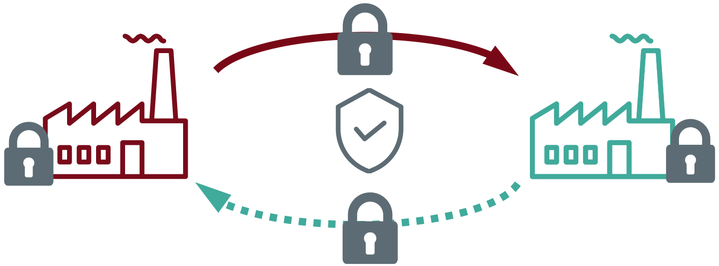
COMMON APPLICATIONS OF DIGITAL TWINS

Common applications for digital twins include:

- Predictive Maintenance
  - calculating when a physical component needs to be replaced/repaired *before* a failure occurs
- Product Design
  - race car aerodynamics design for better handling, more speed, etc
- State Estimation
  - predicting when a physical process may become unstable or dangerous
- Increasing Process Efficiency
  - modelling existing processes to identify bottlenecks

COMPUTER SECURITY OF DIGITAL TWINS

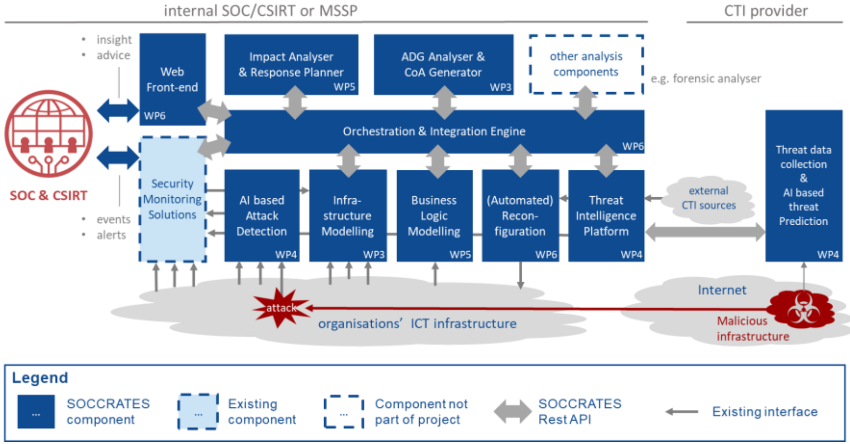
- Ensuring the computer security of digital twins is a concern
- Concerns include the theft of intellectual property
  - In the nuclear domain, theft of sensitive nuclear information could be a concern
- One can think of a digital twin as a potentially highly-distributed control loop; therefore, they are potentially susceptible to the same cyber-attacks as control systems
  - (Stealthy) False data injection attacks
  - Control command manipulation
  - Model and data integrity manipulation
  - …
- There are several computer security solutions that can be applied to address these risks



COMPUTER SECURITY RISK ASSESSMENT

- Determination of risk is typically calculated as risk = likelihood x impact
- Digital twins can be used to provide quantitate insights into these aspects

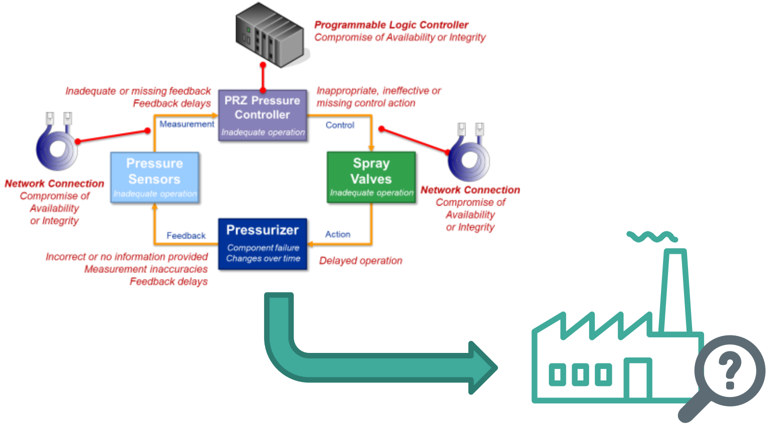
Likelihood


internal SOC/CSIRT or MSSP
CTI provider
insight
advice
events
alerts
SOC & CSIRT
Web Front-end WP6
Impact Analyser & Response Planner WP5
ADG Analyser & CoA Generator WP3
other analysis components
e.g. forensic analyser
Orchestration & Integration Engine WP6
Security Monitoring Solutions
AI based Attack Detection WP4
Infra-structure Modelling WP3
Business Logic Modelling WP5
(Automated) Recon-figuration WP6
Threat Intelligence Platform WP4
external CTI sources
Threat data collection & AI based threat Prediction WP4
Internet
attack
organisations' ICT infrastructure
Malicious infrastructure
Legend
... SOCCRATES component
... Existing component
... Component not part of project
SOCCRATES Rest API
Existing interface

SOCCRATES
SOC & CSIRT Response to Attacks & Threats
based on attack defence graphs Evaluation Systems

Impact

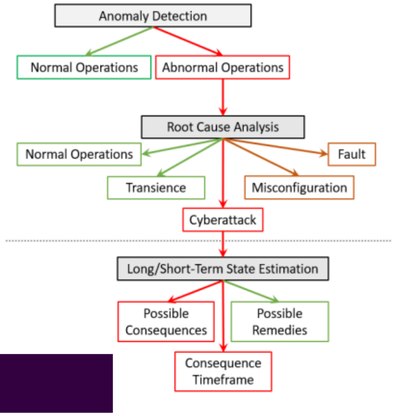
Hazard Analysis (e.g. with STPA)



Consequence analysis with a digital twin

DECISION SUPPORT FOR INCIDENT RESPONSE

- Digital twins can be used to support cyber-physical incident response workflows
  - Anomaly Detection
    - Is everything operating normally?
  - Root Cause Analysis
    - What is the cause of abnormal operations?
  - State Estimation
    - What if questions



Anomaly Detection

Normal Operations

Abnormal Operations

Root Cause Analysis

Normal Operations

Fault

Transience

Misconfiguration

Cyberattack

Long/Short-Term State Estimation

Possible Consequences

Possible Remedies

Consequence Timeframe

Level	Example Questions
1. Association	What is the root cause of this event?
2. Intervention	What if I change my firewall?
3. Counterfactuals	Was it the new policy that caused the security breach?

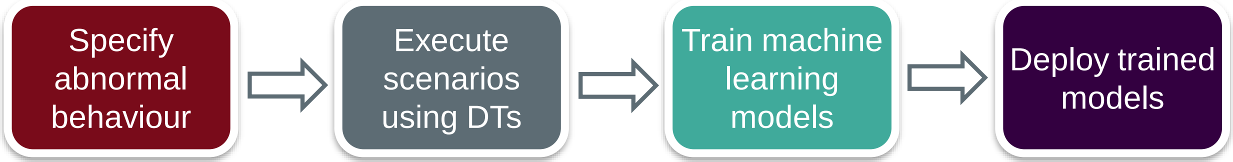
Source: Judea Pearl

MACHINE LEARNING MODEL TRAINING

- It may be desirable to use machine learning models to classify the observed behaviour of a target system
    - For example, classify attack types, abnormal system states, …

- Challenge: there are not an abundance of data that can be used to train models that classify rare behaviour

- Digital twins can be used to train such models



Specify abnormal behaviour → Execute scenarios using DTs → Train machine learning models → Deploy trained models

- Machine learning techniques, such as transfer learning and Few Shot Learning (FSL) could help

COMPUTER SECURITY TRAINING

- Enables computer security training and exercises on representative systems without operational risks
- The Asherah Nuclear Simulator (ANS) develop as part of IAEA CRP J02008 has been used for several exercises
- A major challenge is developing models that are robust to simulated cyber-attacks and integrating models with representative hardware

IAEA ITC ROK (2019)

CONCLUSION

- Digital twins are becoming an increasingly significant technology for non-security applications
  - Benefit could be had by applying them to computer security

- In many cases, these applications relate to decision support for various computer security processes
  - For example, secure design, risk assessment and management, incident response, training, ..
  - Can potentially provide more accurate and quantitative insights
  - Allow the execution of scenarios that would not be permitted or possible on real systems (e.g. to support model training and exercises)

- Value could be had by considering the relationship between digital twins and other emerging technologies (in the nuclear sector), such as Cloud, Industrial IoT, AI and Machine Learning, …

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

David Allison and Paul Smith

{firstname.lastname}@ait.ac.at

The work presented has been supported by the European Union's Horizon 2020 Research and Innovation program, under Grant Agreement No. 833481, and IAEA CRP J02008.