Safety and Security for Industrial Control Systems

Riccardo Ferrari, PhD

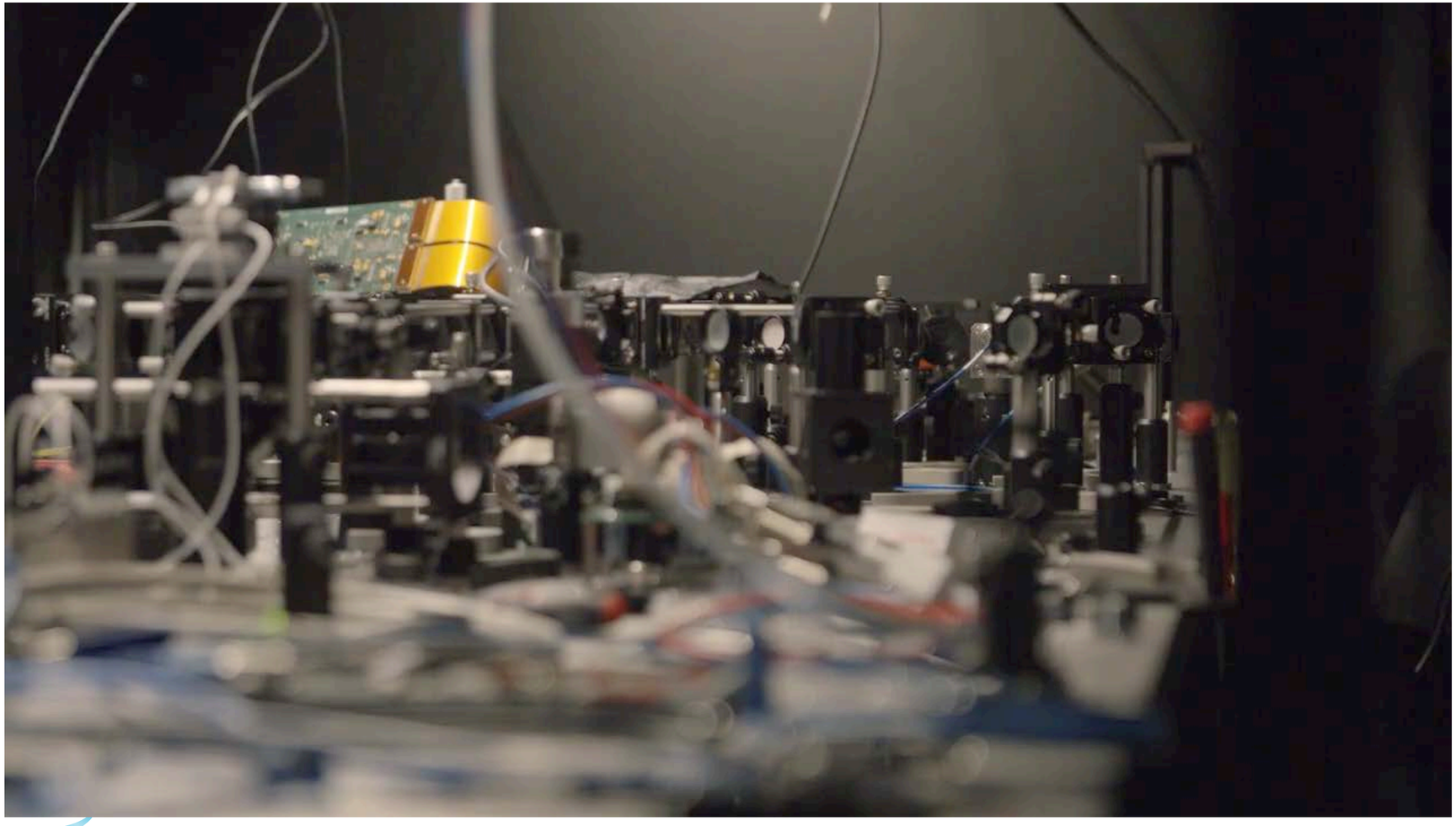
04/04/24

TU Delft

Who We Are

TU Delft

Delft Center for Systems and Control



https://www.youtube.com/watch?v=1KkDk0w6HL4

Staff

24 **Full Professors**
Associate Prof.
Assistant Prof.

ERC grantees

4

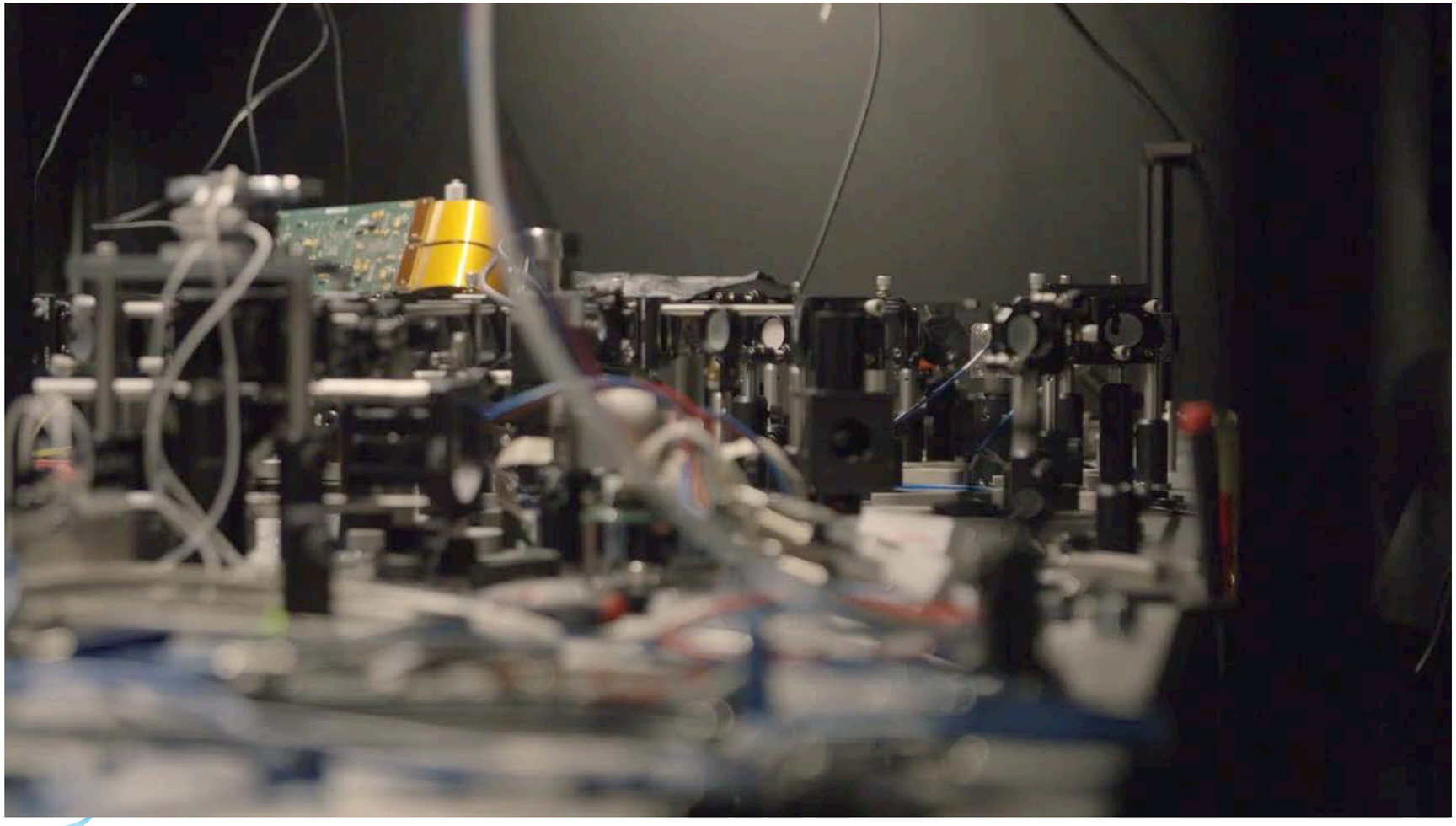
Postdocs

17

PhDs

75

Delft Center for Systems and Control



https://www.youtube.com/watch?v=1KkDk0w6HL4

Staff

24 **Full Professors**
Associate Prof.
Assistant Prof.

ERC grantees

4

Postdocs

17

PhDs

75

“Control is the hidden technology„

K.J. Astrom, Lund University

Safety and Performances require Control ...

https://youtu.be/REUE_XRzj0o?t=40

Safety and Performances require Control ...

https://youtu.be/REUE_XRzj0o?t=40

… AND EVEN BETTER, FAULT TOLERANT CONTROL

No Fault Tolerance

Fault Tolerance

… AND EVEN BETTER, FAULT TOLERANT CONTROL

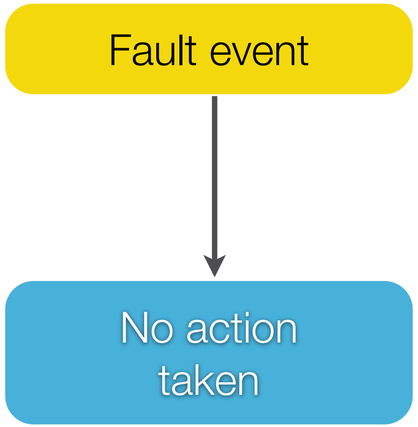
No Fault Tolerance

Fault event

Fault Tolerance

… AND EVEN BETTER, FAULT TOLERANT CONTROL

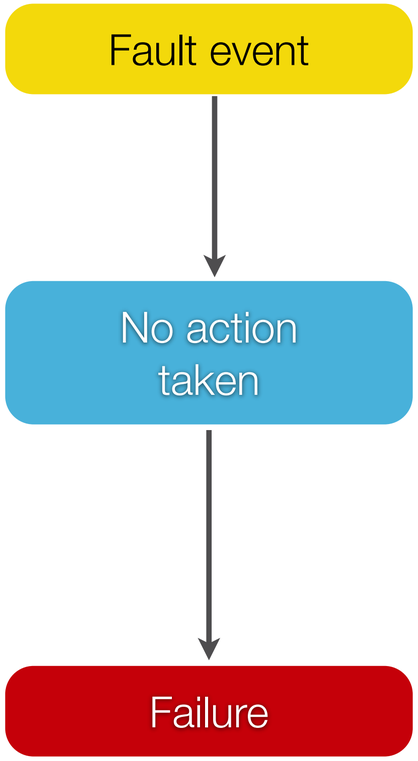
No Fault Tolerance



Fault Tolerance

… AND EVEN BETTER, FAULT TOLERANT CONTROL

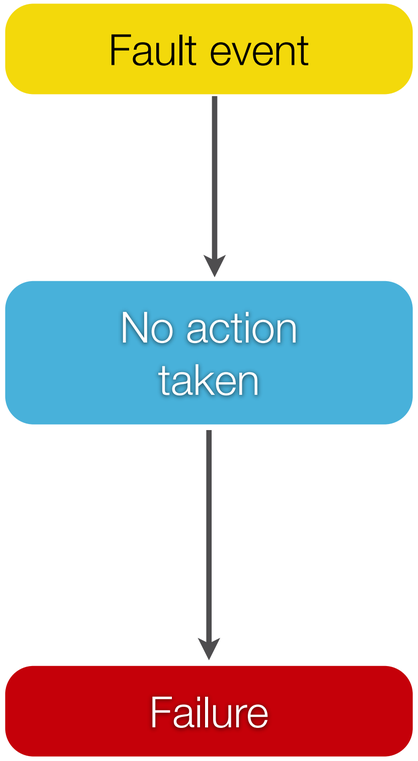
No Fault Tolerance



Fault Tolerance

… AND EVEN BETTER, FAULT TOLERANT CONTROL

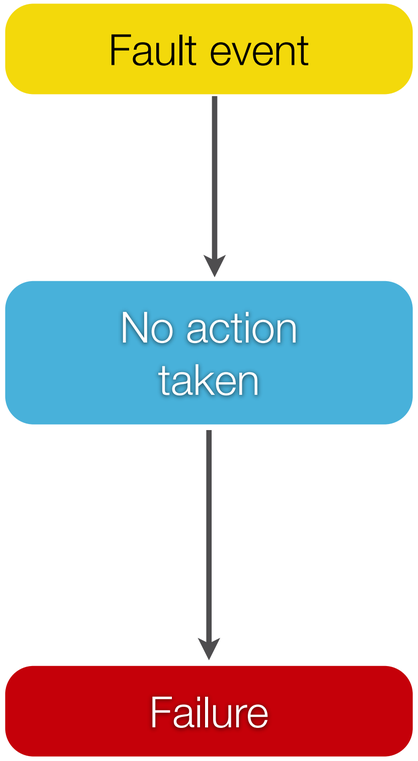
No Fault Tolerance



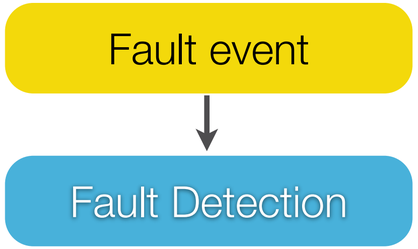
Fault Tolerance

… AND EVEN BETTER, FAULT TOLERANT CONTROL

No Fault Tolerance

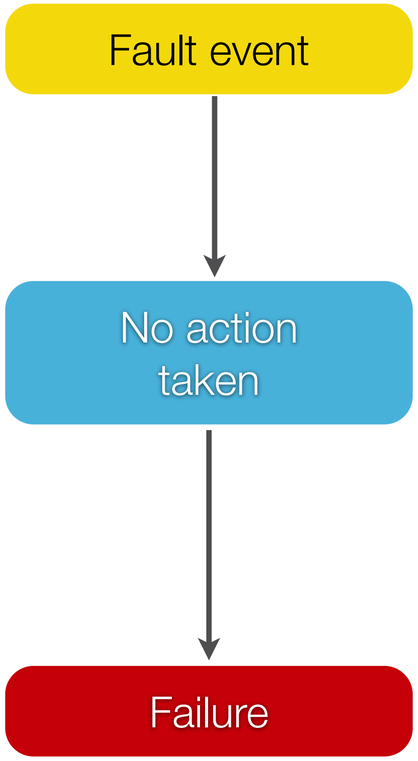


Fault Tolerance

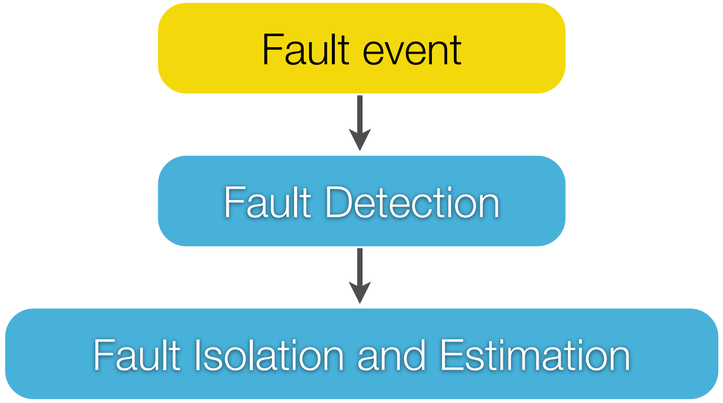


… AND EVEN BETTER, FAULT TOLERANT CONTROL

No Fault Tolerance

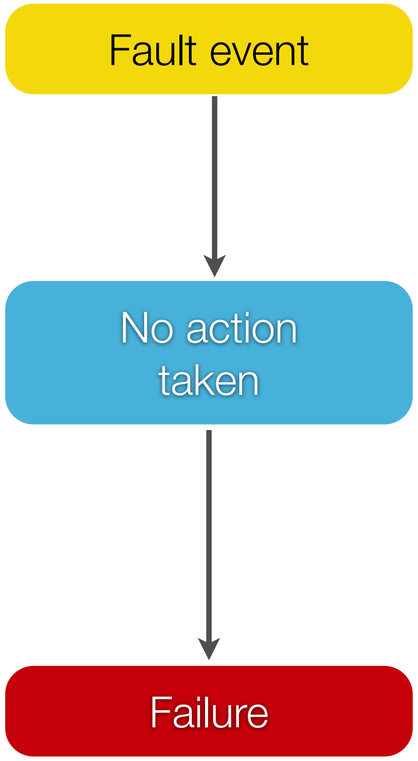


Fault Tolerance

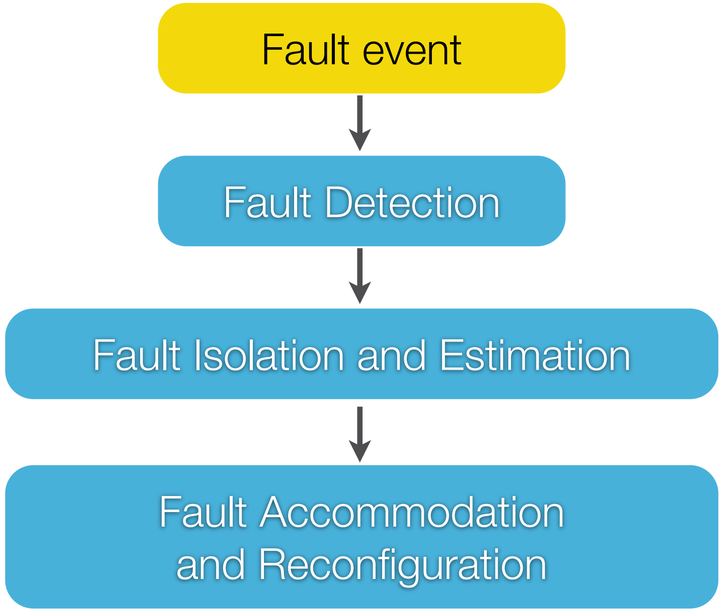


… AND EVEN BETTER, FAULT TOLERANT CONTROL

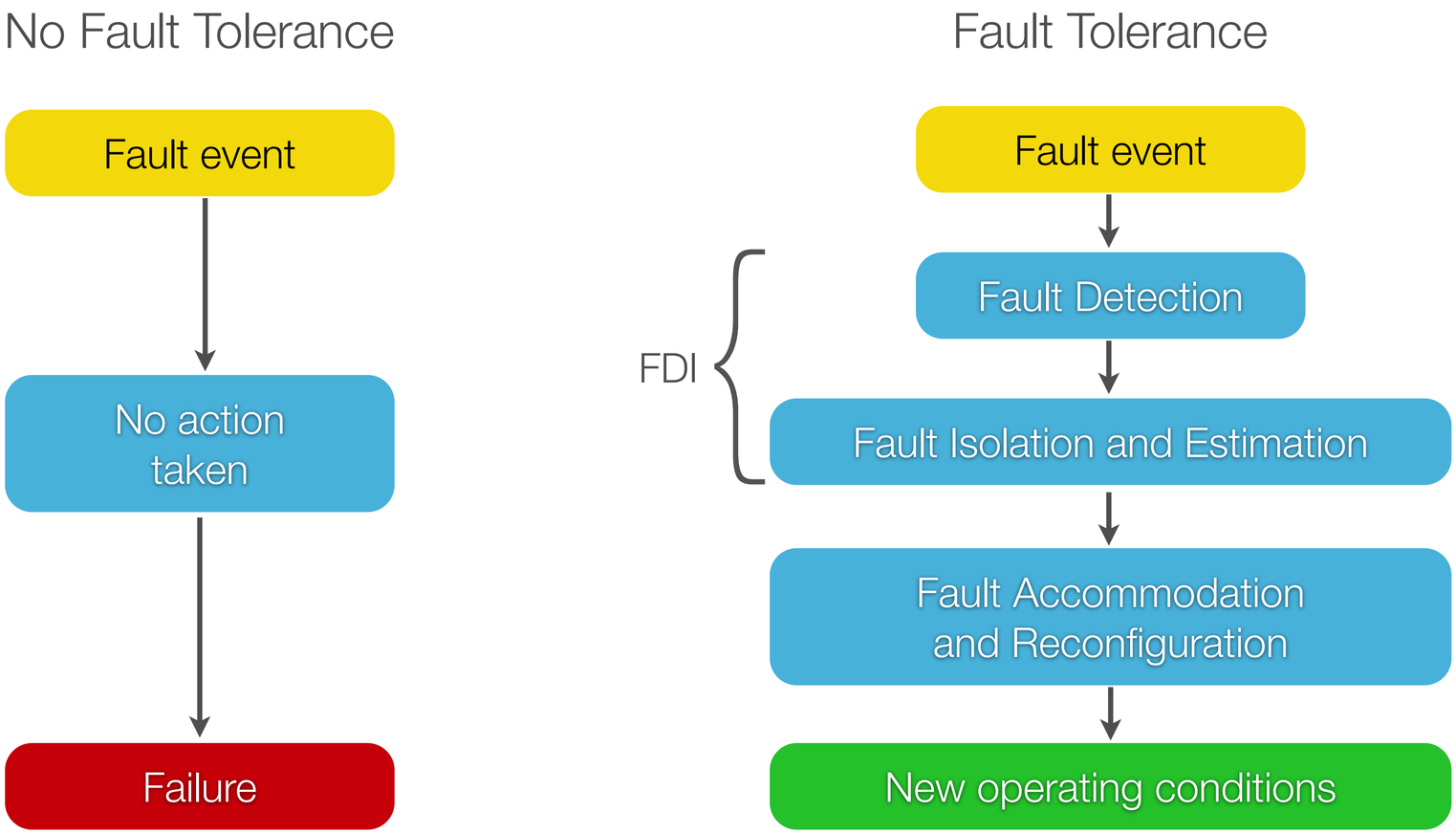
No Fault Tolerance



Fault Tolerance



… AND EVEN BETTER, FAULT TOLERANT CONTROL



The Fault Tolerant Control Group

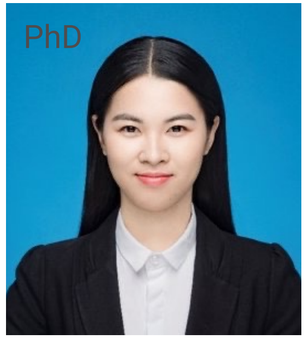

Riccardo

Alex

Wolfram

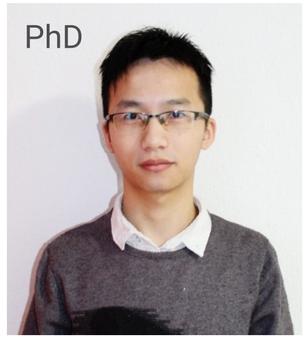
Luca

Jean

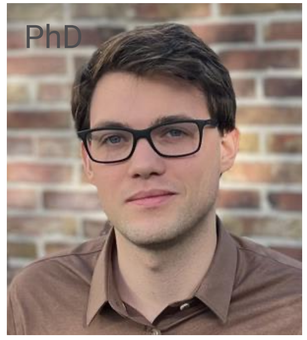


Zhixin

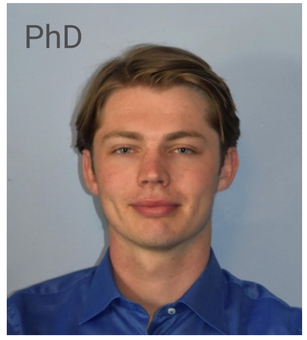
Tushar



Yang



Ivo



Bart

Staff

1 **Associate Prof.**

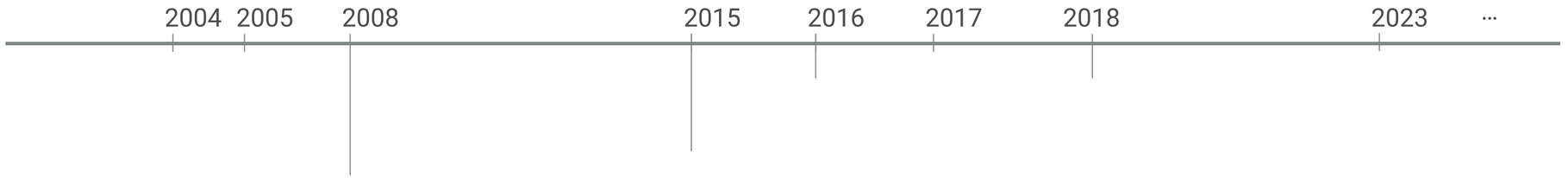
Postdocs

3

PhDs

6

My Visual CV



My Visual CV

Trieste, Italy
("Bora" wind topped 183 km/h in 2012)

MSc in Electronic Engineering

PhD

2004 2005 2008 2015 2016 2017 2018 2023 ...

My Visual CV

Trieste, Italy
("Bora" wind topped 183 km/h in 2012)

Buttrio, Italy
(my industrial period, in steelmaking)

My Visual CV

Trieste, Italy
("Bora" wind topped 183 km/h in 2012)

Buttrio, Italy
(my industrial period, in steelmaking)

Delft, Netherlands
(Max wind speed only 130 km/h)

R&D

MSc in Electronic Engineering | PhD | PostDoc | Assist. Professor in Fault Tolerant Control | Assoc. Prof.

2004 2005 2008 2015 2016 2017 2018 2023 ...

SURE (grant 707546)

Things I do while not working

Teaching children how to skate on ice

THINGS I DO WHILE NOT WORKING

Teaching children how to skate on ice

Angrily hitting snowflakes in a white pyjama (Aikido)

THINGS I DO WHILE NOT WORKING

Teaching children how to skate on ice

Angrily hitting snowflakes in a white pyjama (Aikido)

Hitting the piano with the entire family

What We Do

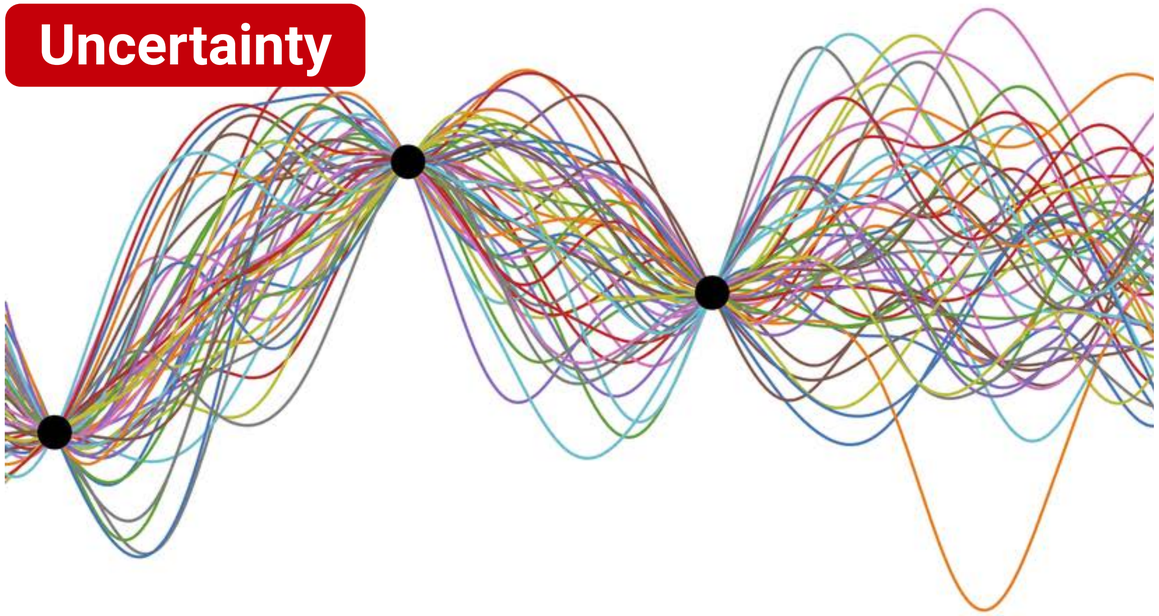
TU Delft


gettyimages
fStop Images - Caspar Benson
FO4305OZ02
104574303

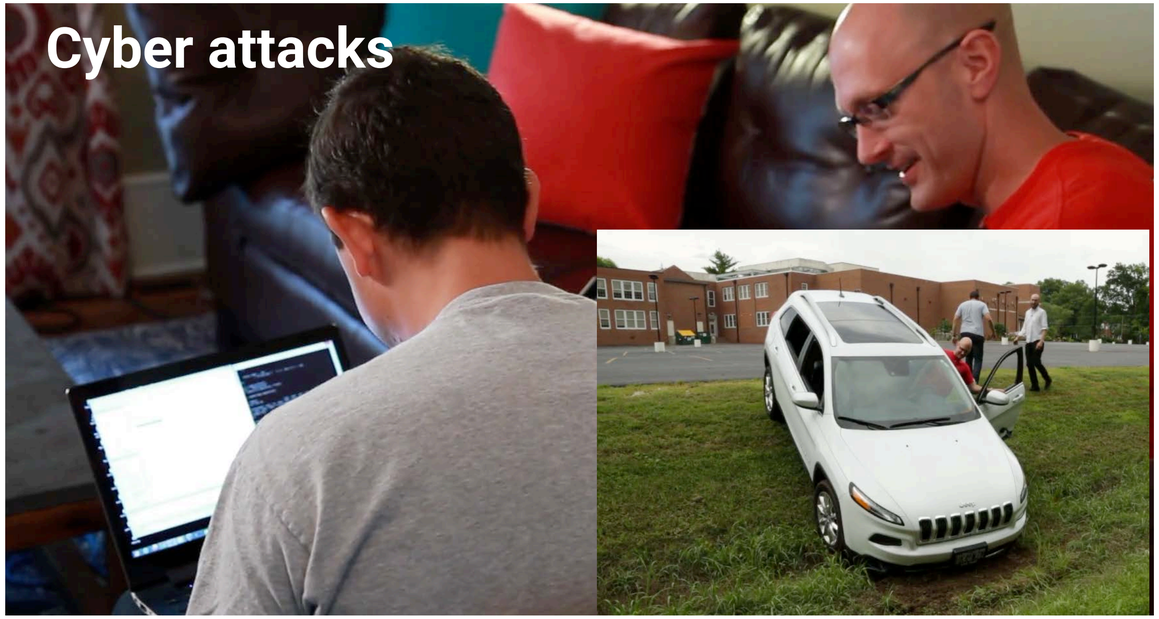
Motivation

Systems which must be designed for safety and resiliency


Faults

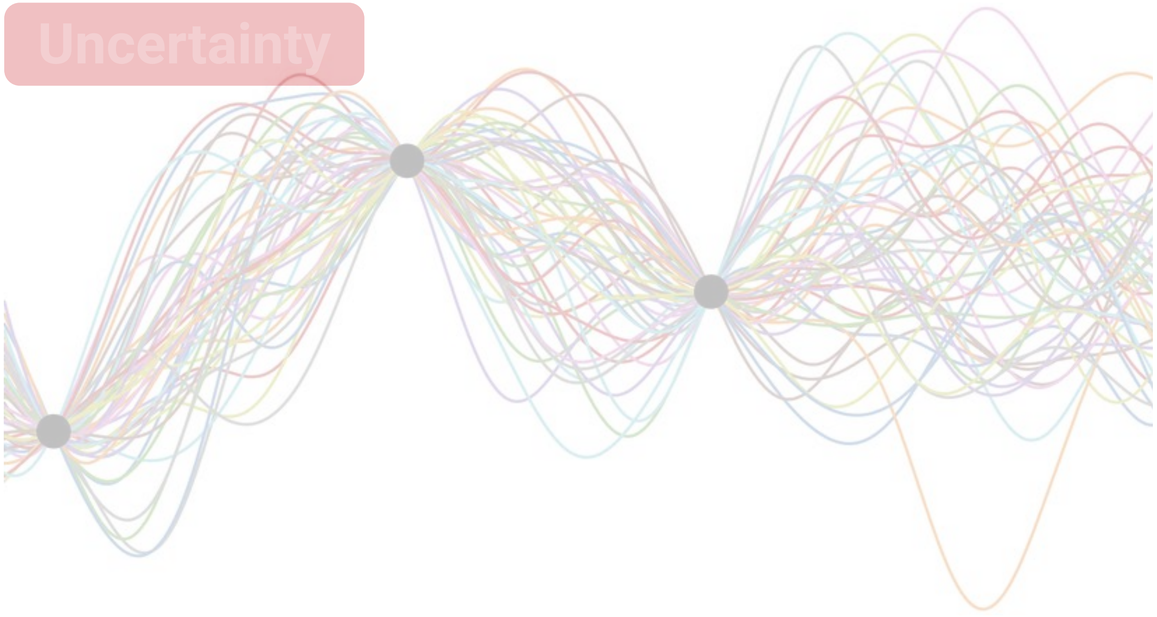

Uncertainty


Degradation
gettyimages
cstar55


Cyber attacks

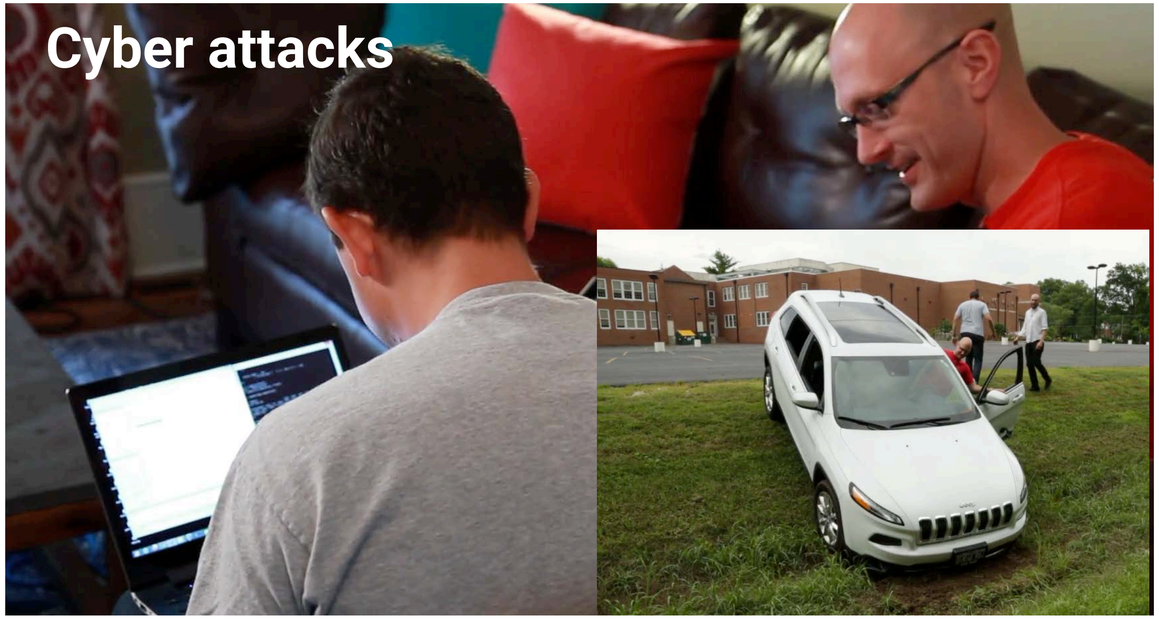
Faults

Uncertainty



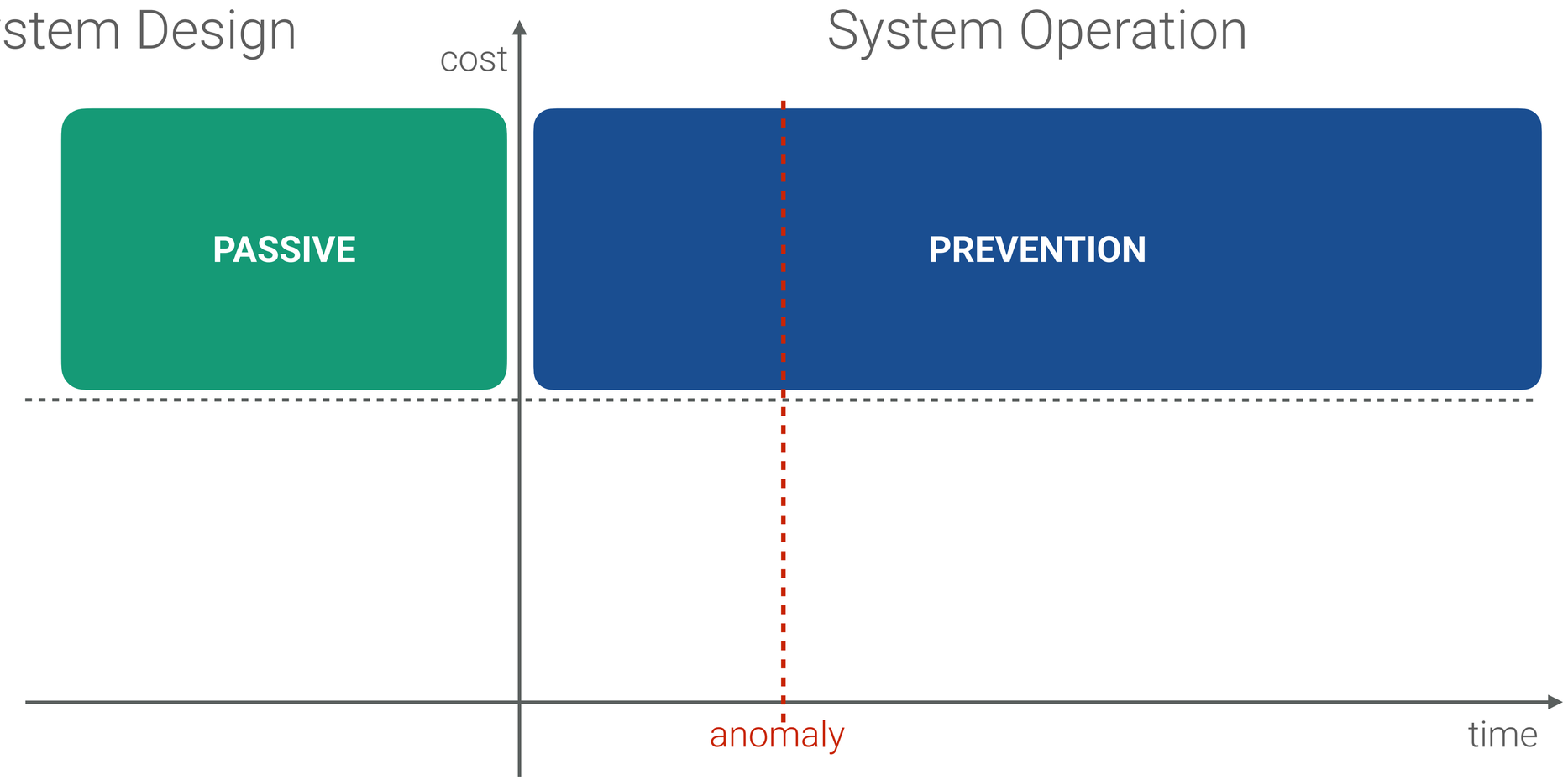
Degradation

Cyber attacks



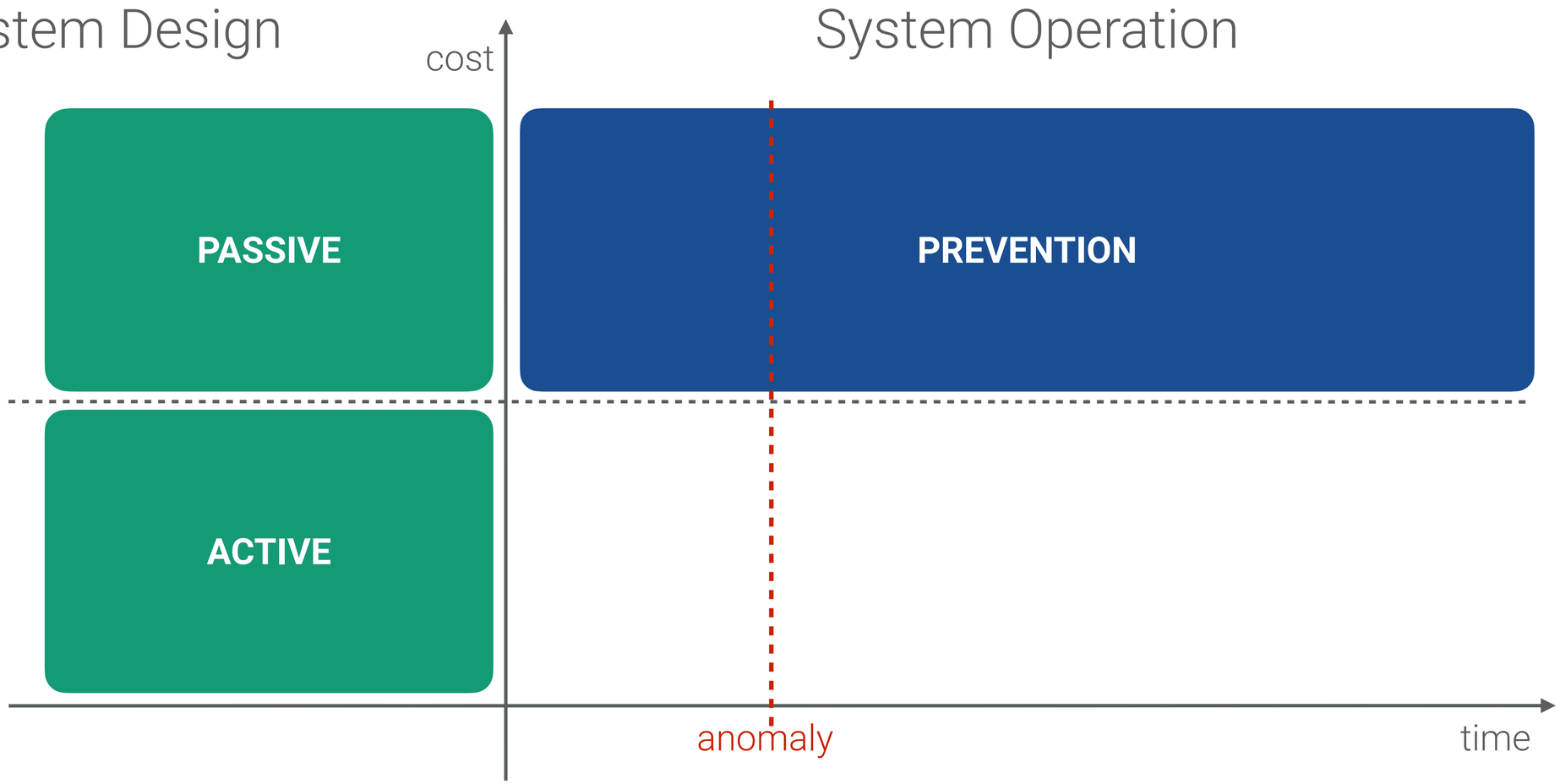
Our Approach

Active Approach to Safety and Resiliency



Our Approach

Active Approach to Safety and Resiliency



Our Approach

Active Approach to Safety and Resiliency

System Design

System Operation

cost

PASSIVE

PREVENTION

ACTIVE

DETECTION

ACCOMMODATION

anomaly

time

Our Approach

Active Approach to Safety and Resiliency

System Design

System Operation

cost

PASSIVE

PREVENTION

ACTIVE

IMPLICIT ACCOMMODATION

DETECTION

ACCOMMODATION

anomaly

time

Our Approach

Active Approach to Safety and Resiliency

System Design

System Operation

cost

PASSIVE

PREVENTION

ACTIVE

ACTIVE PREVENTION

IMPLICIT ACCOMMODATION

DETECTION

ACCOMMODATION

anomaly

time

Industrial Control Systems

TU Delft

Motivation

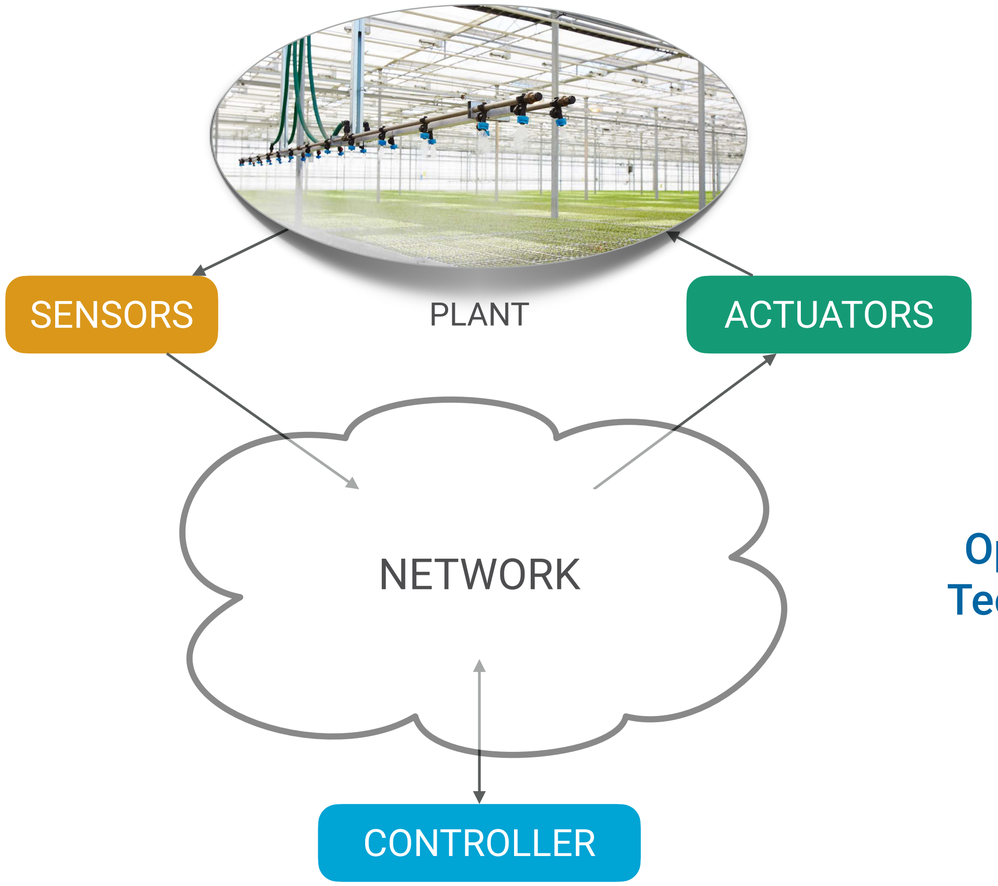
Need for Industrial Control Systems in AgriFood Sector

- To guarantee performances (yield, quality, energy saving, etc.)
- Cannot be obtained manually
- Need an automated system (e.g. for regulation of temperature, humidity, $C0_2$ etc.)

➡ Industrial Control System

Motivation

Our focus is on Cyber-Physical Systems



Cyber-Physical Systems

- An Industrial Control System (ICS) includes
  - The Plant to be controlled (not a 🪴)
  - **Operation Technology**
    - Sensors
    - Actuators
    - A Controller (sort of computer)
    - A Network (called *fieldbus*)

Motivation

Our focus is on Cyber-Physical Systems

PLANT

SENSORS

ACTUATORS

NETWORK

CONTROLLER

Cyber-Physical Systems

Physical

Cyber

Domain

Threats

SAFETY

SECURITY

Goals

Motivation

Our focus is on Cyber-Physical Systems

SENSORS

PLANT

ACTUATORS

NETWORK

CONTROLLER

Cyber-Physical Systems

Physical

Cyber

Domain

FAULTS

DEGRADATION

Threats

SAFETY

SECURITY

Goals

Motivation

Our focus is on Cyber-Physical Systems

PLANT

SENSORS

ACTUATORS

Eavesdropping

NETWORK

Rerouting
Data replay
Data injection

CONTROLLER

Cyber-Physical Systems

Physical

Cyber

Domain

FAULTS

DEGRADATION

Threats

SAFETY

SECURITY

Goals

Motivation

Our focus is on Cyber-Physical Systems

PLANT

SENSORS

ACTUATORS

Eavesdropping

NETWORK

Rerouting
Data replay
Data injection

CONTROLLER

Cyber-Physical Systems

Physical

Cyber

Domain

FAULTS

DEGRADATION

Threats

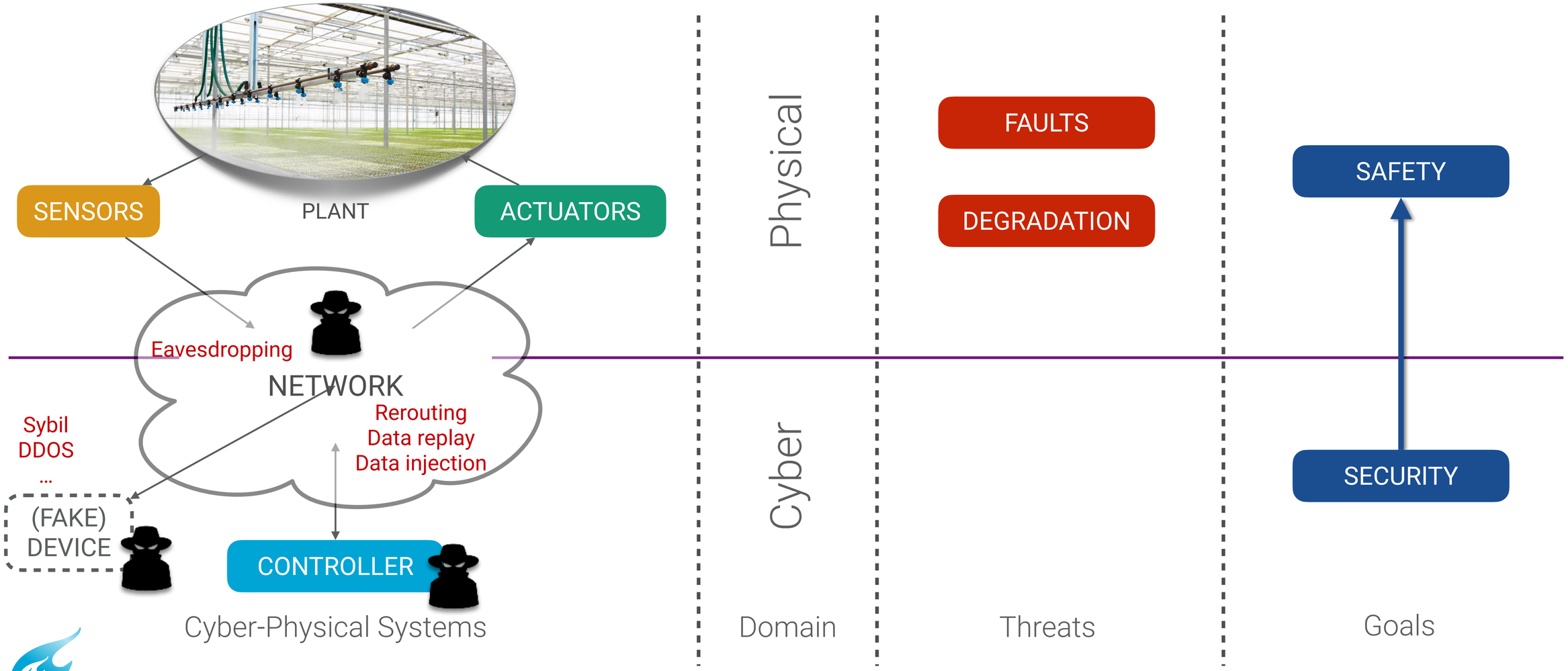
SAFETY

SECURITY

Goals

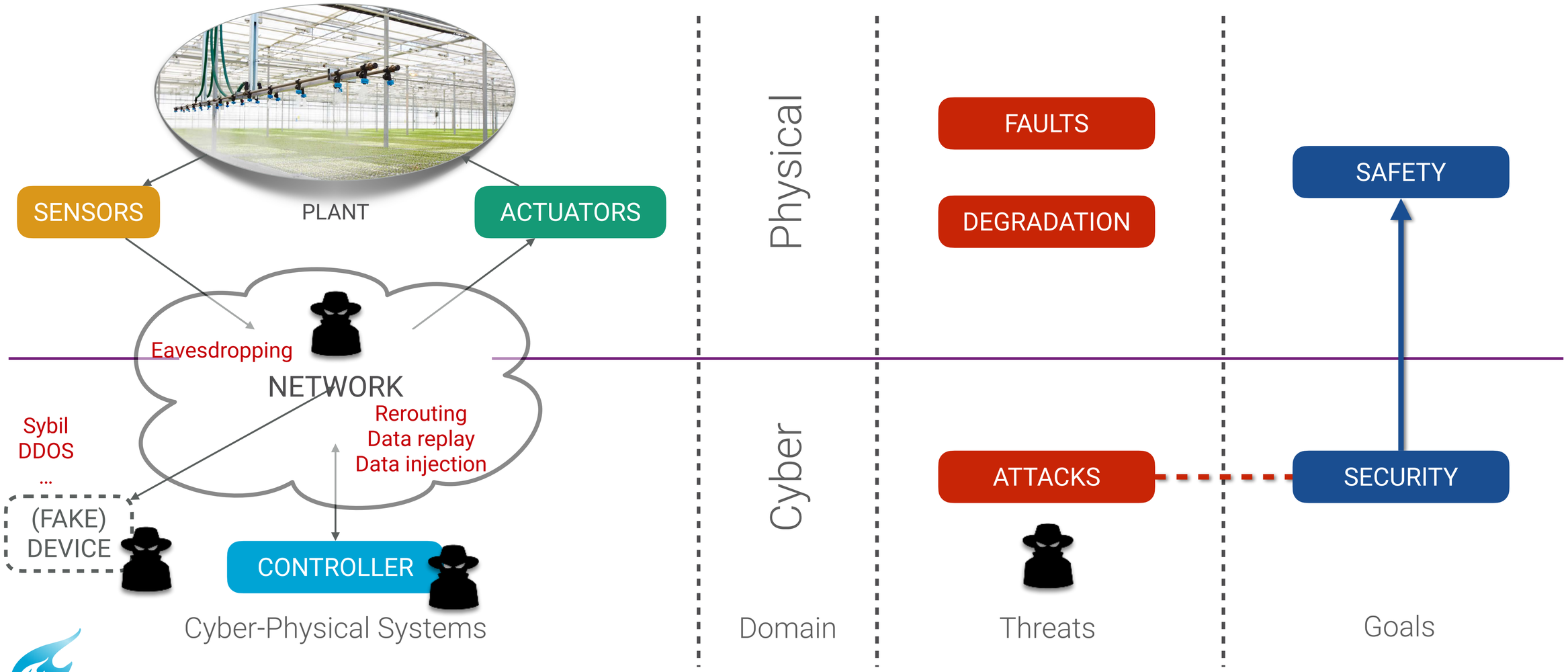
MOTIVATION

OUR FOCUS IS ON CYBER-PHYSICAL SYSTEMS



MOTIVATION

OUR FOCUS IS ON CYBER-PHYSICAL SYSTEMS



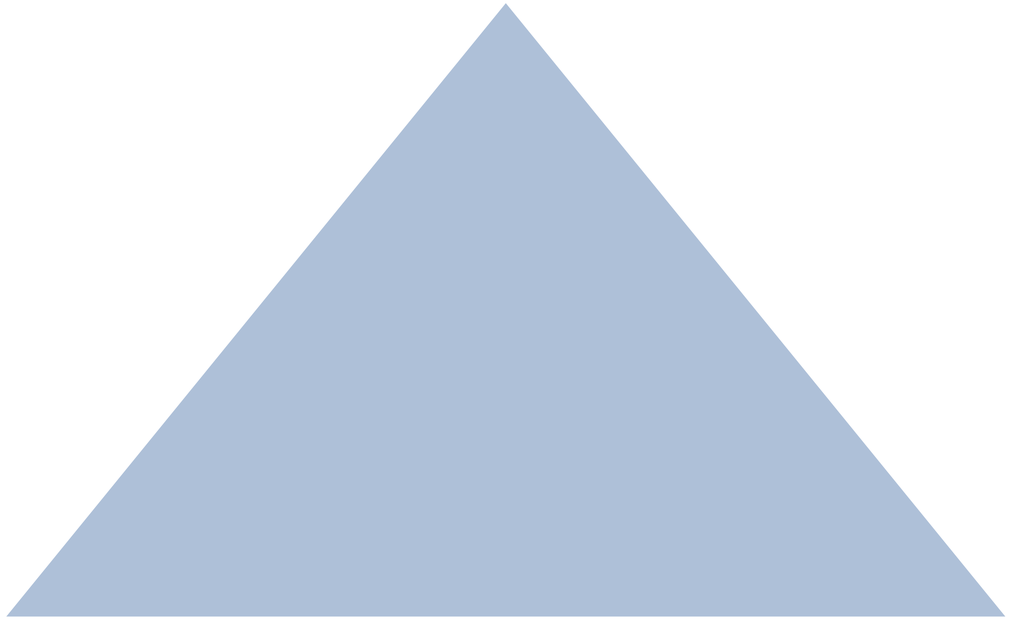
Safety and Security

TU Delft

Security Concepts

A TRIAD OF TRIADS

"The more we depend on data, the more we depend on its security„

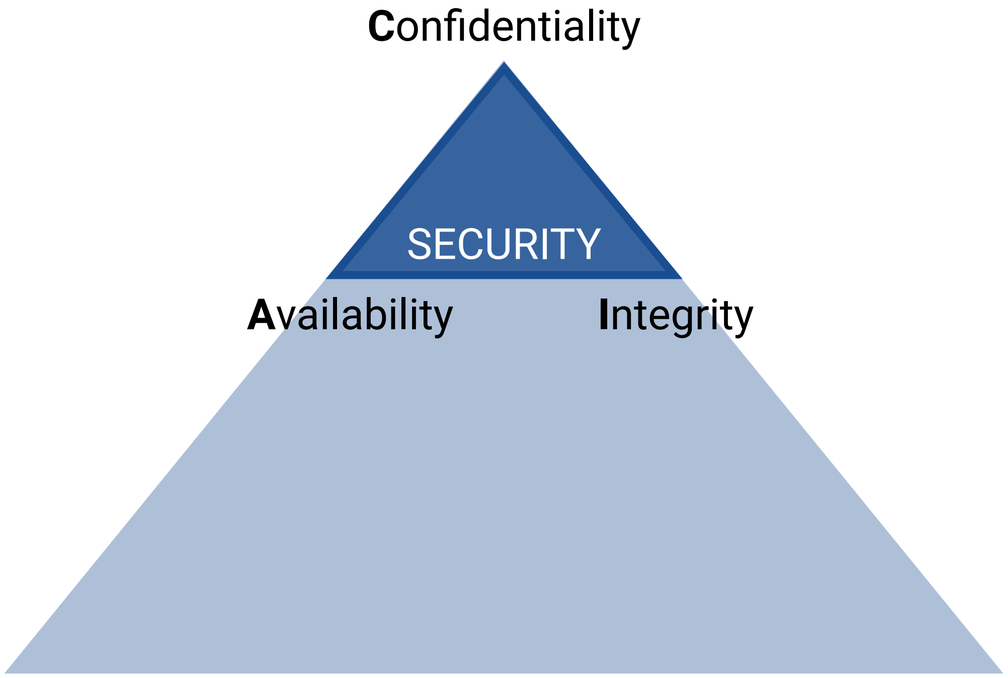


[Bo16] Bogaardt et al., "Cybersecurity in the Agrifood sector. Capgemini Consulting," Technical Report, 2016

Security Concepts

A TRIAD OF TRIADS

"The more we depend on data, the more we depend on its security„

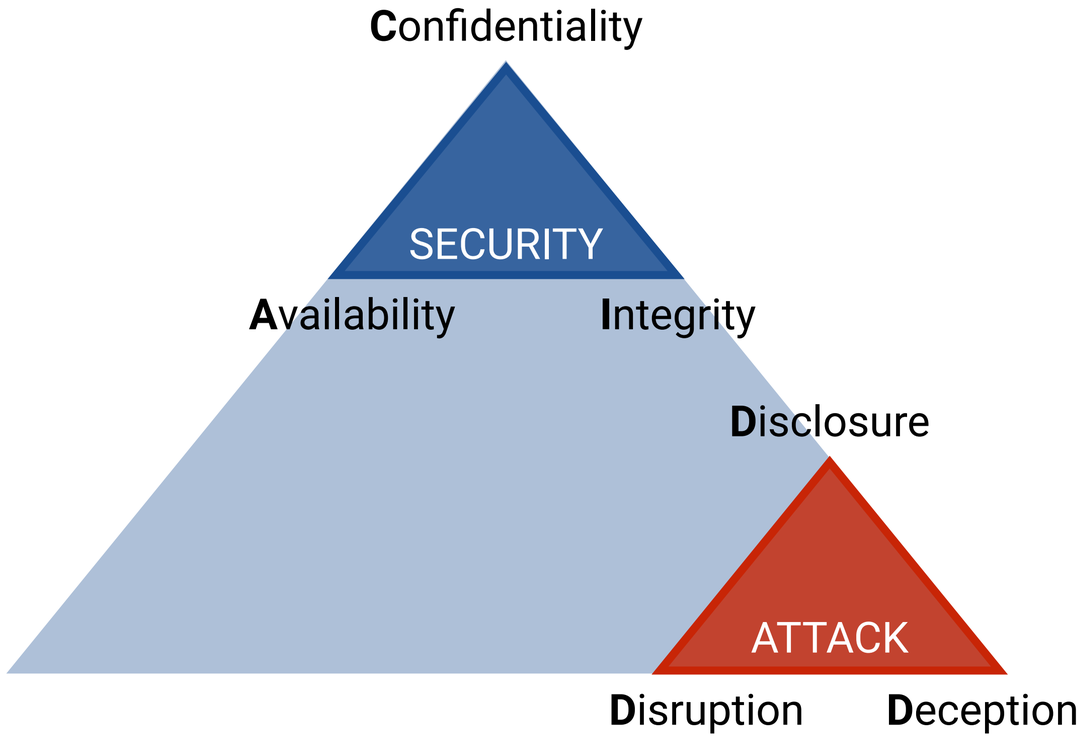


[Bo16] Bogaardt et al., "Cybersecurity in the Agrifood sector. Capgemini Consulting," Technical Report, 2016

Security Concepts

A TRIAD OF TRIADS

"The more we depend on data, the more we depend on its security„

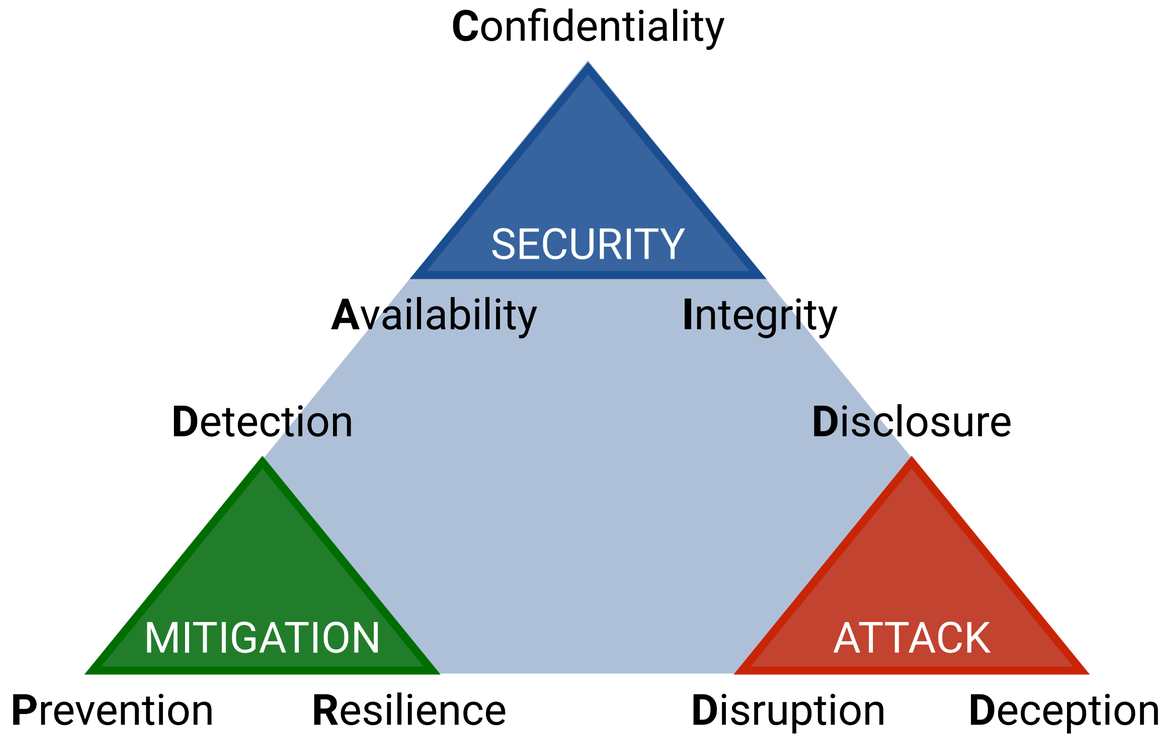


[Bo16] Bogaardt et al., "Cybersecurity in the Agrifood sector. Capgemini Consulting," Technical Report, 2016

Security Concepts

A TRIAD OF TRIADS

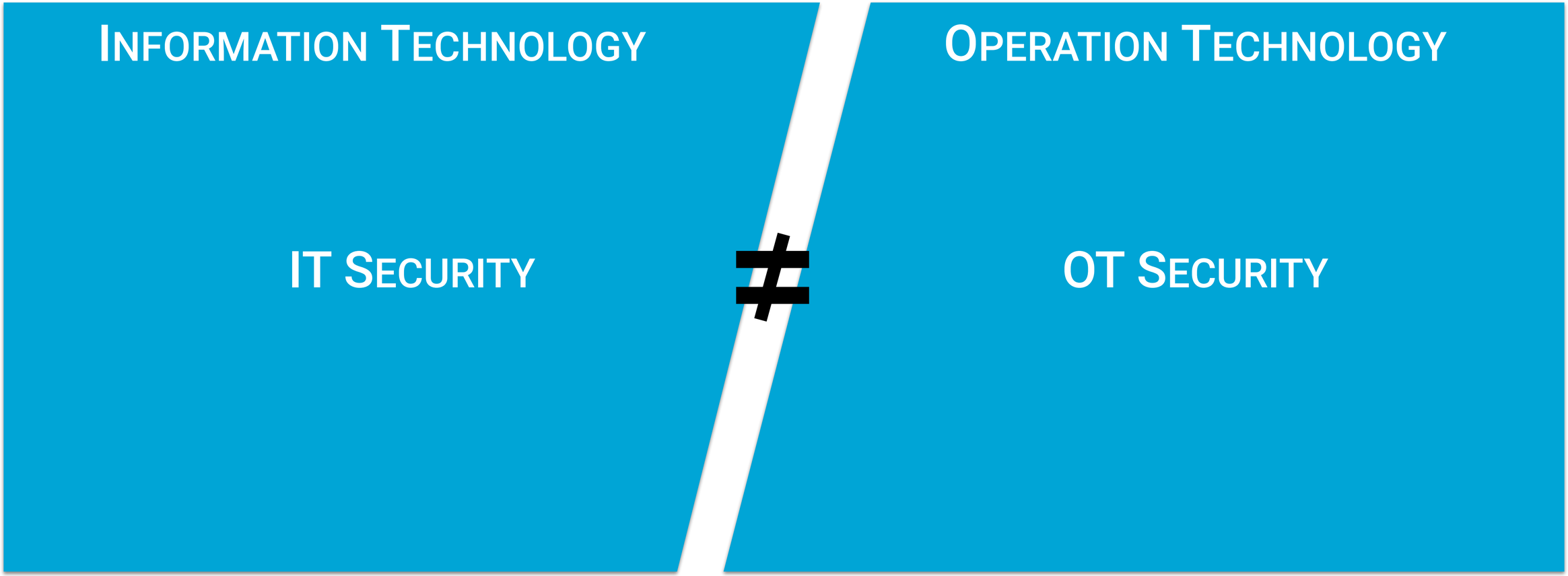
"The more we depend on data, the more we depend on its security„



[Bo16] Bogaardt et al., "Cybersecurity in the Agrifood sector. Capgemini Consulting," Technical Report, 2016

Key message of today

They are not the same



Key message of today

They are not the same

Information Technology

"On average, companies took about 207 days to identify and 70 days to contain a breach in 2022, according to IBM."

Operation Technology

[Kr23] M. Krotofil, "Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle," Technical Report, 2023

Key message of today

They are not the same

Information Technology

"On average, companies took about 207 days to identify and 70 days to contain a breach in 2022, according to IBM."

Operation Technology

"At 1:23 pm reactor cooling problem identified. At 1:33 pm the reactor burst and its contents exploded, killing 4 and injuring 38 people"

[Kr23] M. Krotofil, "Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle," Technical Report, 2023

Key message of today

They are not the same

Information Technology

"On average, companies took about 207 days to identify and 70 days to contain a breach in 2022, according to IBM."

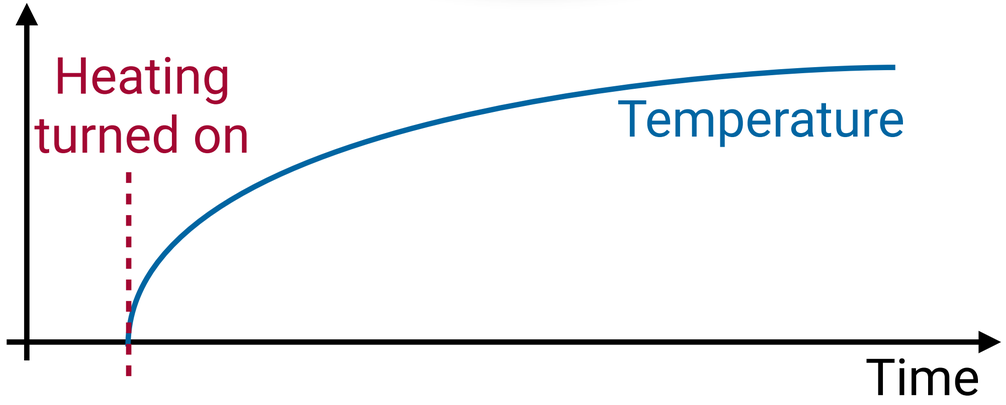
Operation Technology

"At 1:23 pm reactor cooling problem identified. At 1:33 pm the reactor burst and its contents exploded, killing 4 and injuring 38 people"

[Kr23] M. Krotofil, "Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle," Technical Report, 2023

Key message of today

Attacks and Defense need to consider Plant Dynamics

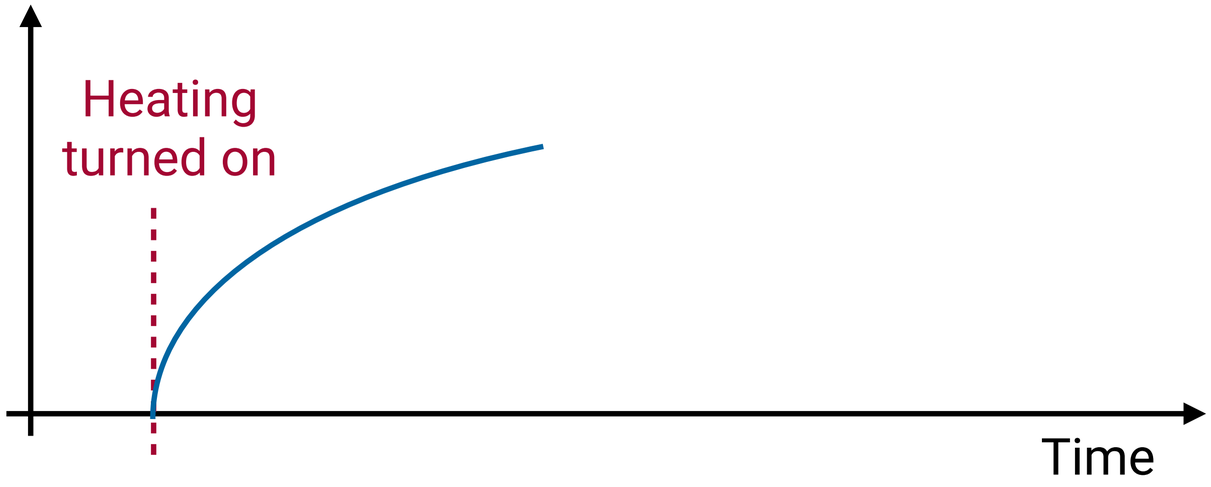


Operation Technology

- Time is fundamental
  - Physics takes time to evolve (dynamics)
  - OT has strict real-time constraints

How can defenders leverage dynamics?

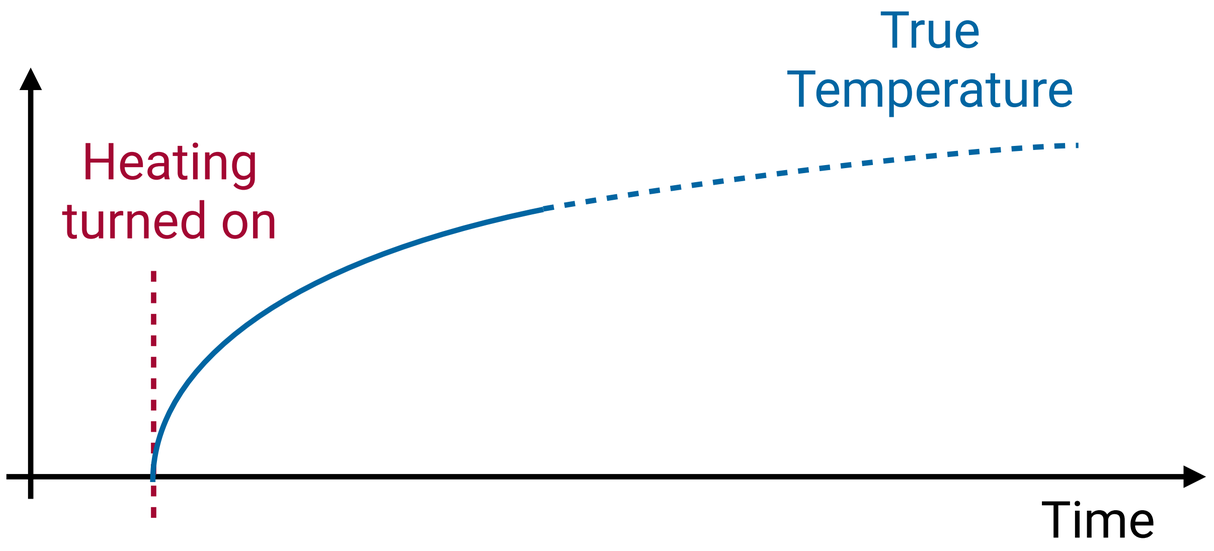
PHYSICS NEVER LIE



- Assume the attacker can compromise a temperature sensor
- They tricks the controller to over-compensate
- This clearly does not match physics
- Can we detect this?

How can defenders leverage dynamics?

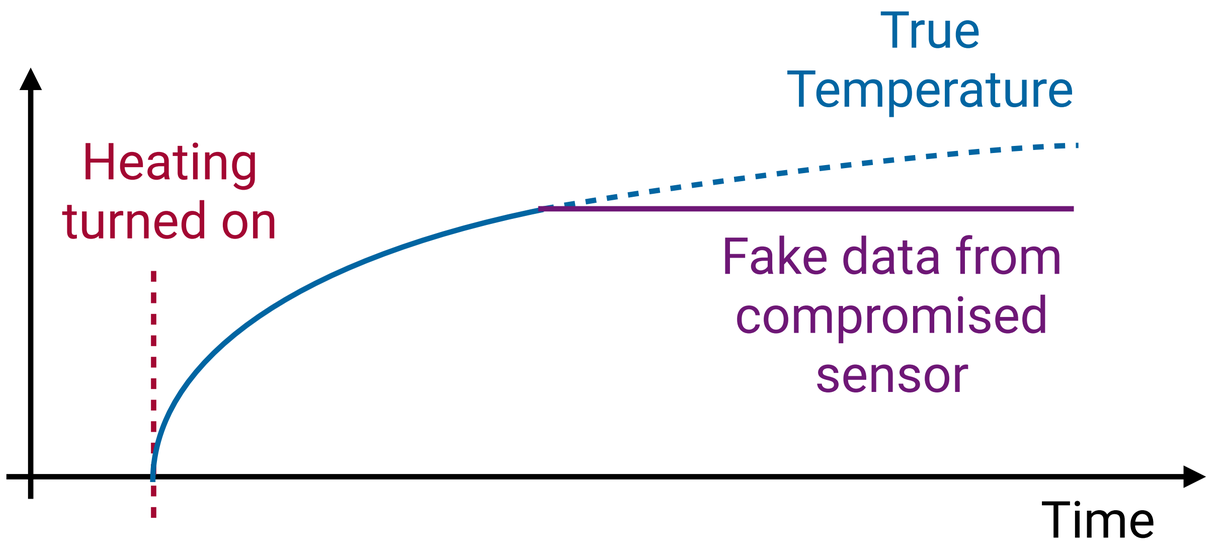
PHYSICS NEVER LIE



- Assume the attacker can compromise a temperature sensor
- They tricks the controller to over-compensate
- This clearly does not match physics
- Can we detect this?

How can defenders leverage dynamics?

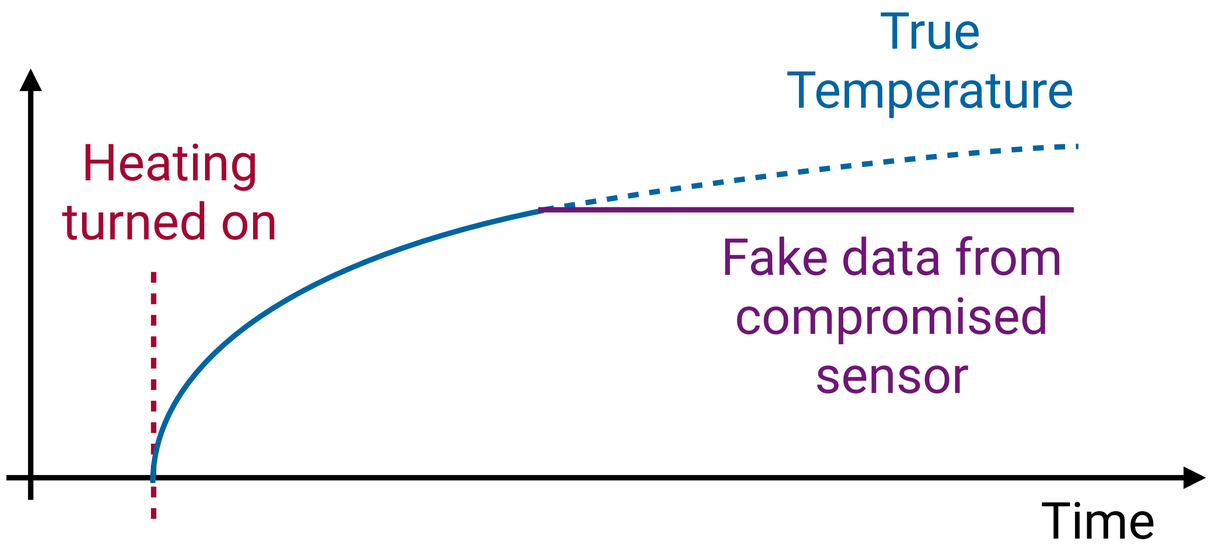
PHYSICS NEVER LIE



- Assume the attacker can compromise a temperature sensor
- They tricks the controller to over-compensate
- This clearly does not match physics
- Can we detect this?

How can defenders leverage dynamics?

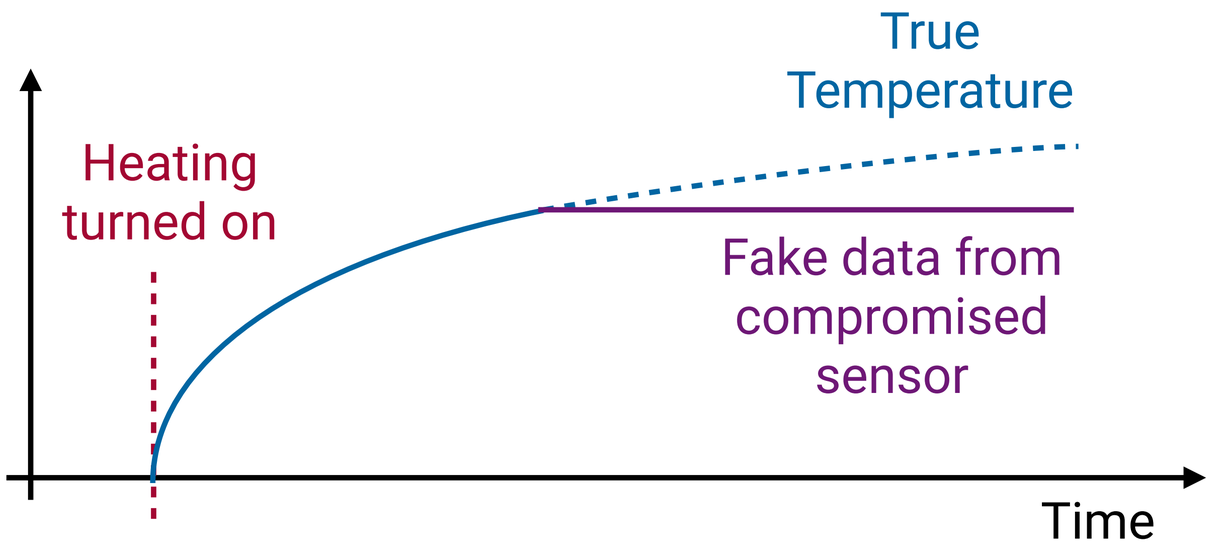
PHYSICS NEVER LIE



- Caveat: a **smart attacker** can do better than this -> **stealthy**
- Can introduce **small offsets** that can lead to l**ower quality products** (e.g. moulds because humidity was wrong)
- We need **very accurate** understanding of our plant **physics**/advanced **AI** to detect this

How can defenders leverage dynamics?

PHYSICS NEVER LIE



- Caveat: a **smart attacker** can do better than this -> **stealthy**
- Can introduce **small offsets** that can lead to l**ower quality products** (e.g. moulds because humidity was wrong)
- We need **very accurate** understanding of our plant **physics**/advanced **AI** to detect this

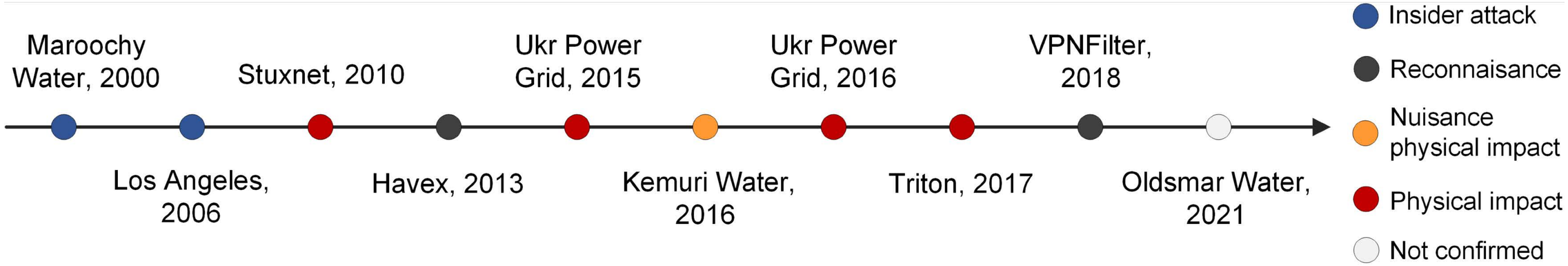
TU Delft

Diving Deeper:
Actual Attacks and ICS structure

TU Delft

Which attacks have been documented so far

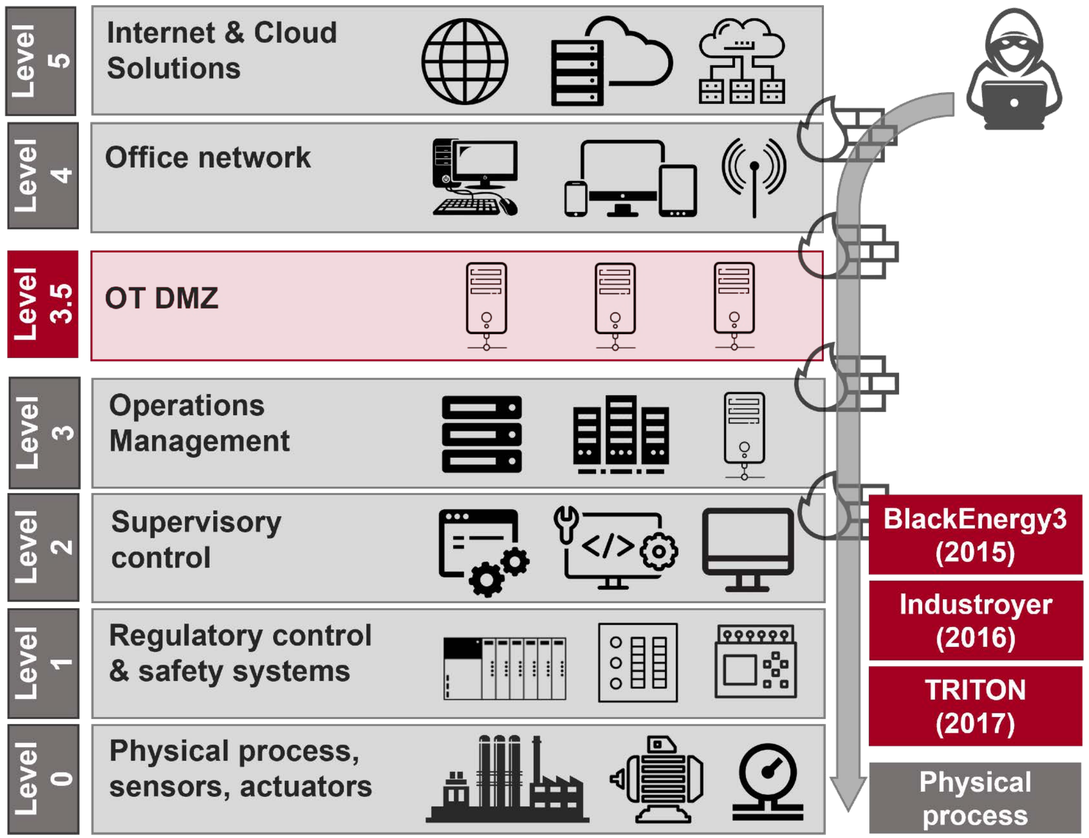
Only at OT level



[Kr23] M. Krotofil, “Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle,” Technical Report, 2023

Which attacks have been documented so far

WHERE DID THEY HAPPEN



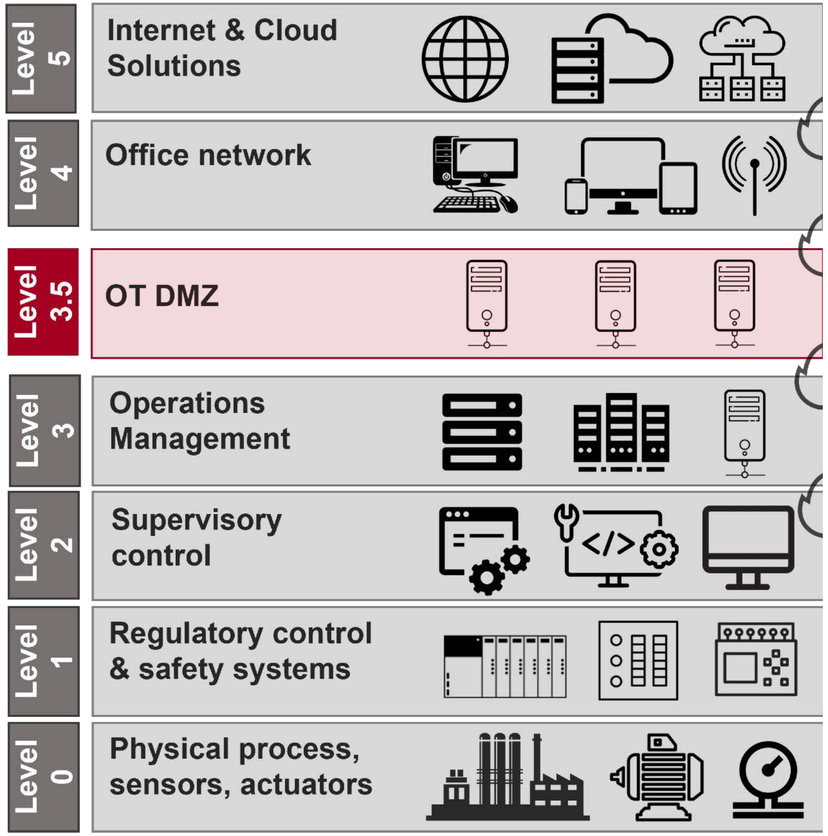
- Actually ICS are structured in a hierarchical way
- Lower layers: OT, closer to physical process
- Higher layers: IT, connected to Internet
- Good practice: separate via a DMZ
- Here we do not address ransomware or other attacks at IT level

[Kr23] M. Krotofil, “Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle,” Technical Report, 2023

Final Recommendations

TU Delft

Recommendations



- **Structure** ICS following **good practices**
- Apply ABC of **IT security** to **upper layers**
- Check **vulnerabilities** at **OT level** as well (example from NIST), patch asap
- Have a system for **detecting anomalies** at lower layers
  - **Protocol** anomalies
  - **Physical** anomalies (our work)

Example of NIST advisory

CVE-2023-49621 Detail

Description

A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Siemens AG **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: The CNA providing a score has achieved an Acceptance Level of Provider. The NVD will only audit a subset of scores provided by this CNA.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf	Patch Vendor Advisory

QUICK INFO

CVE Dictionary Entry:
CVE-2023-49621
NVD Published Date:
01/09/2024
NVD Last Modified:
01/11/2024
Source:
Siemens AG

Example of NIST advisory

Do a cost/benefit analysis

- What is the likelihood you are targeted by a state-actor?
  - Likely low ➡ you do not need to secure everything at maximum level
- Is a disgruntled employee your likeliest threat?
- There is no cure that fits all, needs case-by-case analysis
- Still, please avoid plain Modbus-TCP protocol
  - We have a MSc thesis showing how easy it is to hack it
  - V. S. Ranade, “A laboratory for cyber-attack generation and testing in Industrial Control Systems: Design and Simulation”, MSc thesis, 2021.

Thank you for your attention!

Riccardo Ferrari (r.ferrari@tudelft.nl)

… keep your *plant* safe!