MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Introduction

Version: 1.3

Luca Haab | 16.02.2026 | Cours MSE

The course in a nutshell

Understand what Operational Technology (OT) means - the characteristics, the issues - and how to ensure that the challenges of these systems are addressed properly

Some administrative matters

- Lecture schedule
  - 13h10-13h55 + 14h05-14h50 + 15h00-15h45
- Resources
  - Site: https://secindopt.github.io/homepage
  - Openstack (SwithEngine) + a remote device (your task)
- Project
  - Along the semester, you have 3 deliveries.
  - Working in team of 3 students.
  - The project is evaluated after each phase.
  - The project grade can increase your mark up to 0.3 (bonus, no malus)
  - Note: you need to deliver all 3 phases or otherwise no bonus granted
- Course grade
  - The project/exam grade : $\text{mark}_{\text{exam}} + \text{mark}_{\text{bonus}}$

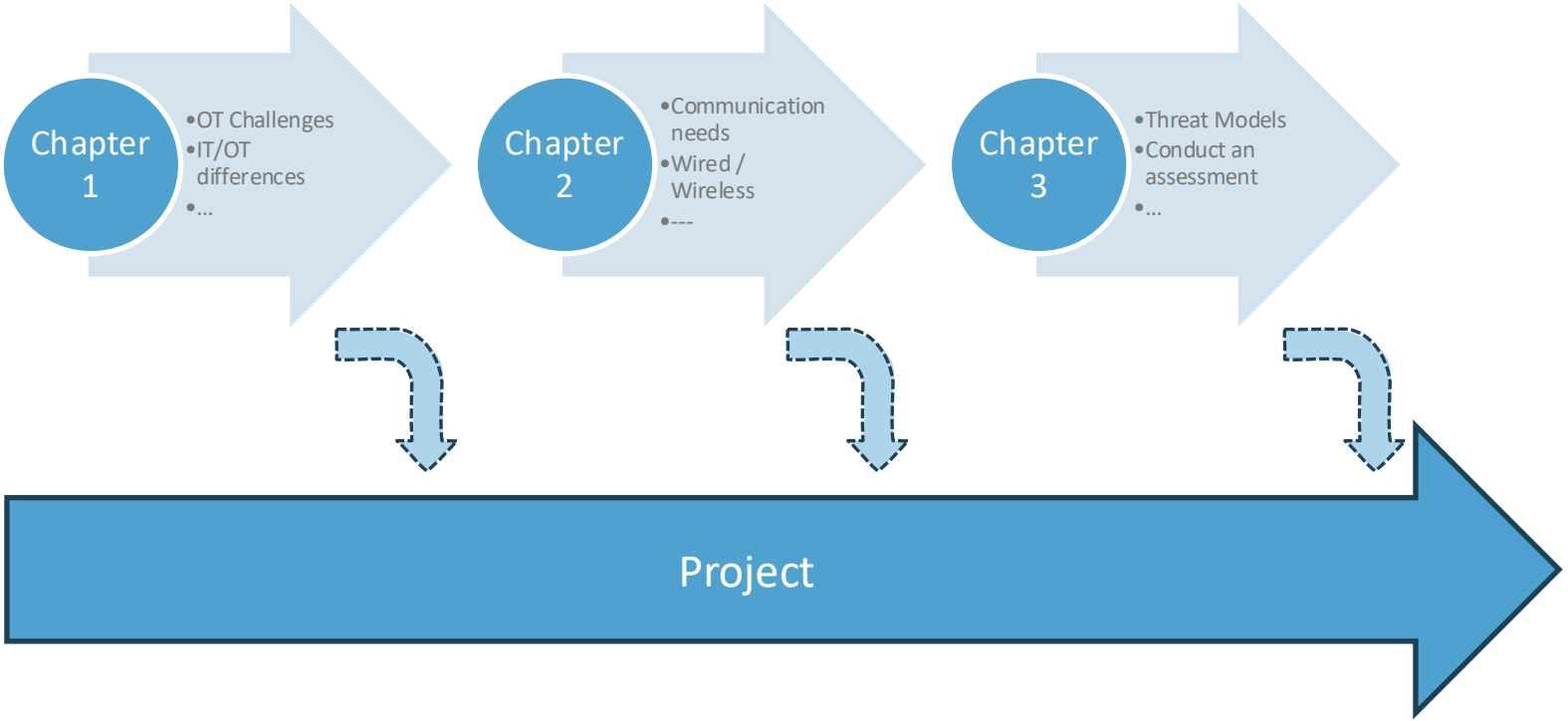
Communication / Logistics

- Courses take place physically in ZH
- Session available in Moodle
- Communication:
  - Email to professors: profs@secindopt.ch
  - Whole class: class@secindopt.ch

Course content

- Entire content available on the lecture website : https://secindopt.github.io/homepage
- Organisation
  - Course description, objectives, planning and logistical information
- Documentation
  - Documents and references
- Lecture
  - Content delivered on slides
- Exercises
  - Addressing specific problems
  - Solutions made available after a few weeks
  - Some parts may be hidden at first, with solution made available after two weeks
- Project
  - To be implemented based on theory and exercises
  - Implemented in 3 phases, delivered on GitHub with feedback and, possibly, issues to be fixed

Project (I)


Chapter 1
•OT Challenges
•IT/OT differences
•…
Chapter 2
•Communication needs
•Wired / Wireless
•---
Chapter 3
•Threat Models
•Conduct an assessment
•…
Project

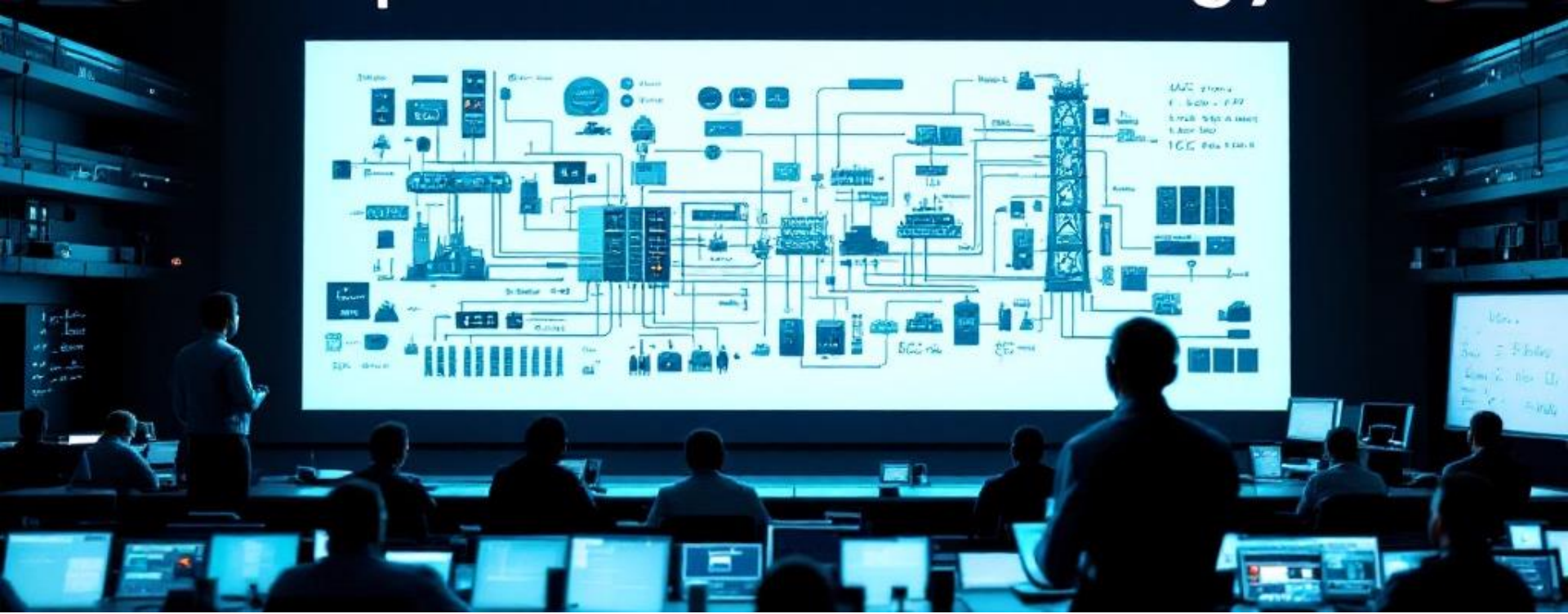
Project (II)

- A way to put into practice what we will look into on the theoretical side
- Is realized in groups of 3
- Is hosted on github and switchEngine
- Contains 3 phases
- Results in a bonus to your final mark (max 0.3)

Disclaimer: 2nd version of the course

A few questions to you

https://app.wooclap.com/SECINDOP

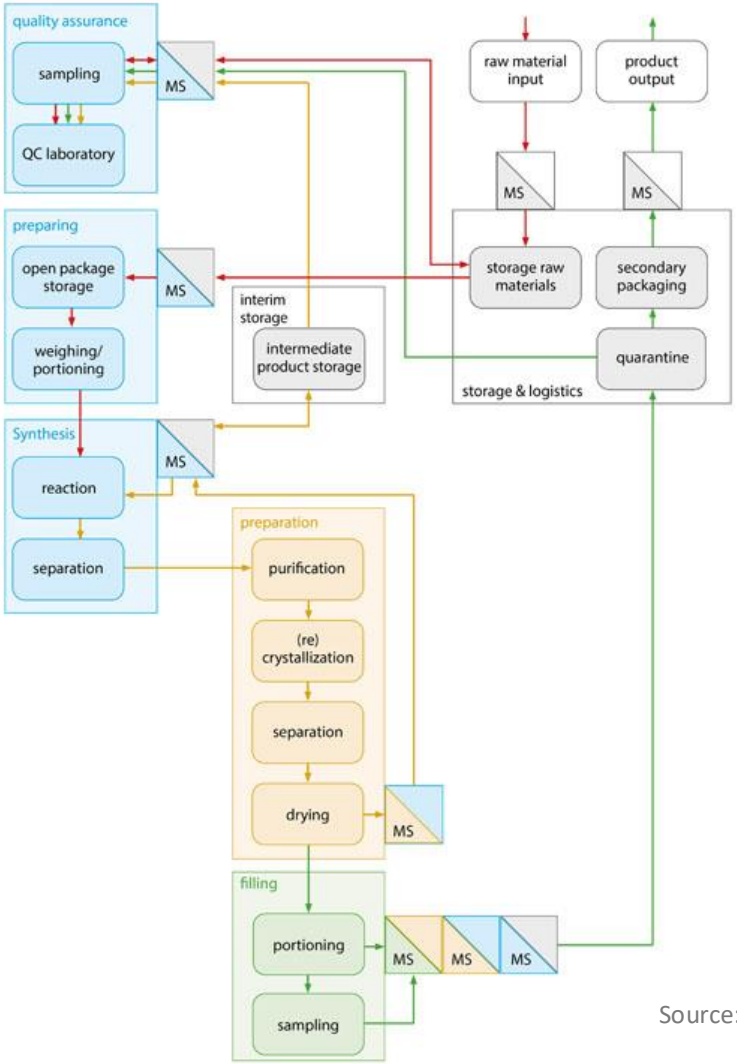


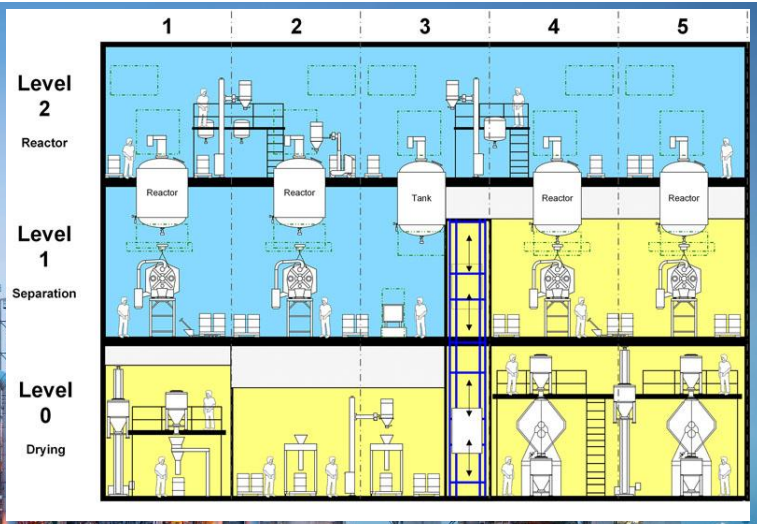
Operational Technology (OT)

Generated with https://chat.mistral.ai/chat

What is it? Really?


NETFLIX
OFFICIAL
TRAILER





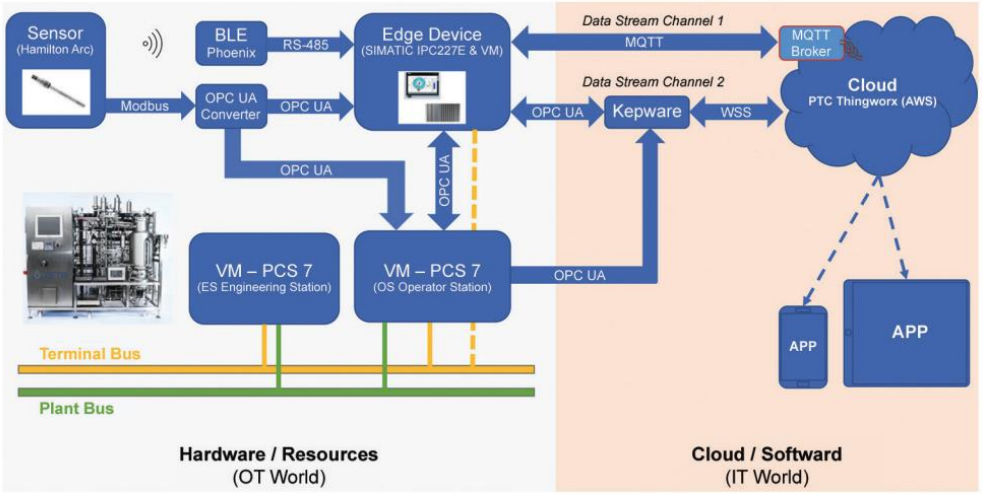
ion Plant

What does API mean?

Active Pharmaceutical Ingredients (APIs)

Source: https://manufacturingchemist.com/the-design-and-modularisation-of-api-synthesis-plants

Source: https://www.ibef.org/industry/pharmaceutical-india



OT – What's that? (Part 3)

Pharmaceutical Application

https://ispe.org/sites/default/files/concept-papers/ISPE-CP_IT-OT%20Architectures%20CP_Pharma%204.0.pdf

OT – What's that? (Part 4)

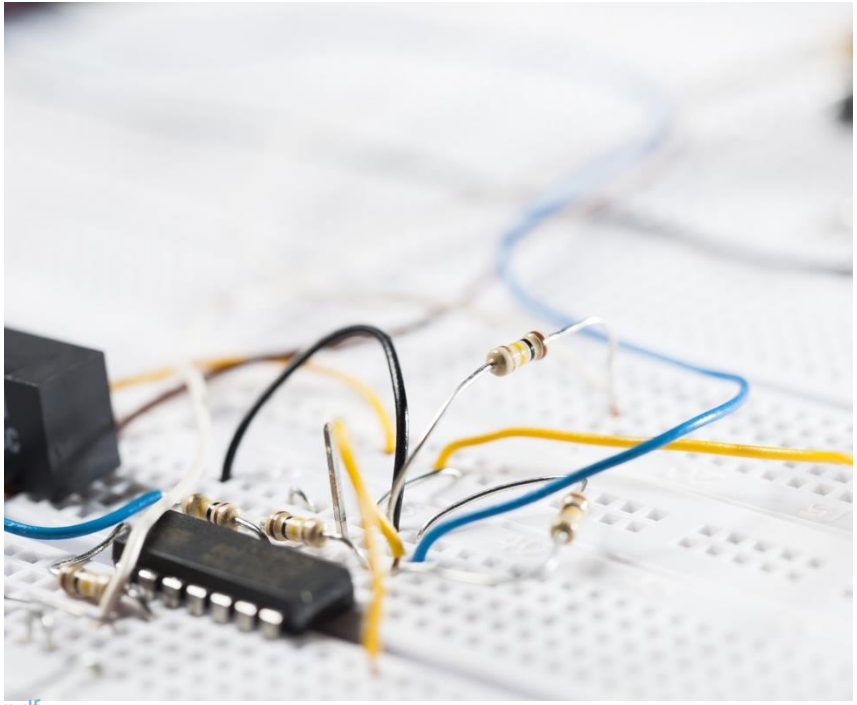
Digital substation

OT – What's that? (Part 5)

North America Black out 2003

Industrial Control System (ICS)

"An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes."

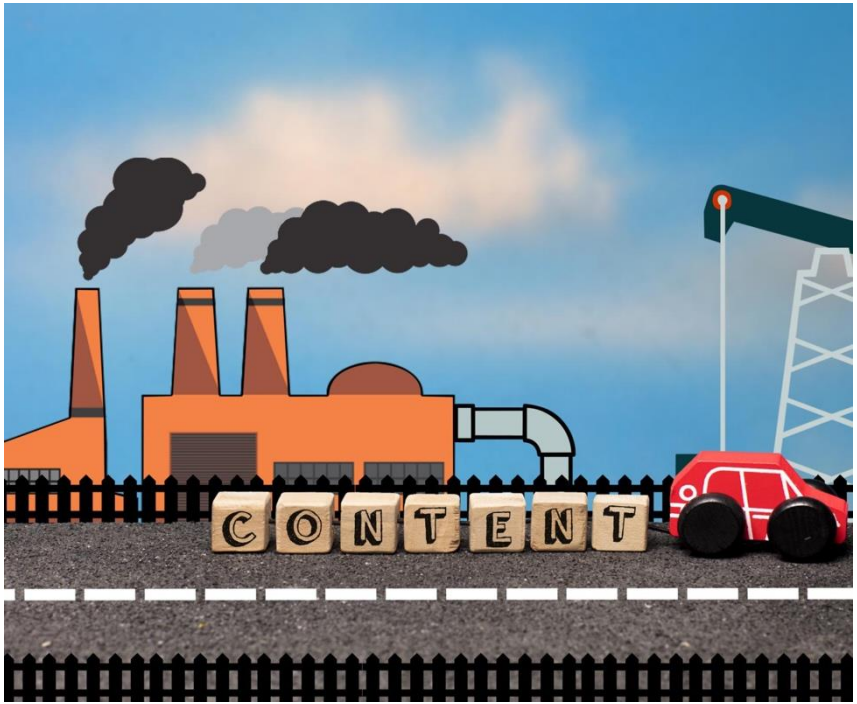


Source: https://csrc.nist.gov/glossary/term/ics, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Understanding Differences Between IT & OT

- IT focuses on data management, while OT focuses on physical processes
- IT systems prioritize confidentiality; OT systems prioritize availability and safety
- OT environments have stricter uptime requirements due to real-time operations

Key OT Threats



Differing Operational Priorities

Operational Technology (OT) has unique priorities that differ significantly from Information Technology (IT), necessitating specialized security approaches.

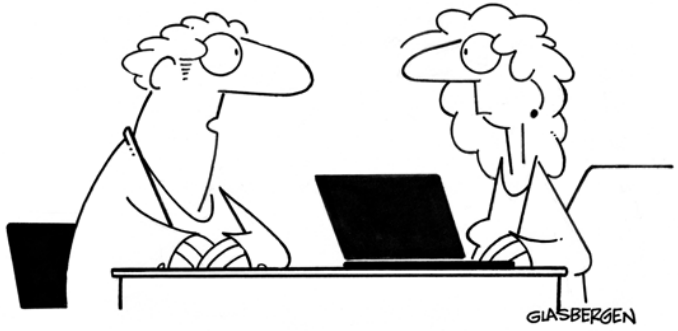
Unique Risk Profiles

OT risk profiles are distinct, often involving critical infrastructure where security breaches can have severe consequences.

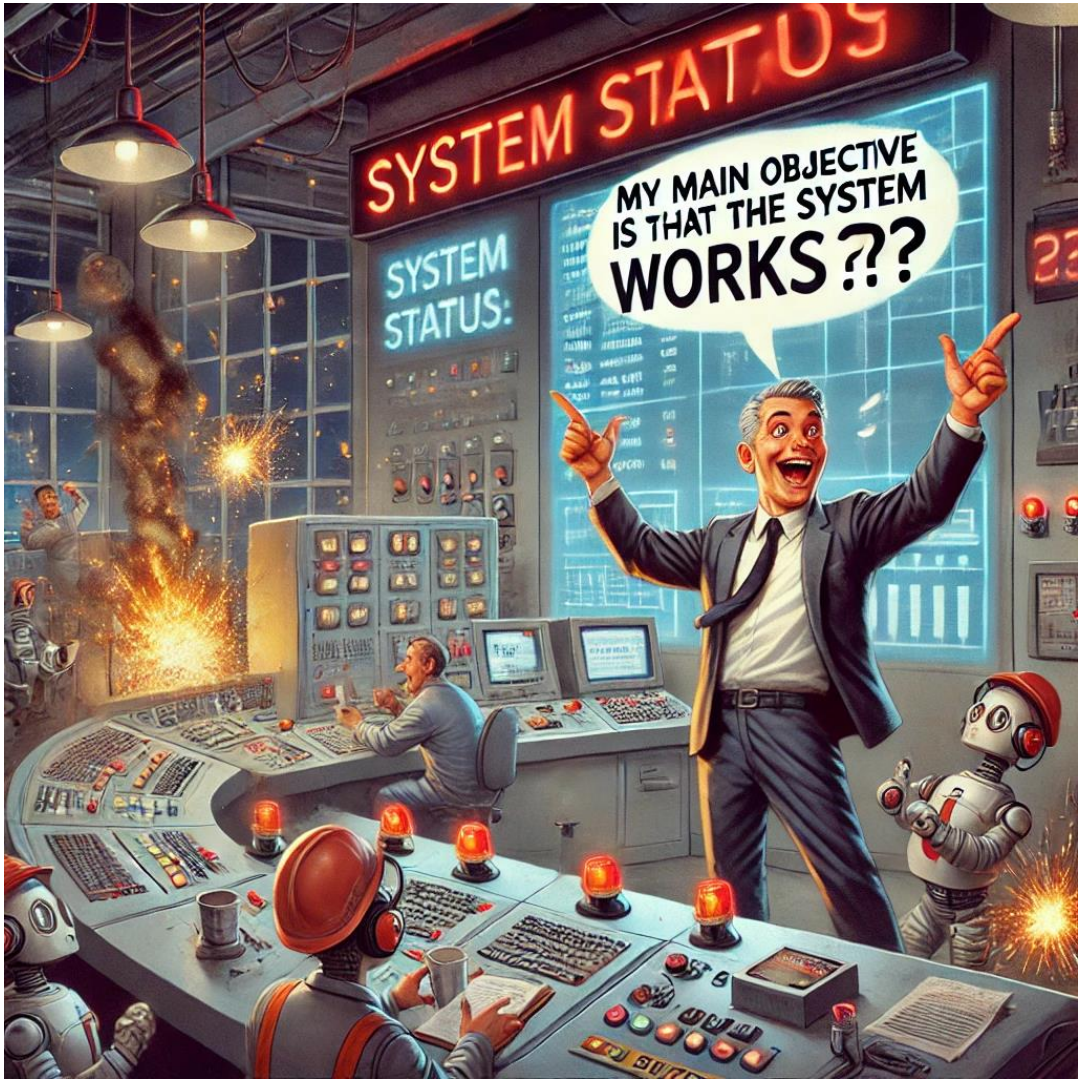
Consequences of Breaches

Security breaches in OT systems can lead to significant operational disruptions and safety hazards in critical infrastructure sectors.

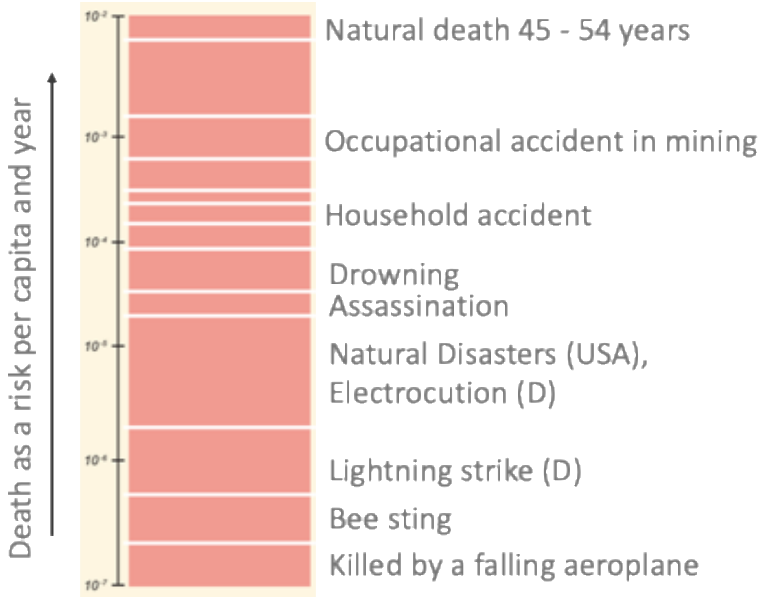
Operational priorities



"My short-term financial strategy is to survive until Tuesday.
My long-term financial strategy is to survive until Friday."



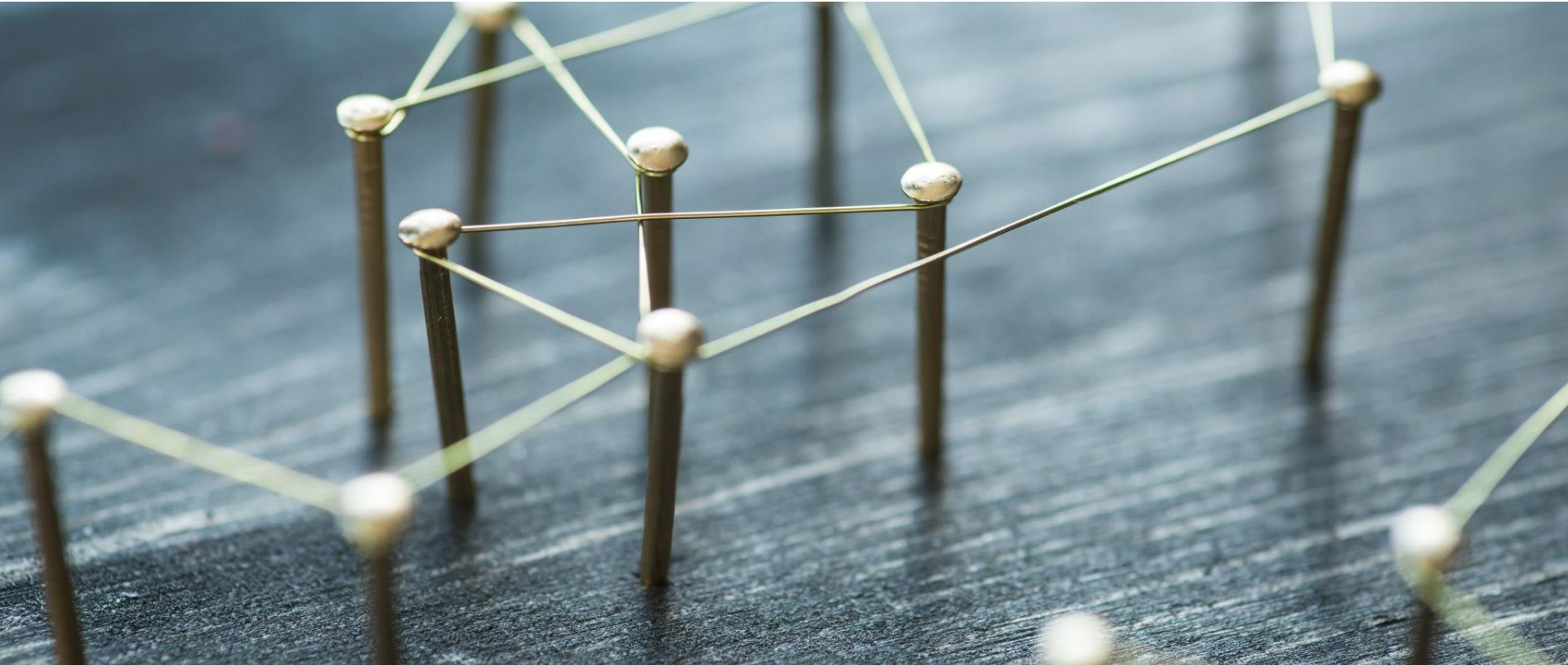
Risk profile? What could that be?



SIL	Low Demand Mode: Average Probability of Failure on Demand	High Demand or Continuous Mode: Probability of Dangerous Failure per Hour
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$ (1 dangerous failure in 1140 years)
4	10^{-5} to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

IEC61508 SIL: Safety Integrity Level

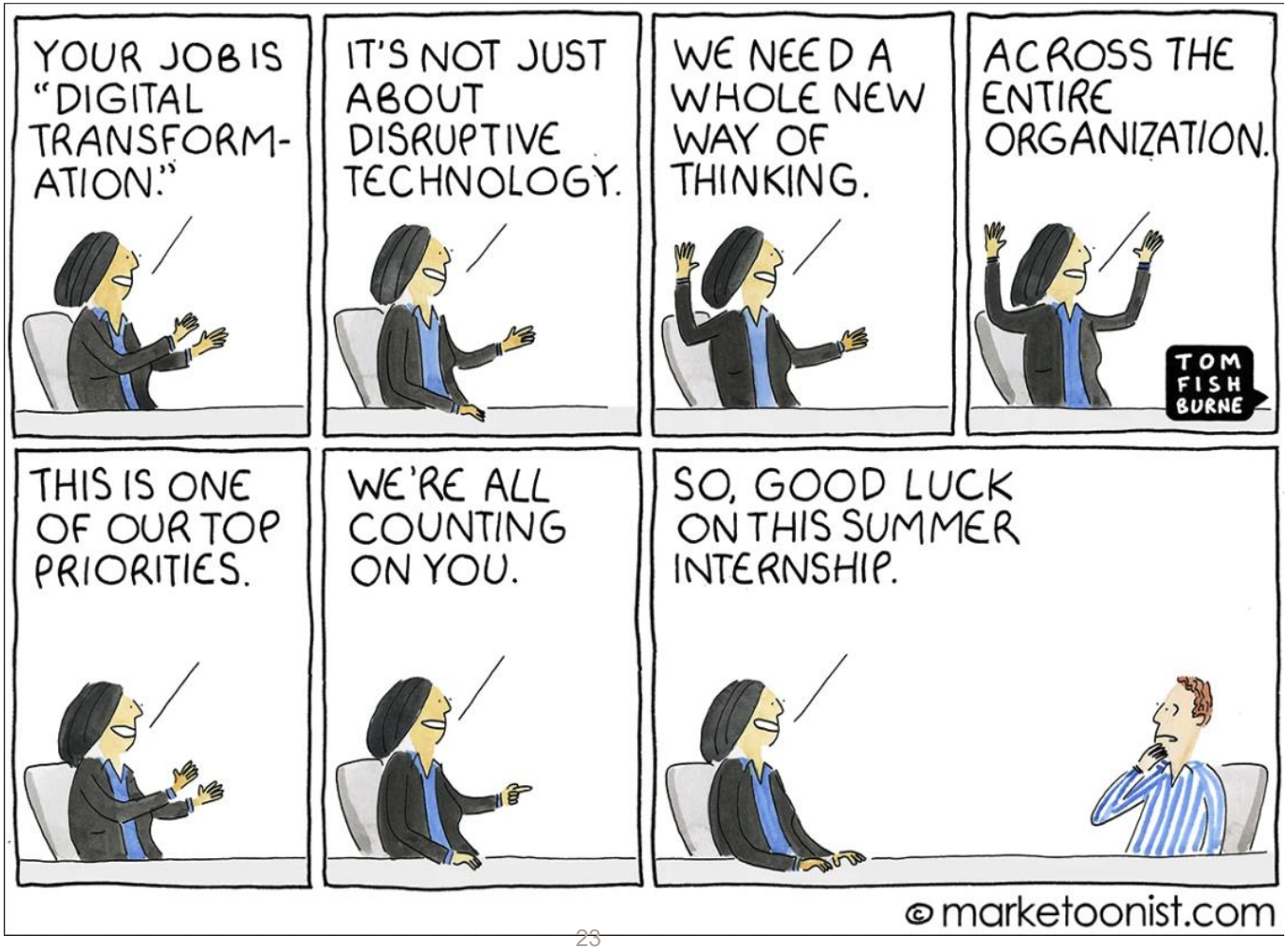
Other challenges



Standard Bodies

And the list is far from being complete

- erican ability (NERC)
- International Council on Large Electric Systems (CIGRE)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- nternet n (IIC)
- OPC Foundation
- American Water Works Association (AWWA)
- DNP3 Users Group
- Underwriters Laboratories (UL)
- American Petroleum Institute (API)
- ...


YOUR JOB IS "DIGITAL TRANSFORM-ATION."
IT'S NOT JUST ABOUT DISRUPTIVE TECHNOLOGY.
WE NEED A WHOLE NEW WAY OF THINKING.
ACROSS THE ENTIRE ORGANIZATION.
TOM FISH BURNE
THIS IS ONE OF OUR TOP PRIORITIES.
WE'RE ALL COUNTING ON YOU.
SO, GOOD LUCK ON THIS SUMMER INTERNSHIP.
© marketoonist.com

What’s the link to cybersecurity?

Notable Attacks in OT – in practice

Stuxnet Attack

The Stuxnet attack was a sophisticated cyber operation targeting Iran's nuclear facilities, exposing vulnerabilities in operational technology.

Ukraine Power Grid Attack

The Ukraine power grid attack demonstrated the potential for cyber threats to disrupt critical infrastructure and services.

Need for Security Measures

These incidents highlight the urgent need for robust security measures in operational technology to protect against cyber threats.

Stuxnet & Ukranian Power Grids

- Stuxnet
- Cyberattacks on Ukraine's Power Grid 2015–2016

More detailed view on Stuxnet: https://www.youtube.com/watch?v=DDH4m6M-ZIU
Other links: https://en.wikipedia.org/wiki/Stuxnet, https://github.com/uraninite/stuxnet and https://github.com/cloudfellows/stuxnet-worm

Common Cybersecurity Threats in OT

Malware Threats

Malware remains a significant threat in operational technology, potentially disrupting systems and causing downtime.

Ransomware Attacks

Ransomware can lock critical systems and demand payment, making it a severe risk for OT environments.

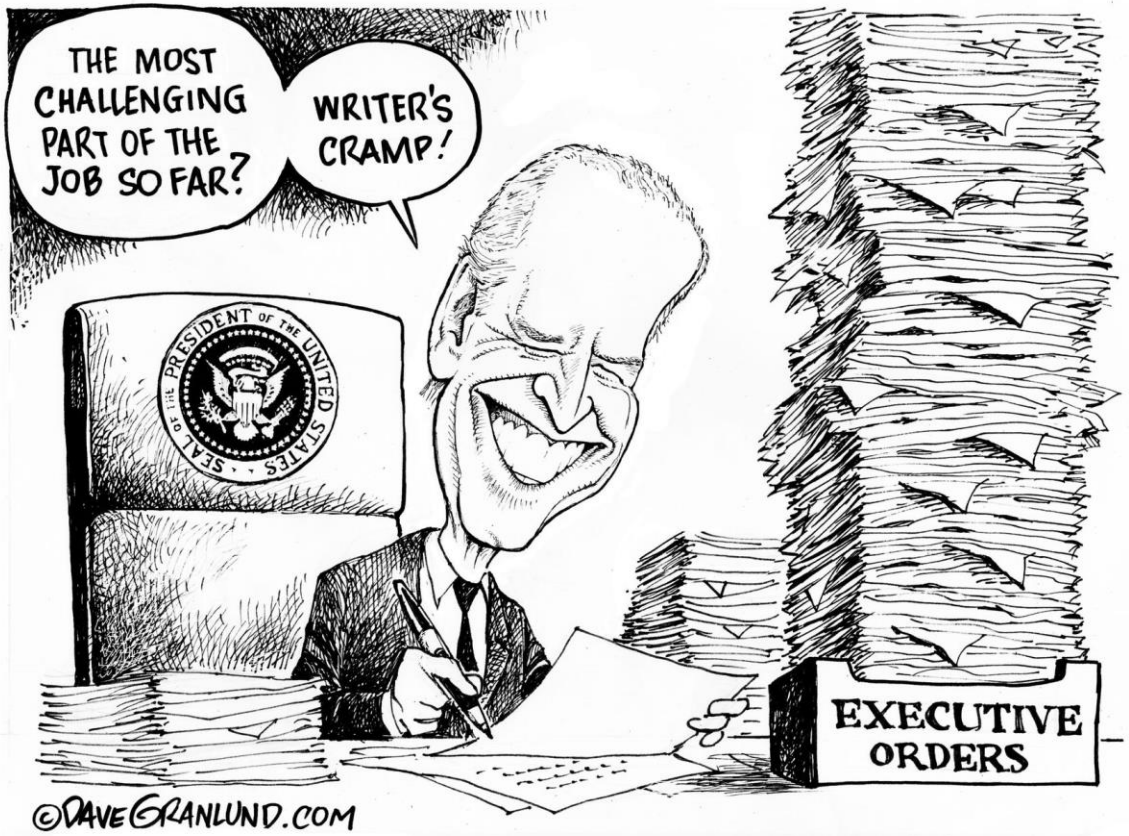
Advanced Persistent Threats (APTs)

APTs involve stealthy and continuous hacking processes aimed at stealing sensitive information from OT systems.

Insider Threats

Insider threats arise from individuals within the organization who can exploit access to OT systems, creating security vulnerabilities.

Consequence?



Before you start with the exercices

- Define groups of two (random.org may be a solution if need be ; -))
- Fill the form with your information and the group you belong to

References

- Course site: https://secindopt.github.io/homepage
- Links to papers/articles/…
  - The design and modularisation of API synthesis plants : https://manufacturingchemist.com/the-design-and-modularisation-of-api-synthesis-plants
  - Pharma 4.0 – Towards IT/OT Architectures for Prescriptive Maintenance : https://ispe.org/sites/default/files/concept-papers/ISPE-CP_IT-OT%20Architectures%20CP_Pharma%204.0.pdf
  - NIST Glossary: https://csrc.nist.gov/glossary/term/ics
  - NIST Information security : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- Videos
  - Virtual tour of the new Patriotes substation: https://www.youtube.com/watch?v=XP4fV-j5LB0
  - Blackout: The Power Outage That Left 50 Million W/o Electricity | Retro Report | The New York Times : https://www.youtube.com/watch?v=nd3teNgUq8E
  - Everything is Going Wrong | American Blackout : https://www.youtube.com/watch?v=qjJT8ZV6jaA
  - STUXNET: The Virus that Almost Started WW3 : https://www.youtube.com/watch?v=7g0pi4J8auQ
  - What happens when a power plant comes under attack? : https://www.youtube.com/watch?v=bV47gBsrDkc