SAVONIA

IoT Architecture and Security Models

Cybersecurity Fundamentals

Markku Kellomäki

SAVONIA

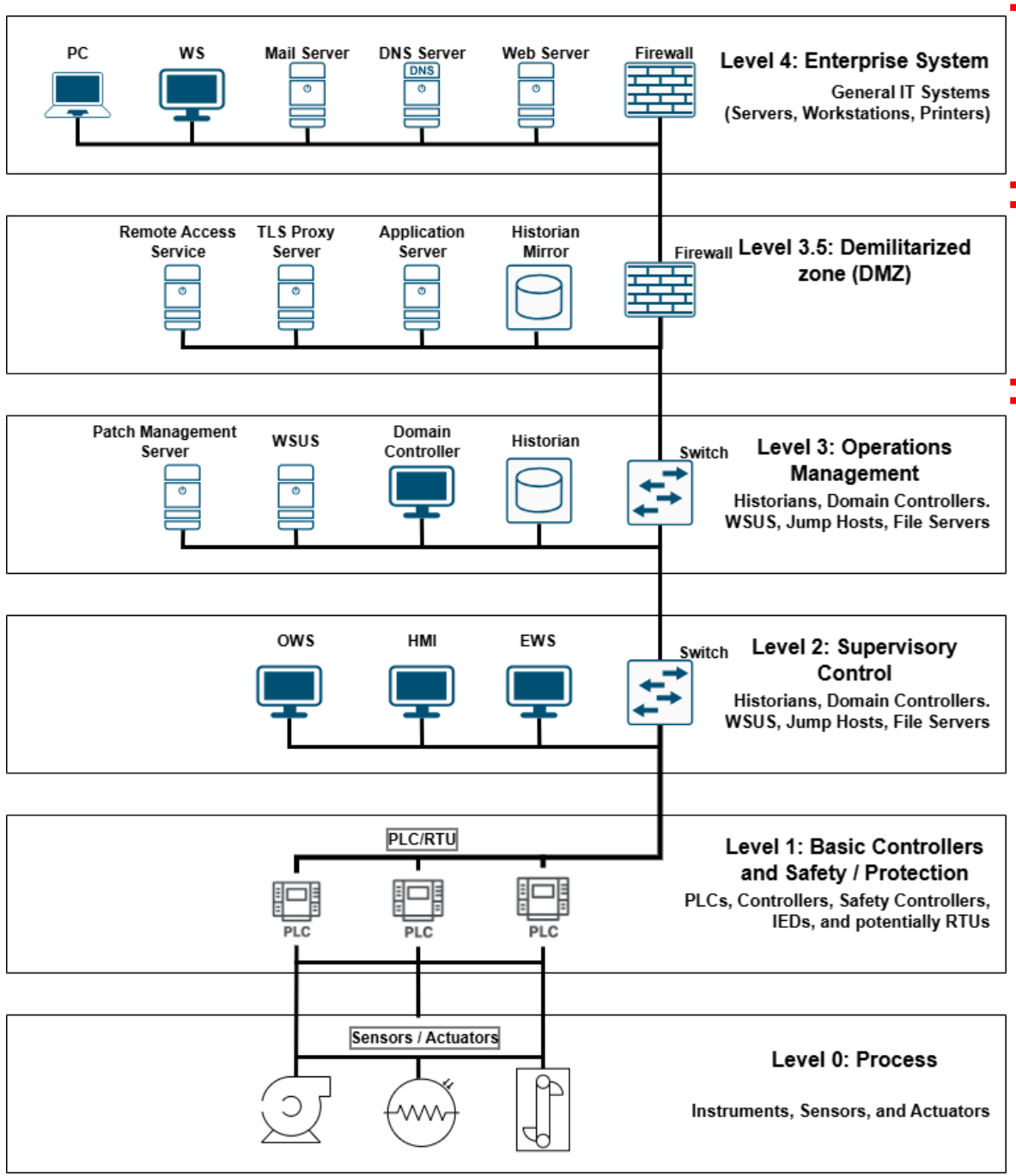
IoT Architecture

ICS for manufacturing - Purdue model

- The Purdue Enterprise Reference Architecture (PERA) is a widely used model for industrial automation and enterprise integration.
  - https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
- It was developed at Purdue University and serves as the foundation for many modern Industrial Control Systems (ICS).
- Some cybersecurity frameworks follow Purdue structure.
  - A nice article: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

SAVONIA

Purdue model for Industrial Control Systems



IT systems

IT/OT convergence layer

OT systems

OT and IT

- Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings.
- IT combines technologies for networking, information processing, enterprise data centers, and cloud systems.
- OT devices control the physical world, while IT systems manage data and applications.
- https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

Purdue model levels and risks

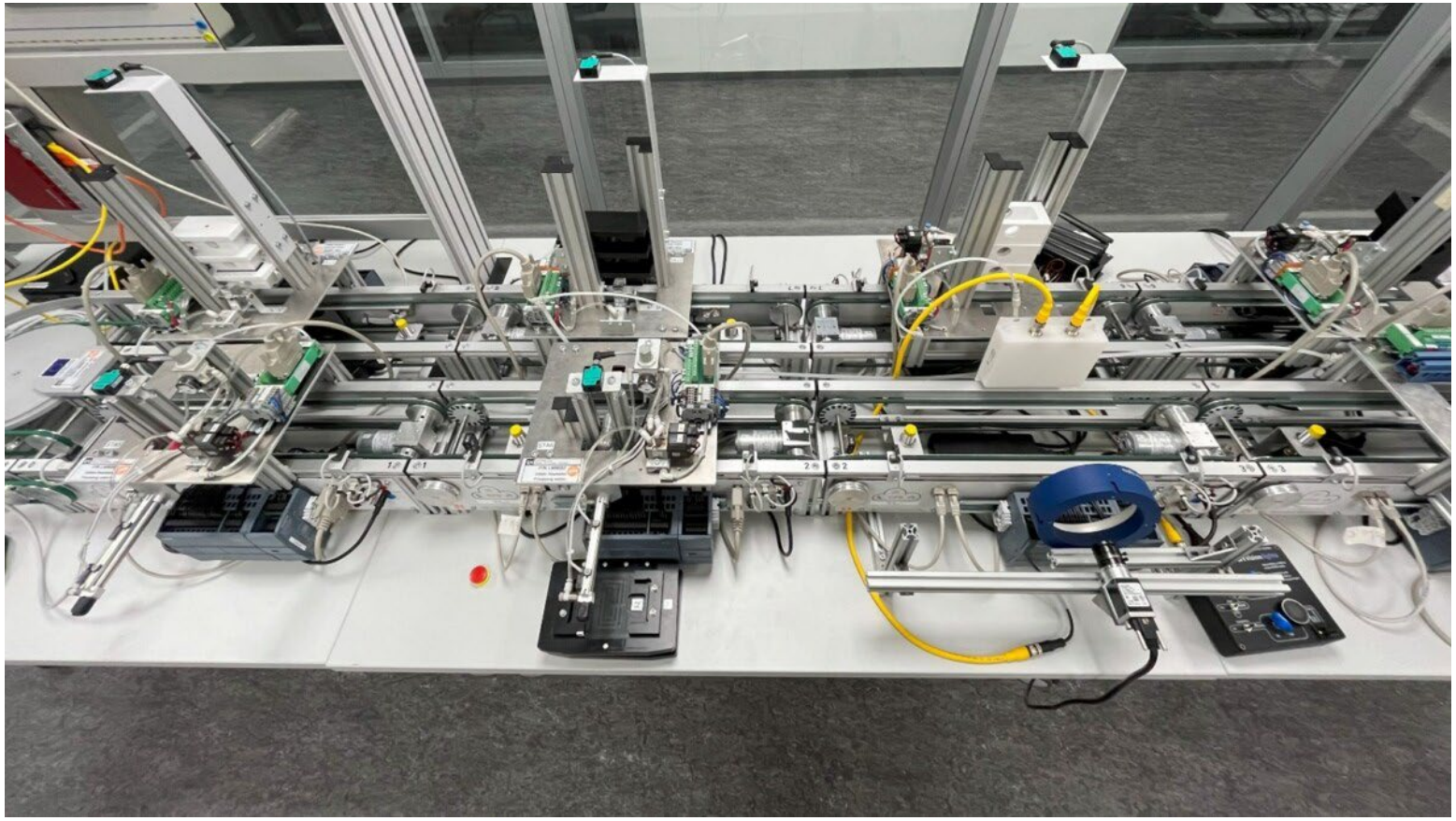
- Level 4/5: Enterprise Zone
  - ERP (Enterprise Resource Planning)
  - Disruptions ➔ prolonged downtime, with the potential for economic damage, failure of critical infrastructure, or revenue loss.
- Level 3.5: Demilitarized Zone (DMZ): used to be "air gap"
  - Firewalls and proxies, prevent threat movement between OT and IT
  - https://www.armis.com/blog/chapter-2-the-ot-air-gap-dissolved-a-playbook/)
- Level 3: Manufacturing Operations Systems Zone
  - Customized OT devices that manage production workflows on the shop floor (MOM, MES, Data historians)
  - Disruptions ➔ economic damage, failure of critical infrastructure, risk to people and plant safety, or lost revenue.

Purdue model levels and risks

- Level 2: Control Systems Zone
  - Systems that supervise, monitor, and control physical processes: SCADA, DCS, HMIs
- Level 1: Intelligent Devices Zone
  - Instruments that send commands to the devices at Level 0: PLCs and RTUs
- Level 0: Physical Process Zone
  - Sensors, actuators, and other machinery directly responsible for assembly, lubrication, and other physical processes
  - Disruptions ➔ this is where security incidents could become real (loss of production, fire, gas leak, explosion, etc).

Savonia Smart Factory

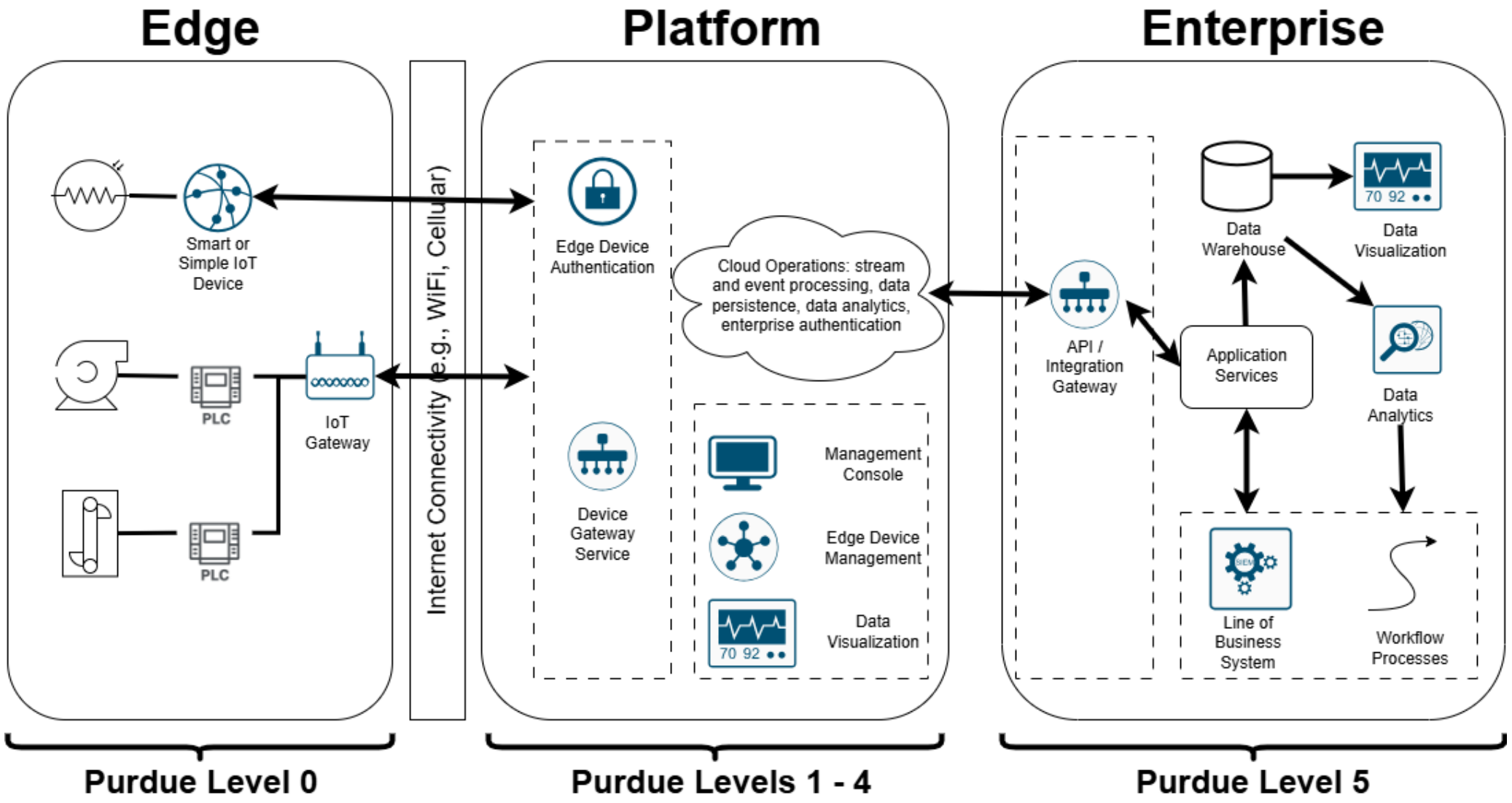
- Industry 4.0 smart factory located in classroom D1006



Revisions to Purdue model – IIoT and Cloud Services

- With Industrial Internet of Things (IIoT) data no longer lives entirely within the enterprise.
  - Cloud services
  - Wireless technologies (e.g. 5G)
- IIoT reference architecture:
  1. Edge
     - Traditional OT equipment (sensors and actuators)
     - IoT gateway: data operations, device management, access control, communication to networks
  2. Cloud Platform
     - Typically Platform-as-a-Service (PaaS)
  3. Enterprise
     - Backend applications

Gartner IoT Reference Architecture, check discussion here: https://www.spiceworks.com/it-security/cyber-risk-management/articles/industroyer-and-ot-security/

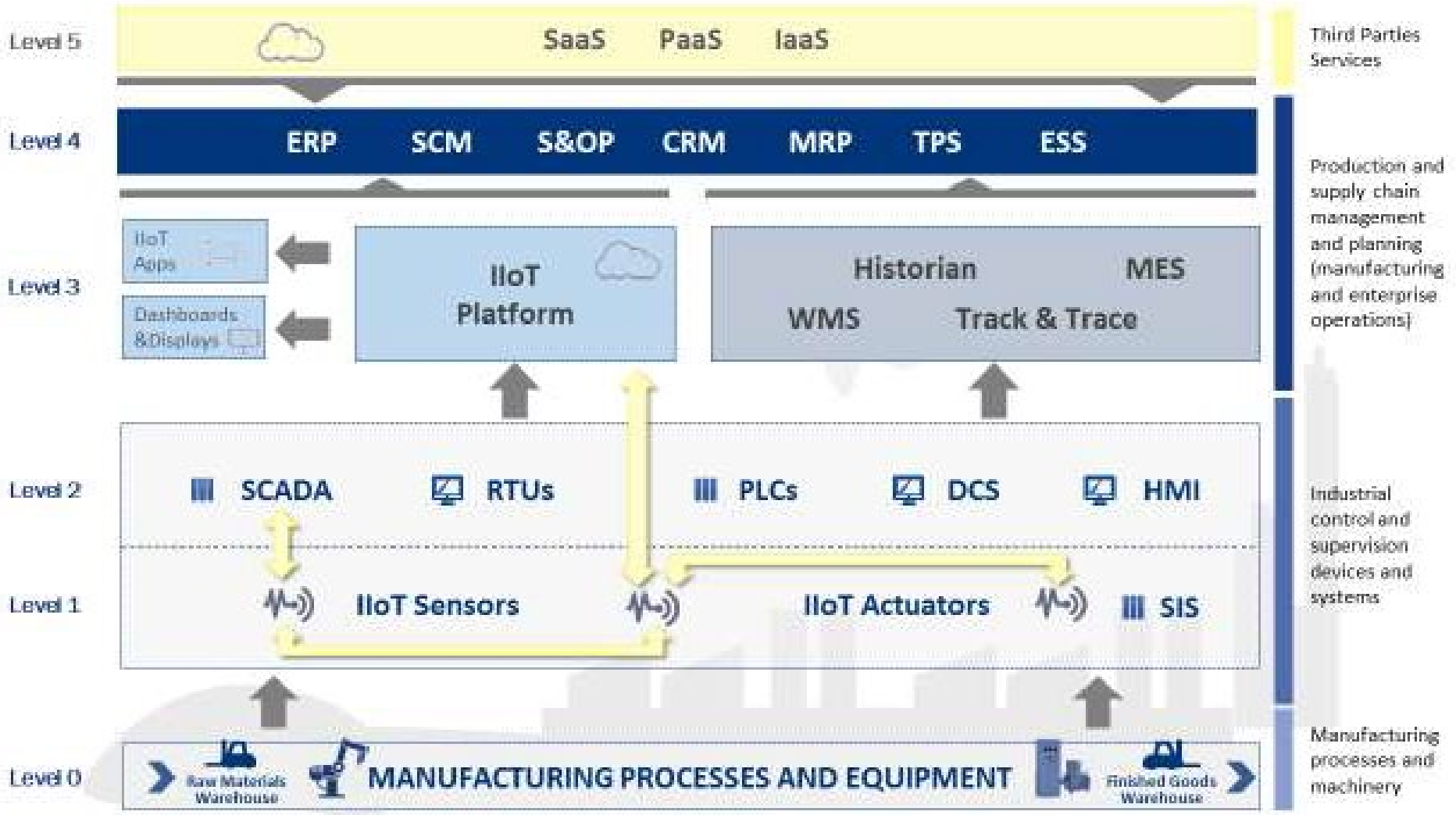


IIoT and the Purdue model

- Long-time trend: IT systems moving further down the traditional Purdue model architectural stack.
- Level 3: IIoT gateway ⇔ critical security concern
  - Could open up entire OT infrastructure to attack
- ENISA has proposed a revision to Purdue model (next page) which recognized Level 3 IIoT gateway ⇔ Level 1 IIoT device communication
  - https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Revised Purdue model (by ENISA)

https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot



SAVONIA

IoT Security Models

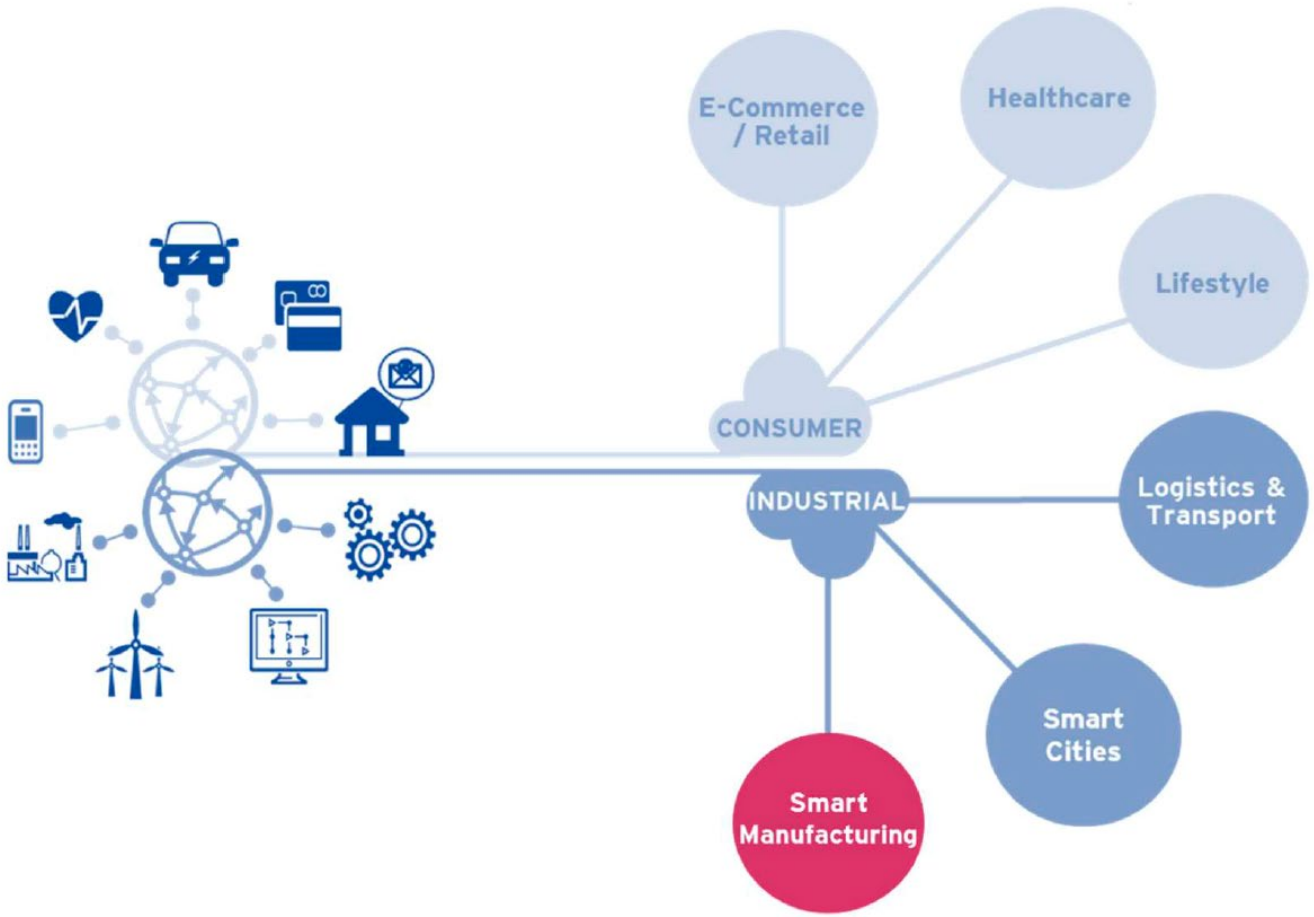
CIA triad (introduced earlier)

- **Confidentiality** involves the efforts of an organization to make sure data is kept secret or private
- **Integrity** involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.
- **Availability** involves making sure your data is available when you need it, and it does not take an inordinate amount of time to access it. This means that systems, networks, and applications must be functioning as they should and when they should.

The CIA triad is a common model that forms the basis for the development of security systems.

Read more: https://www.fortinet.com/resources/cyberglossary/cia-triad

Industrial IoT vs Consumer IoT



https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Focus and implications of security

SELECTED CHARACTERISTICS	INTERNET OF THINGS	INDUSTRIAL INTERNET OF THINGS
Focus	Protection of personal data and assets.	Prevention of process interruption, safety
Priorities	Confidentiality, Integrity, Availability	Availability, Integrity, Confidentiality
Device Failure Implications	No critical consequences	Interruption of processes, Impact on production, Potential physical threats
Reaction to threat	Possible shut down and remediation	Maintenance of operation
Upgrades and Patch Management	Possible during operation time, no reasons for significant delays.	Need to be scheduled and performed during down time, which may postpone the upgrade for a considerable amount of time.
Lifecycle of the device	Relatively frequent upgrades of equipment	Long lifespan of the devices (over 15 years[47])
Conditions of deployment	Regular	Harsh environments (temperature, vibration, etc.)

Table 4: Indicative differences in terms of selected aspects between IoT and IIoT

https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Observations

- CIA triad lists relevant focus areas for both consumer IoT and IIoT
- However, priorities are different.

source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

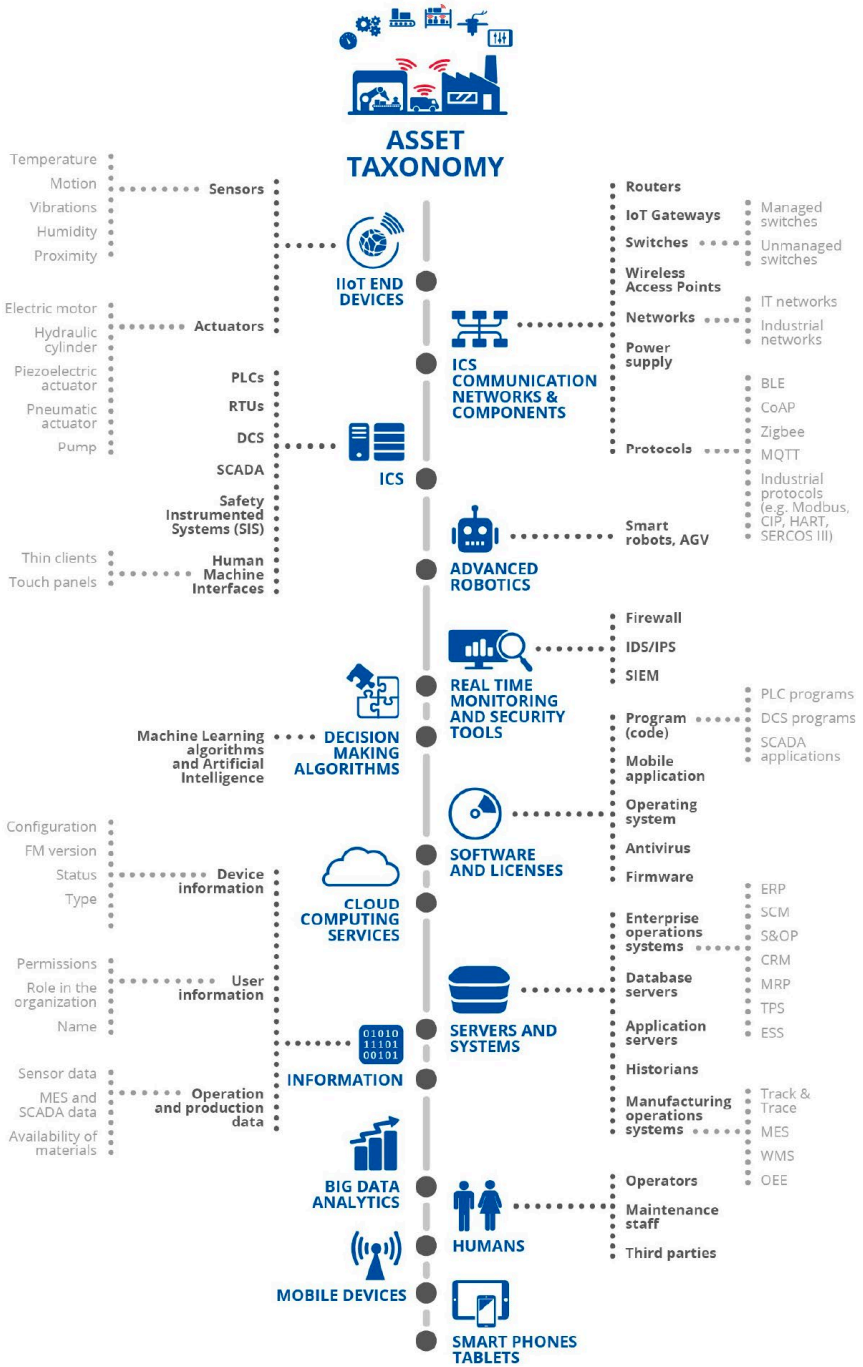
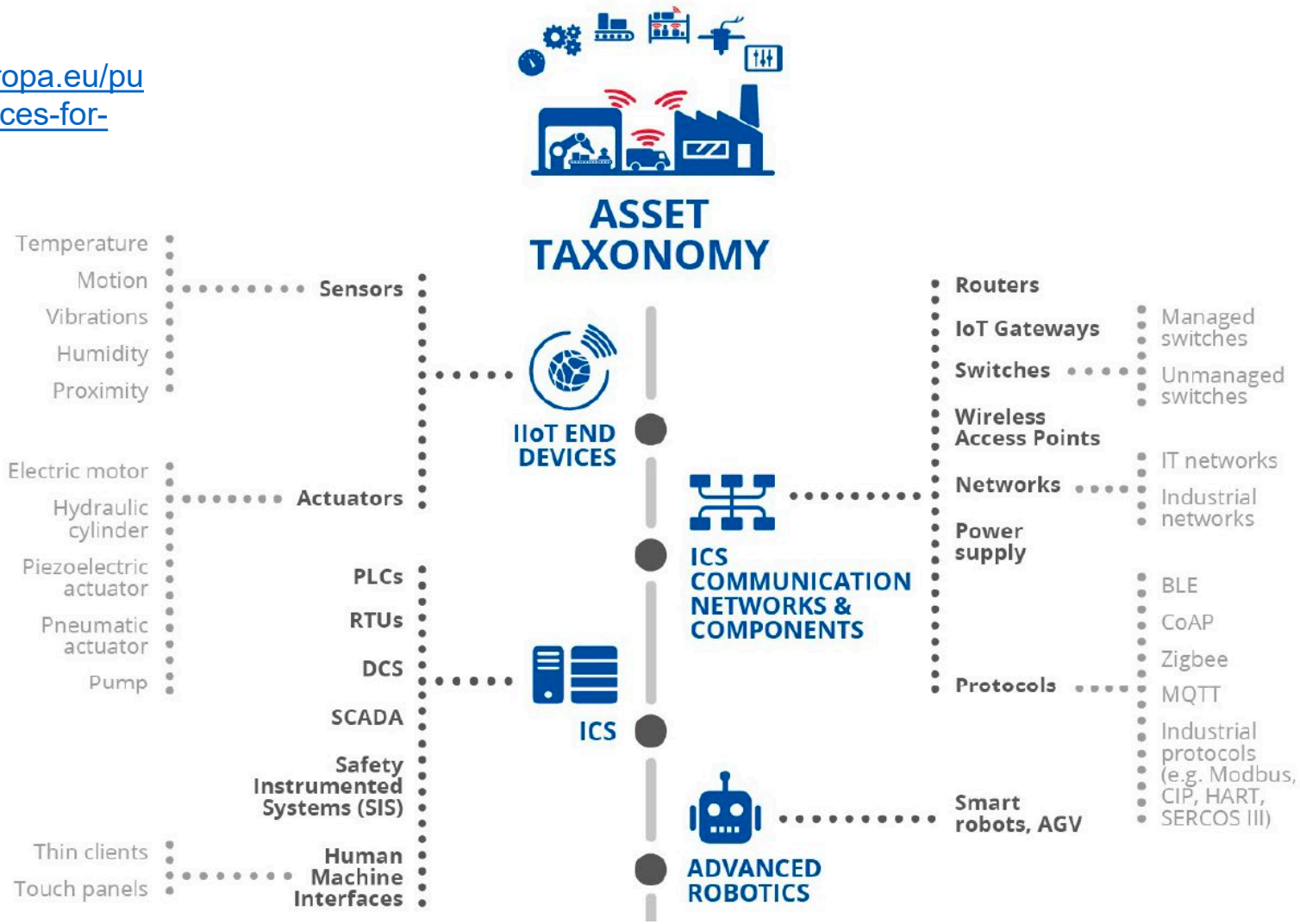


Figure 6: Industry 4.0 asset taxonomy

source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot



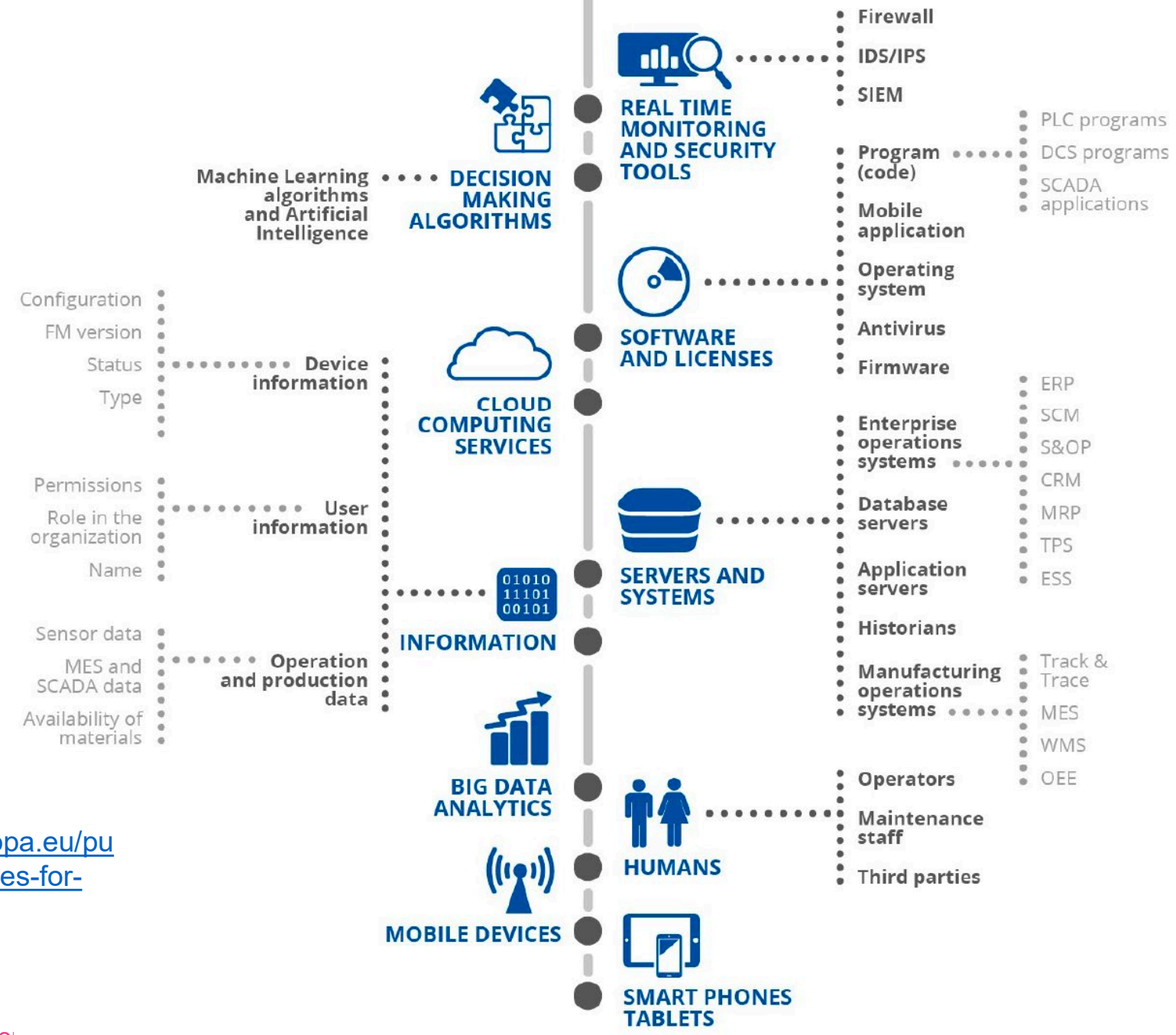


Figure 6: Industry 4.0 asset taxonomy

source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Asset criticality for cybersecurity

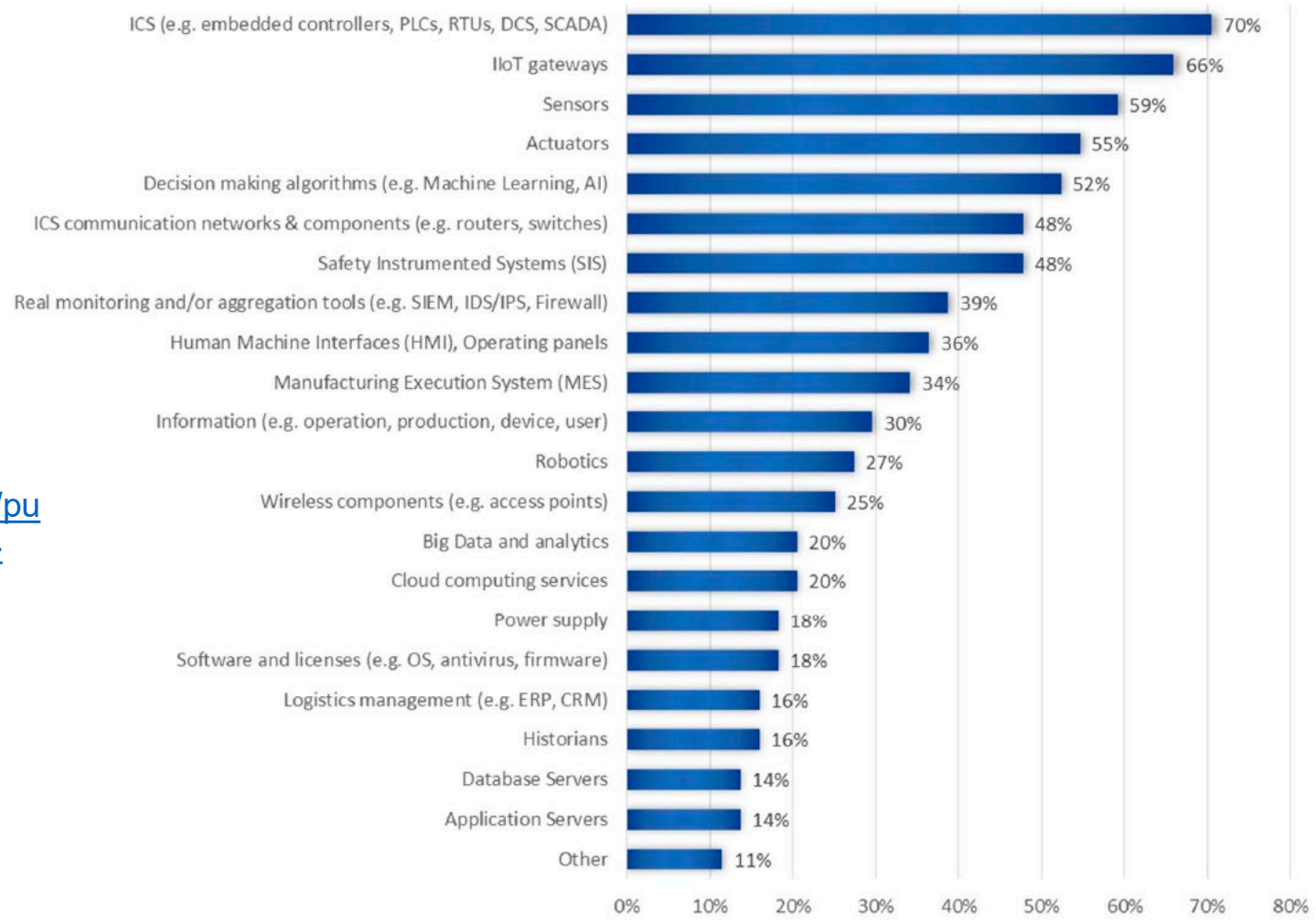


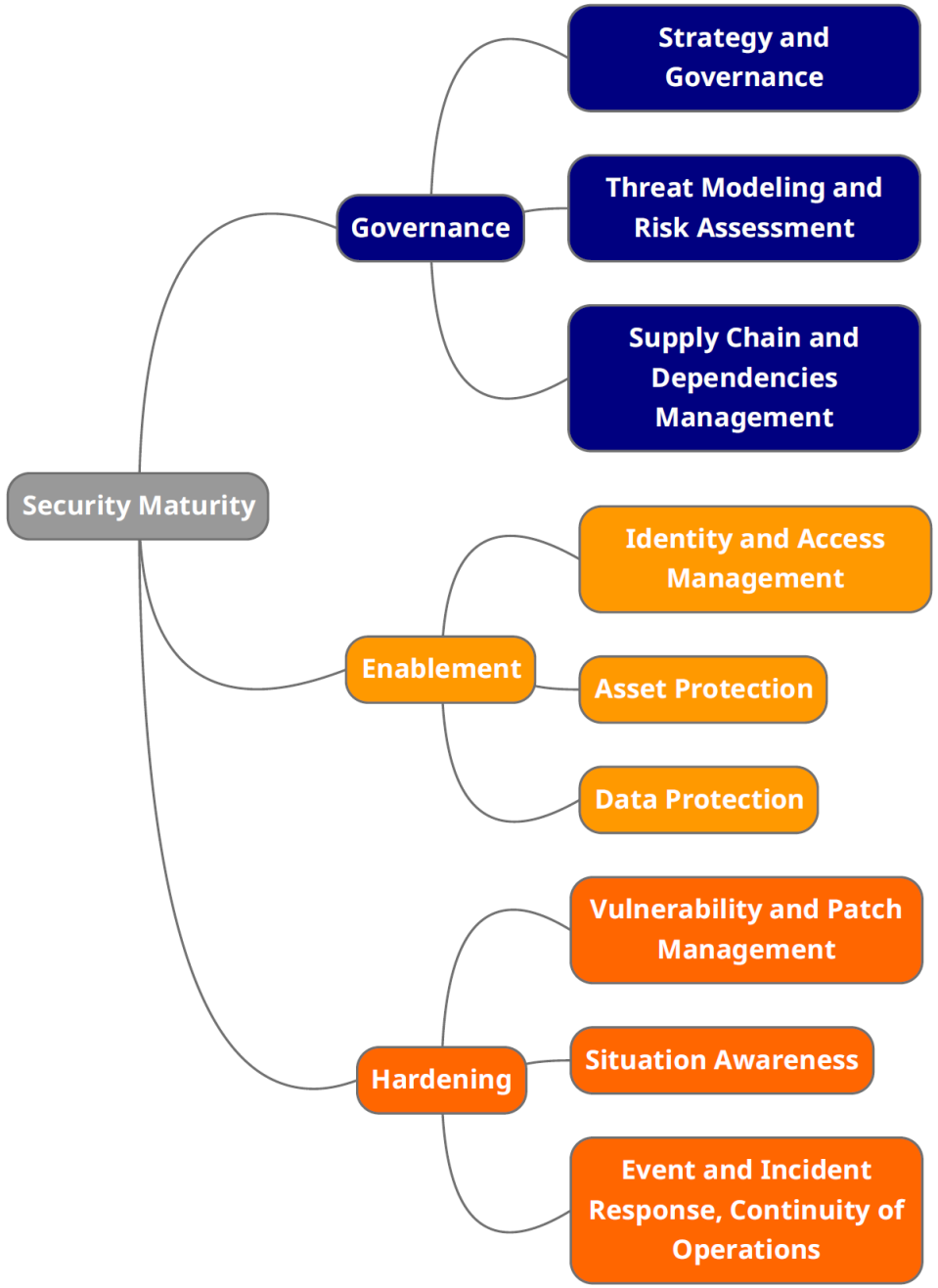
Figure 7: Asset criticality

source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

IoT Security Maturity Model (SMM)

- Industry IoT Consortium has developed a comprehensive model for IoT security.
- This model has been introduced in the following publications:
  - Website: https://www.iiconsortium.org/smm/
  - White paper: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf
  - How-to manual: https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

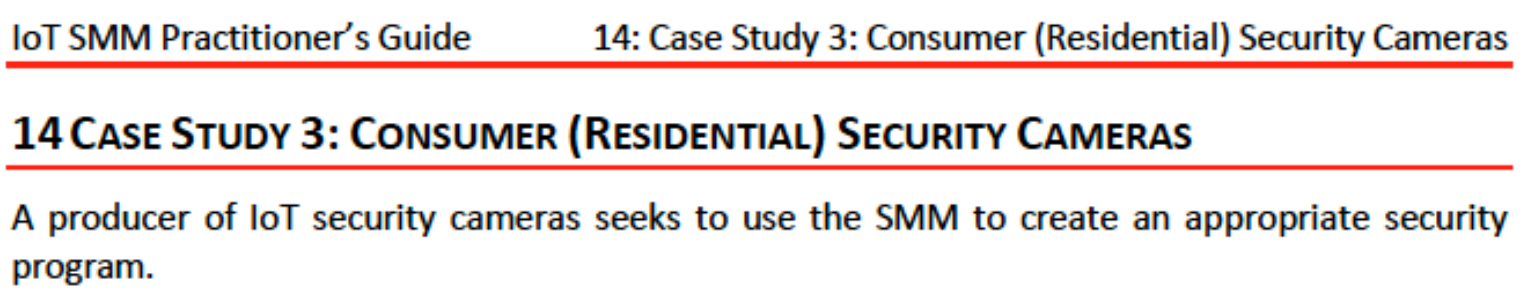
IoT Security Maturity Model (SMM) by Industry IoT consortium



Study more here:
https://www.iiconsortium.org/smm/

Assignment: CCTV cameras

- Write a one-page summary with observations on case study on residential CCTV cameras in https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf
  - What is the relative importance of security domains?
  - What practices on subdomains you think are important for this case?



IoT SMM Practitioner's Guide 14: Case Study 3: Consumer (Residential) Security Cameras

14 Case Study 3: Consumer (Residential) Security Cameras

A producer of IoT security cameras seeks to use the SMM to create an appropriate security program.

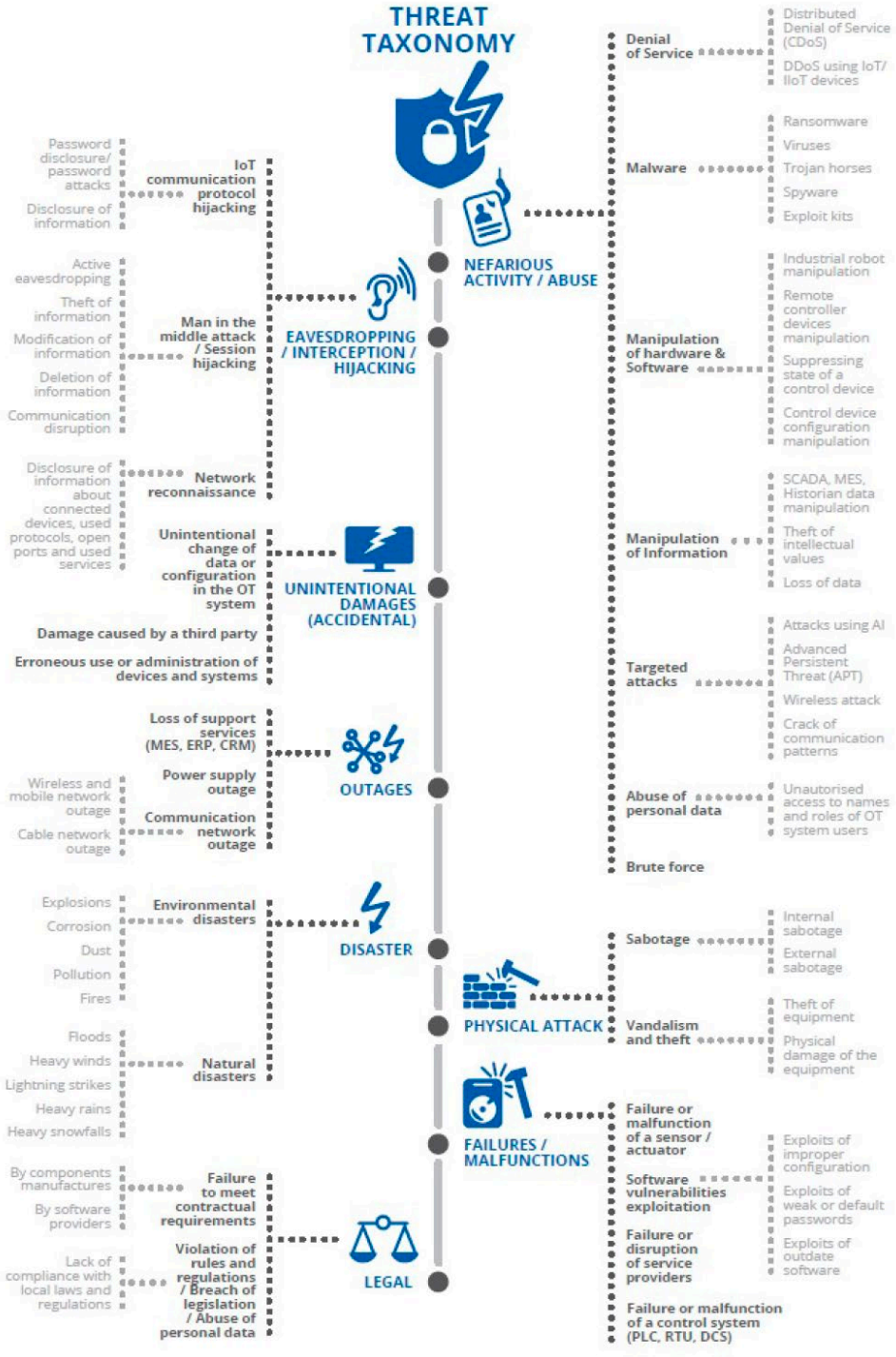
SAVONIA

Threats

IIoT threat taxonomy

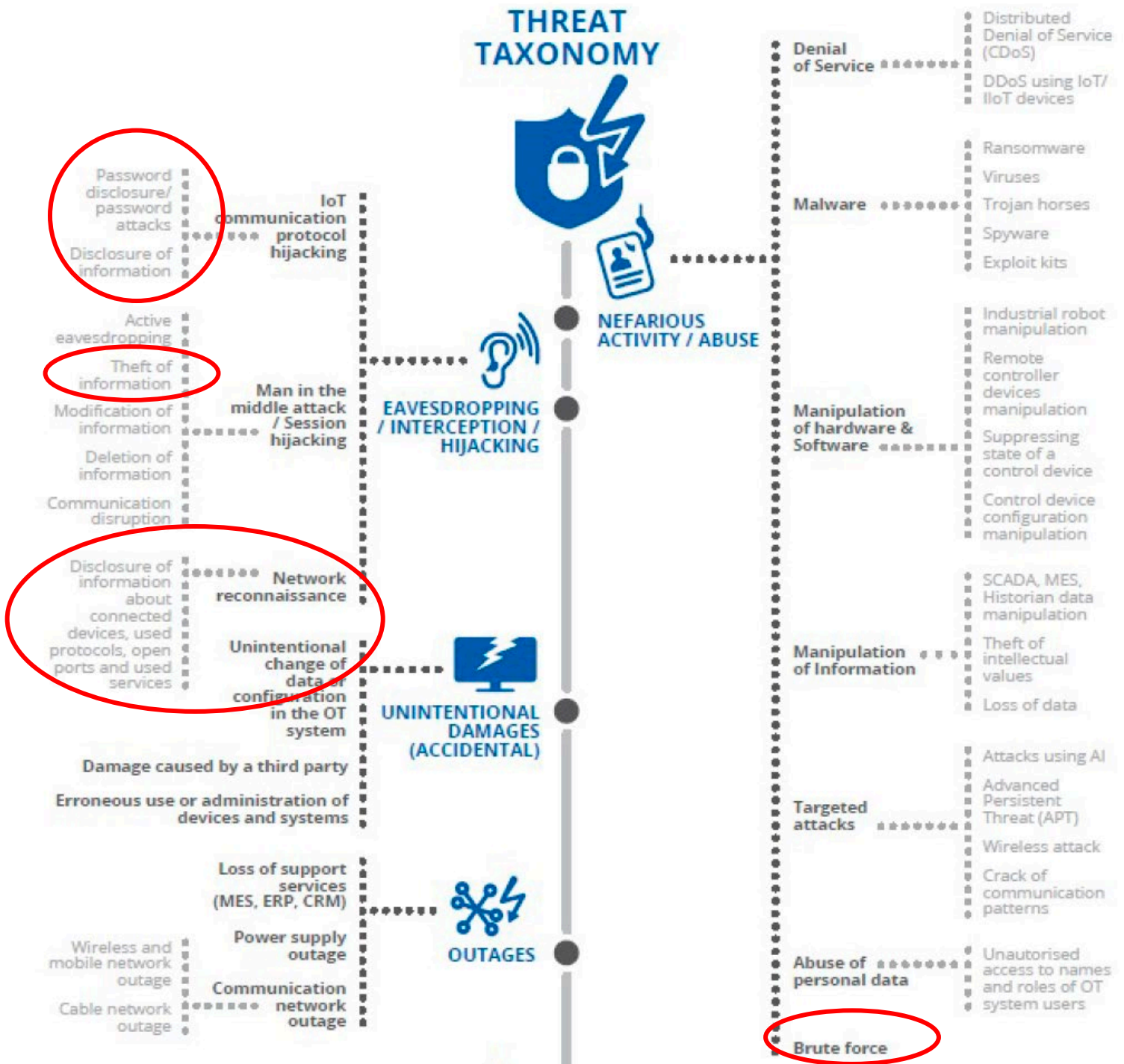
- In the ENISA document which we studied earlier, a taxonomy of threats regarding assets is drawn.
- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

IIoT threat taxonomy

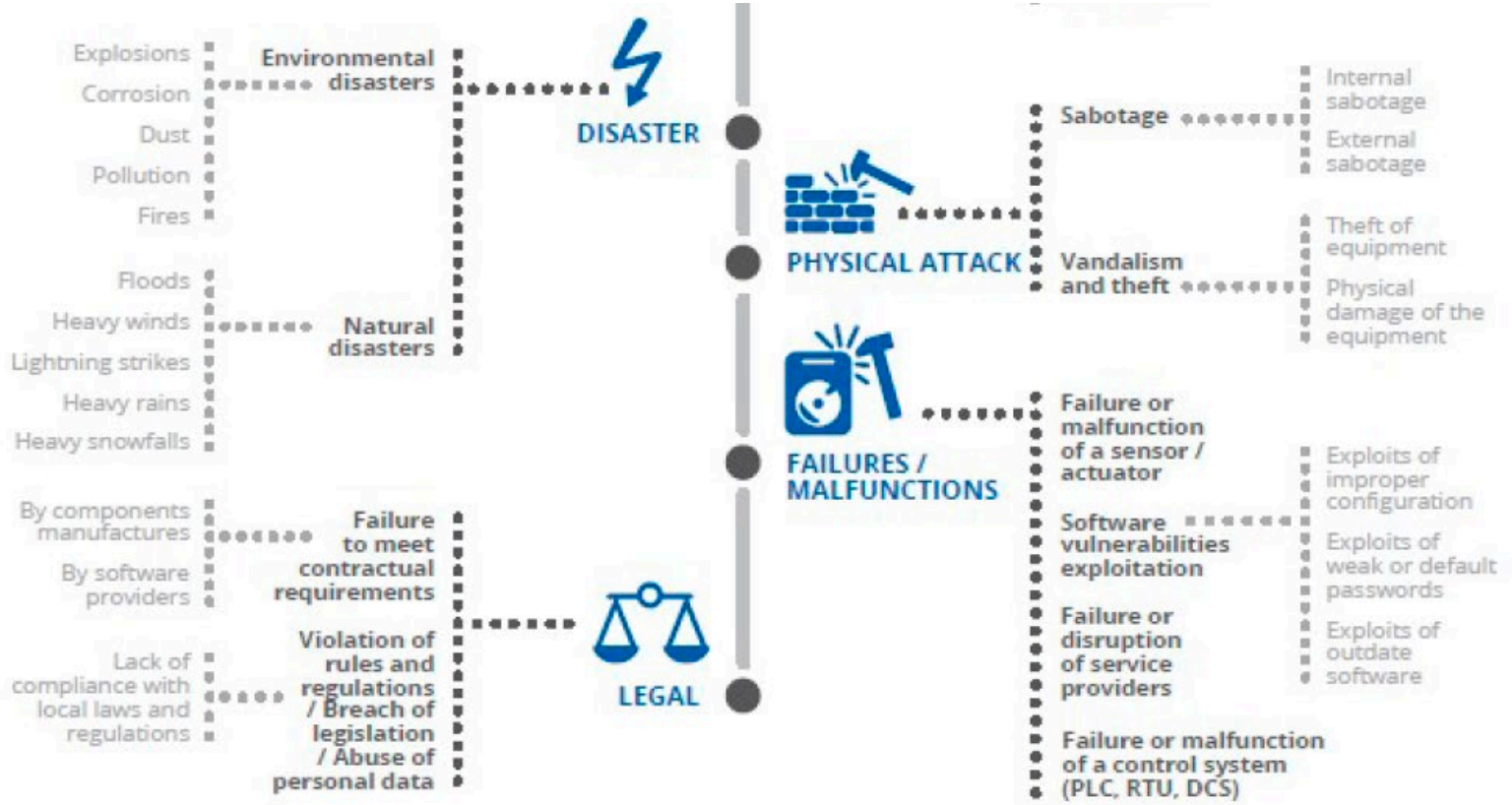


source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Lab 2 exercises



source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot



source:
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Threat modeling

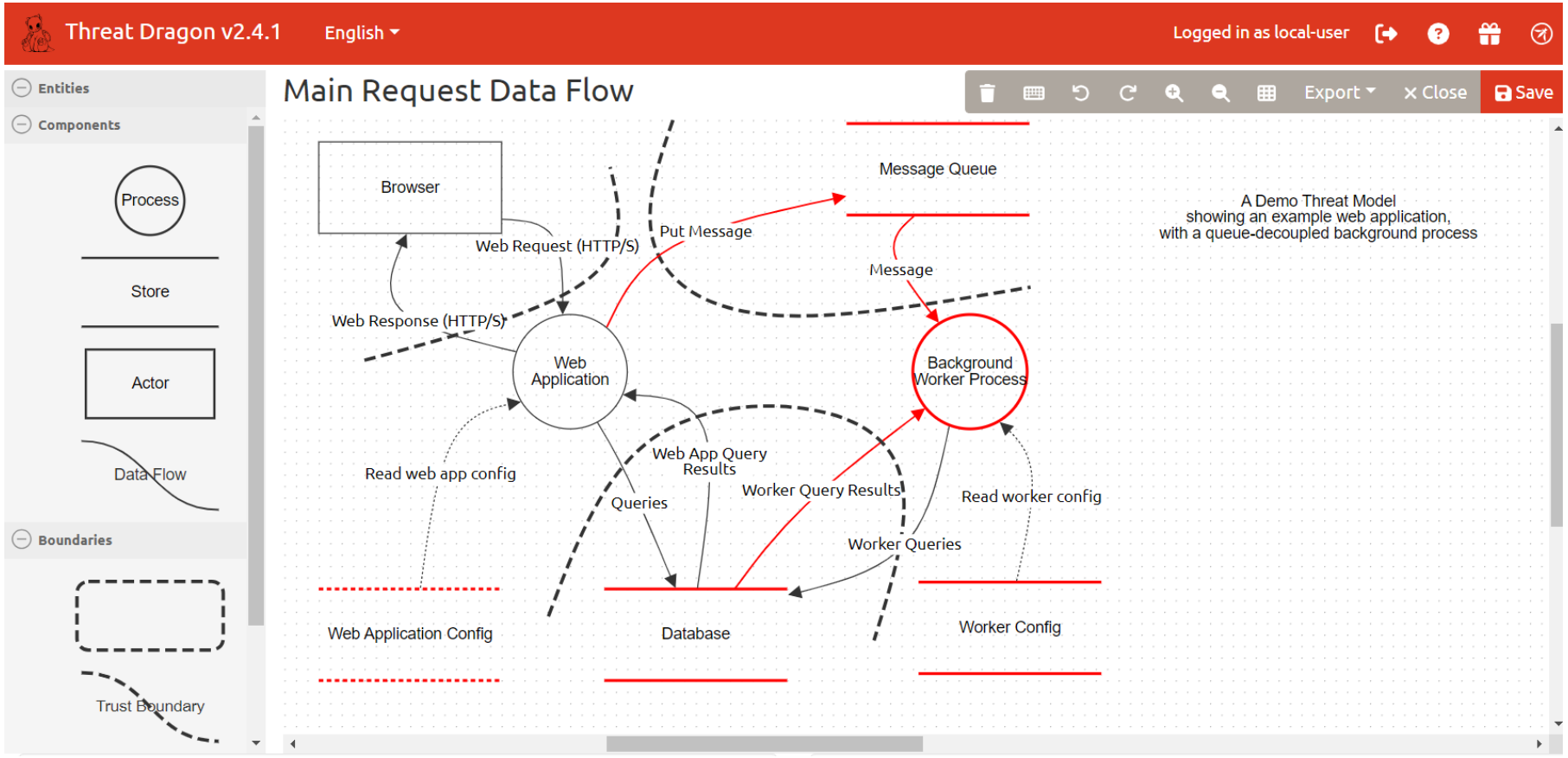
- According to OWASP foundation (https://owasp.org/www-community/Threat_Modeling):
  - Threat modeling is a family of activities for improving security by identifying threats, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.
  - A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device).
- Threat modeling is a **planned activity for identifying and assessing application threats and vulnerabilities**.
- Threat modelling techniques are best applied to inform the design and development phases of a technology system or service life cycle.

Threat modeling process

- OWASP threat modeling process (https://owasp.org/www-community/Threat_Modeling_Process#introduction) consists of four steps:
  1. Step 1: Scope your work
     - Drawing diagrams, often data flow diagrams.
     - Identifying entry points
     - Identifying trust levels that represent the access rights
     - Reading a user story or creating one.
  2. Step 2: Determine Threats
     - STRIDE methodology (https://en.wikipedia.org/wiki/STRIDE_model)
  3. Step 3: Determine Countermeasures and Mitigation
     - Accept, eliminate, mitigate, transfer
  4. Step 4: Assess your work

Data flow diagram example: library website

- Tool: Threat Dragon: https://owasp.org/www-project-threat-dragon/



STRIDE

- Each threat is a violation of a desirable property for a system
- Table below from https://en.wikipedia.org/wiki/STRIDE_model

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Source: https://en.wikipedia.org/wiki/STRIDE_model

CIA triad