

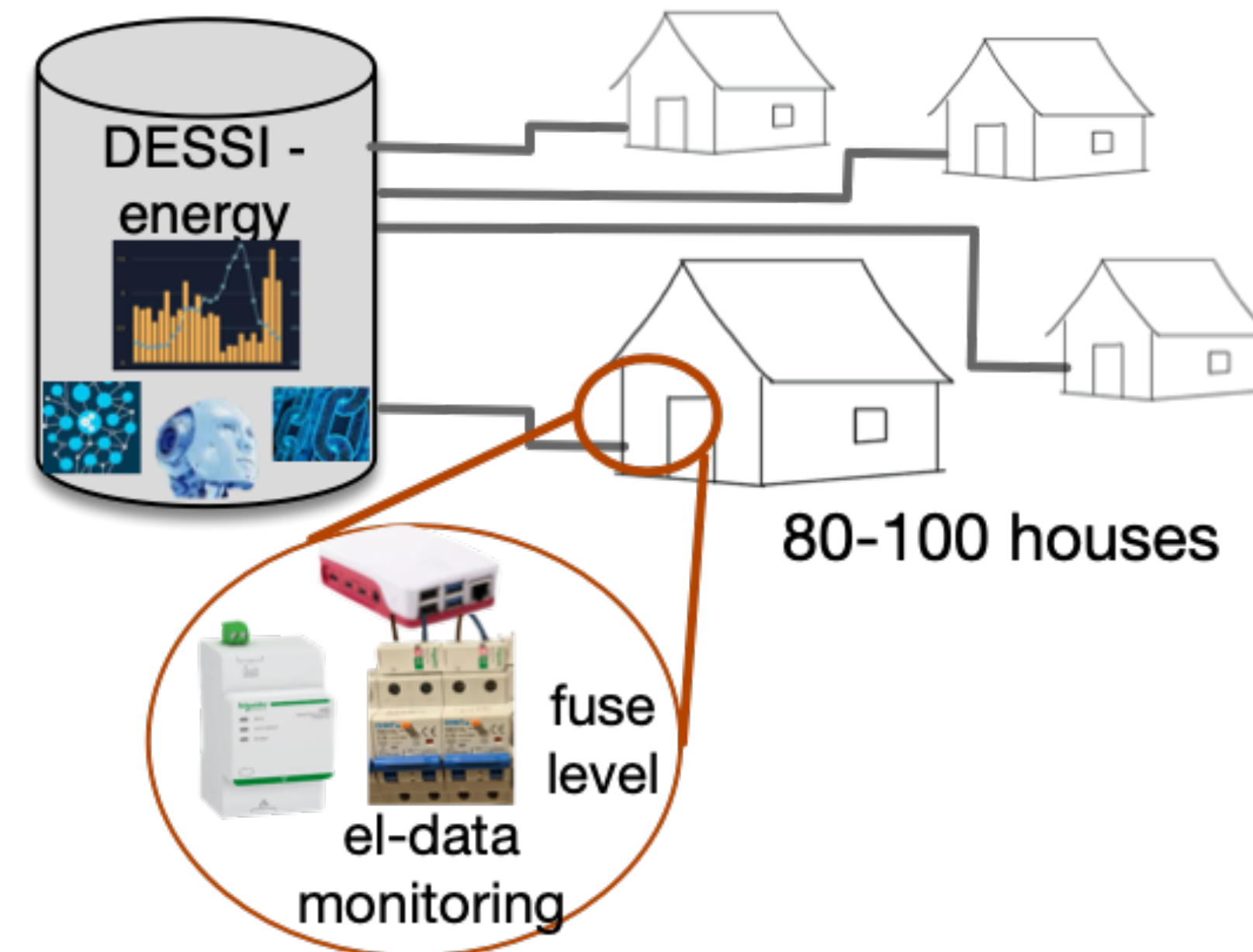
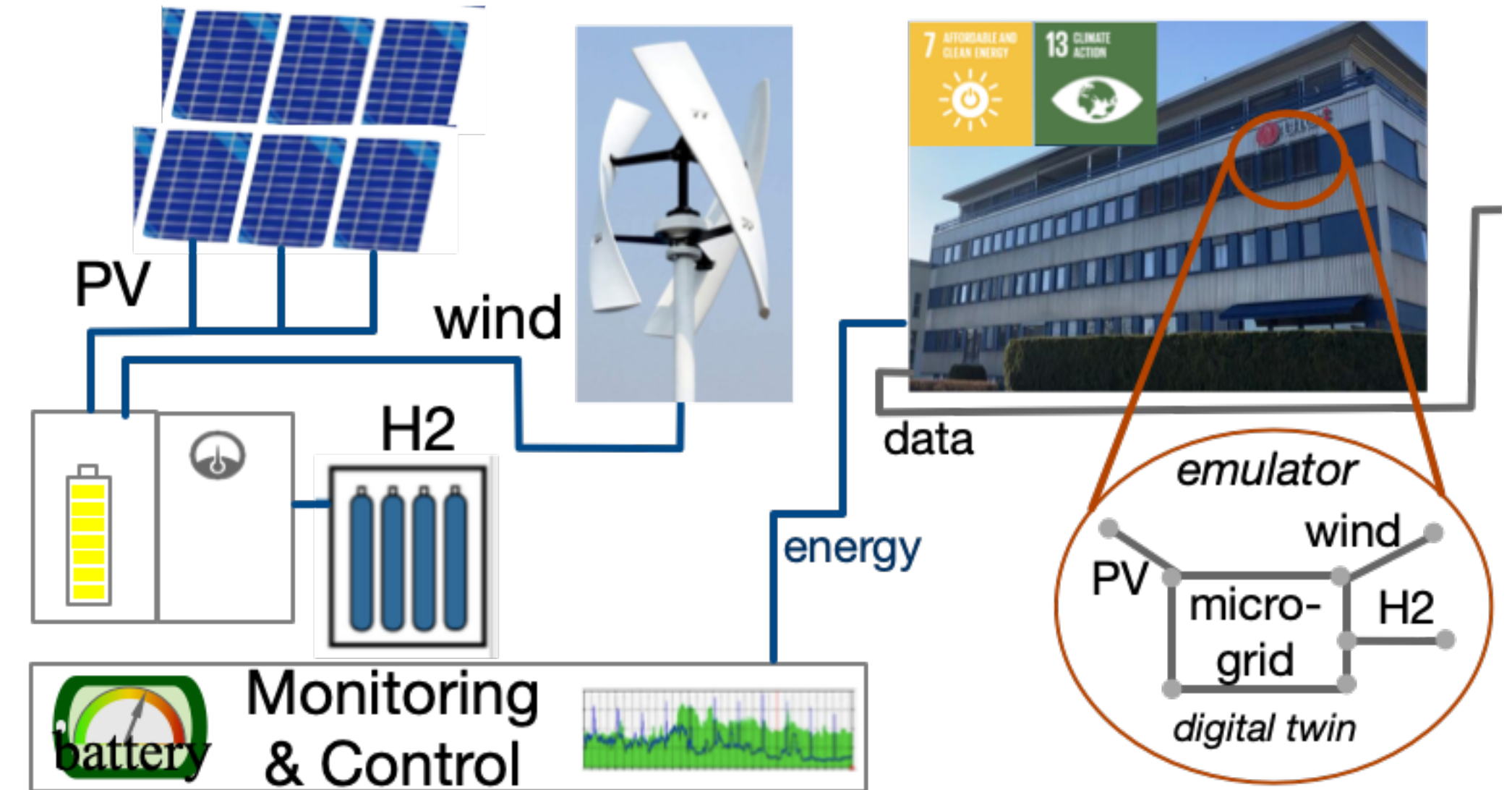
UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

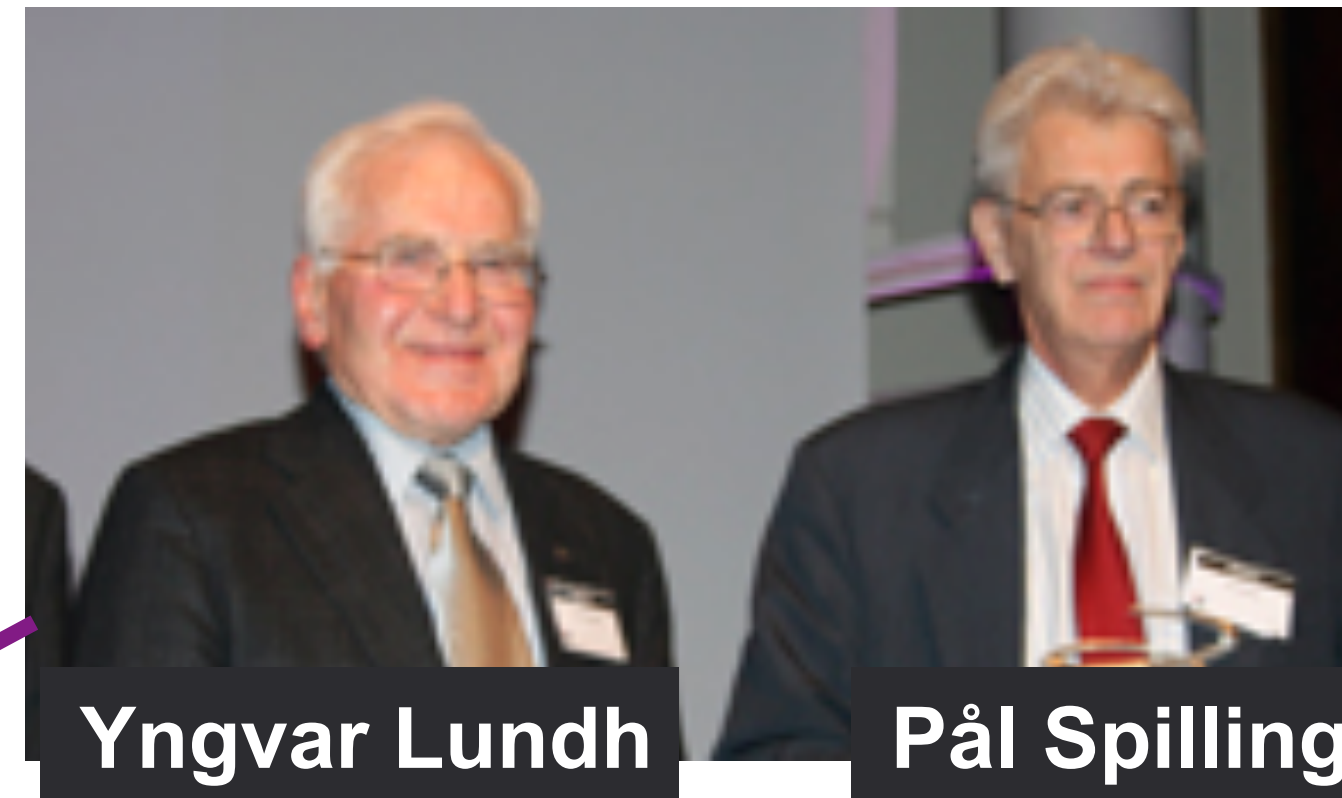
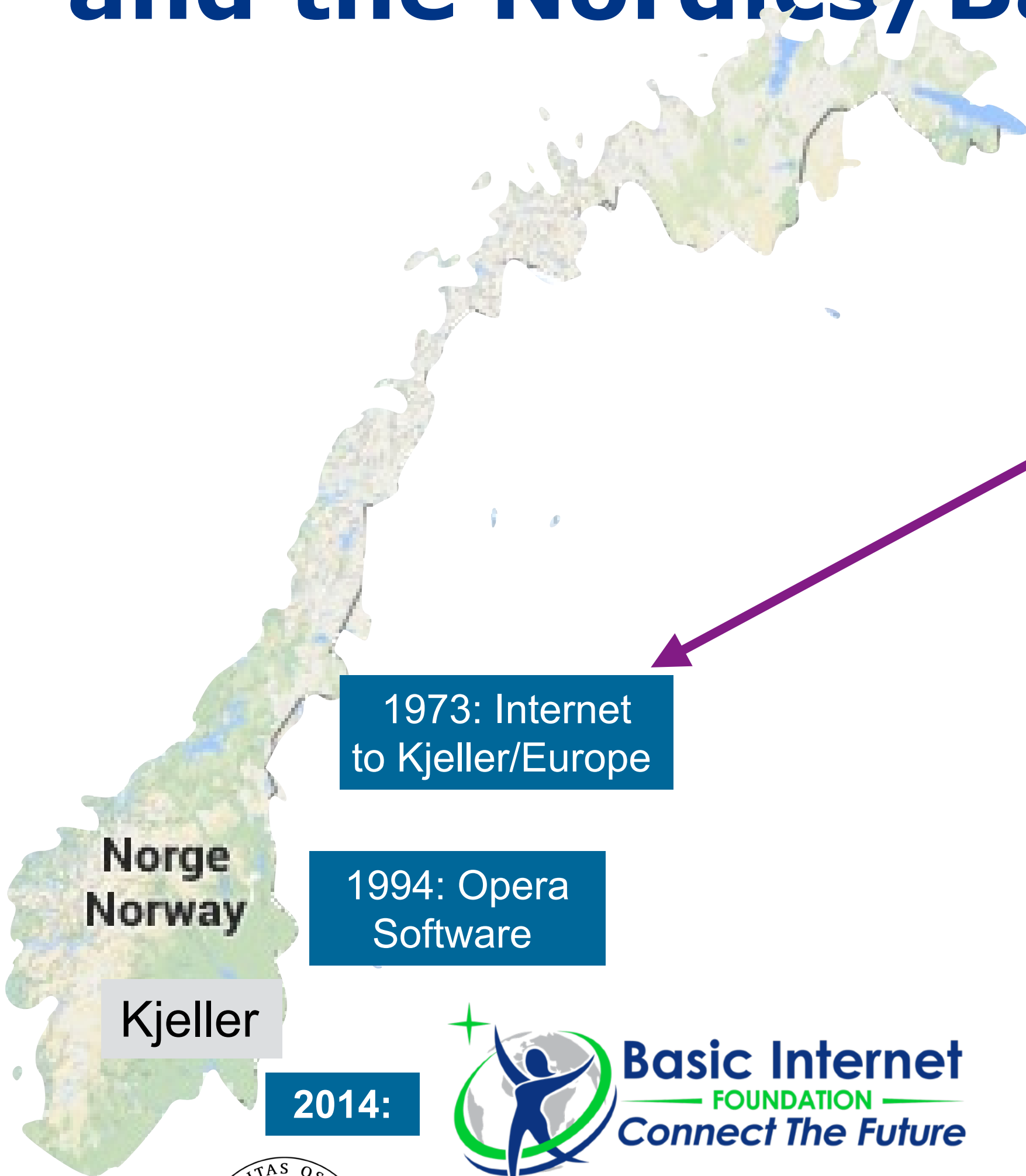
L1 Introduction

Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

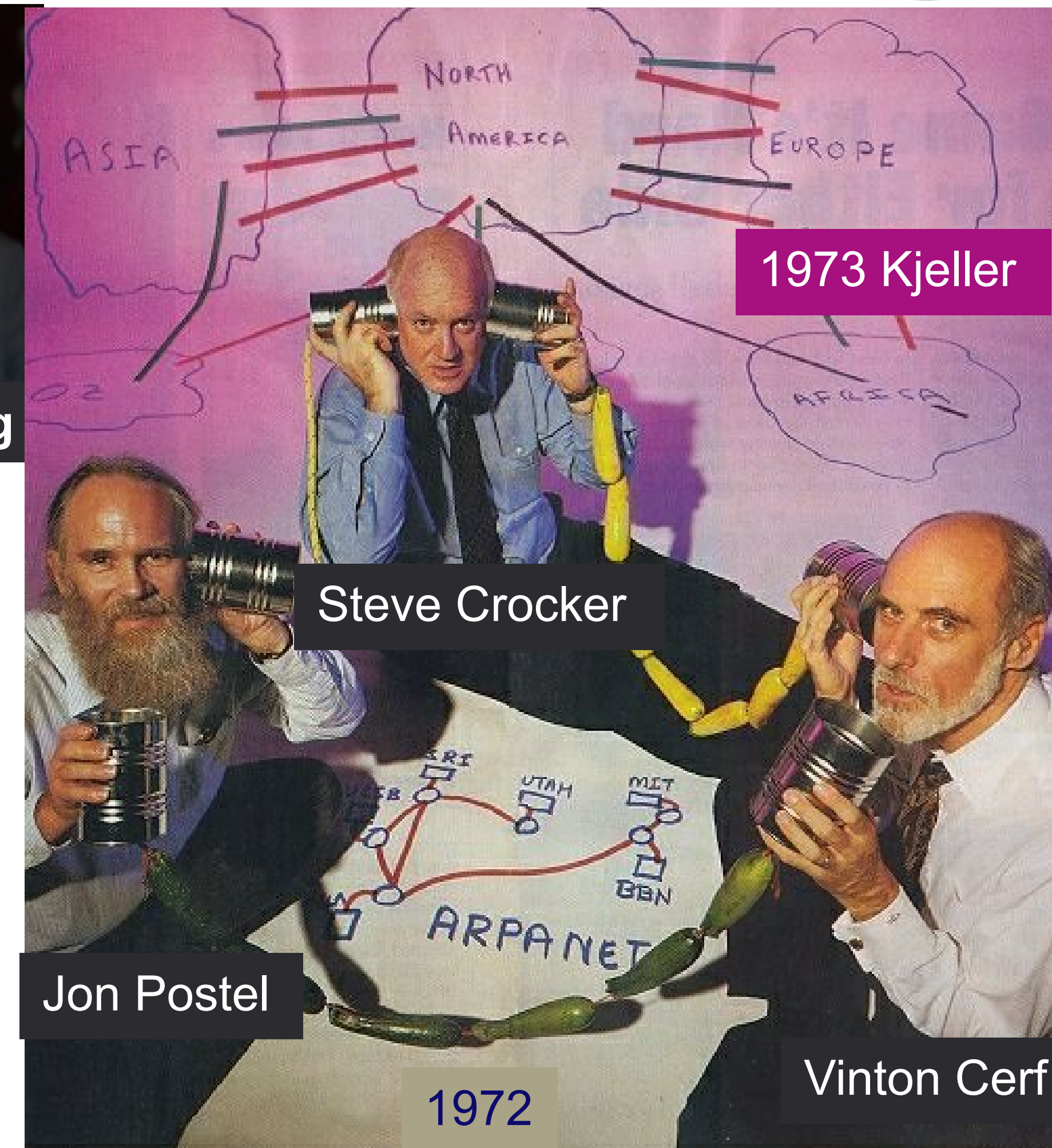


Inclusive digitalisation in Norway and the Nordics/Baltics (N8)



Nordics & Baltics (N8)

- php, OpenSource, Linux, Skype, Spotify
- Opera Software, FAST search
- Nokia, Ericsson
- GSM
- GovStack.global, X-Roads



Source: <http://www.michaelkaul.de/History/history.htm>

TEK5530: Before we start - interactivity - participation

Reach out: Josef Noll +47 9083 8066 (ph, SMS, WhatsApp/Threema/Signal/Telegram/Wire....)

Zoom

- have camera on if possible (easier for me to talk to people, not to blank screens)
- say hello from everybody before we start the lecture (5-10 min social talk)
- fixed stops to ask questions

Other forms for feedback

- directly through WhatsApp/Telegram.../Metamost?
- Exchange through Canvas?
- common Telegram/WhatsApp/Signal/Threema group?

Info on our wiki: <http://its-wiki.no/wiki/TEK5530>

Overview

- Expectations
- Lecture overview & Group work
- Exam
- Topic introduction

Expected outcome:

- Describe application-driven security and establish challenges of sensor-driven systems
- Provide industrial examples, e.g. Smart Grid and automatic meter readings
- Establish application-driven security goals as well as the semantics of your system
- Be able to describe the security impact of components and sub-systems
- Perform a multi-metrics analysis to measure the system security
- Analyse application goal versus system security, be able to describe differences and mitigation solutions
- Be able to analyse and present own thoughts on a scientific paper
- Group work with distribution of workload

Department of Technology Systems (ITS) at Kjeller



Long and nice history on communications and the birth of internet

Was home of the first ARPANET link to Europe made possible by internet-pioneer Pål Spilling.



Cooperation with the Kjeller-Institutes

First implementation of OLSR routing protocol

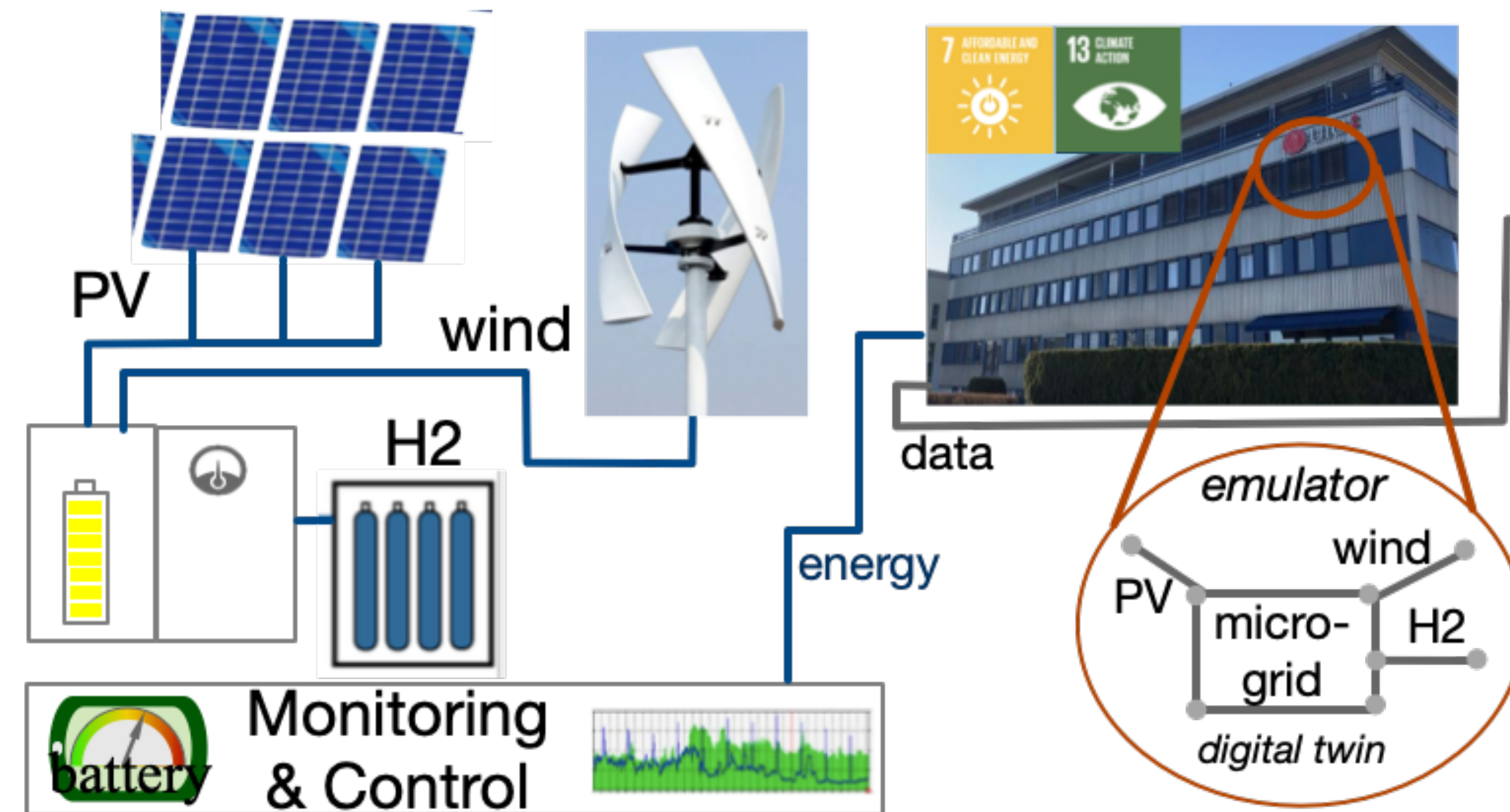
The threat dimension

- Ukraine blackout
- Surveillance camera DDoS
- AMS attack surface
- Exploiting cloud-elasticity
- Smart home – Always online
- Autonomous vehicles
- Ransomware
- Unauthorized resource usage (e.g. mining)

- Worth reading:
 - OWASP Internet of Things project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
 - Amazon Web Services IoT
<https://aws.amazon.com/iot/>

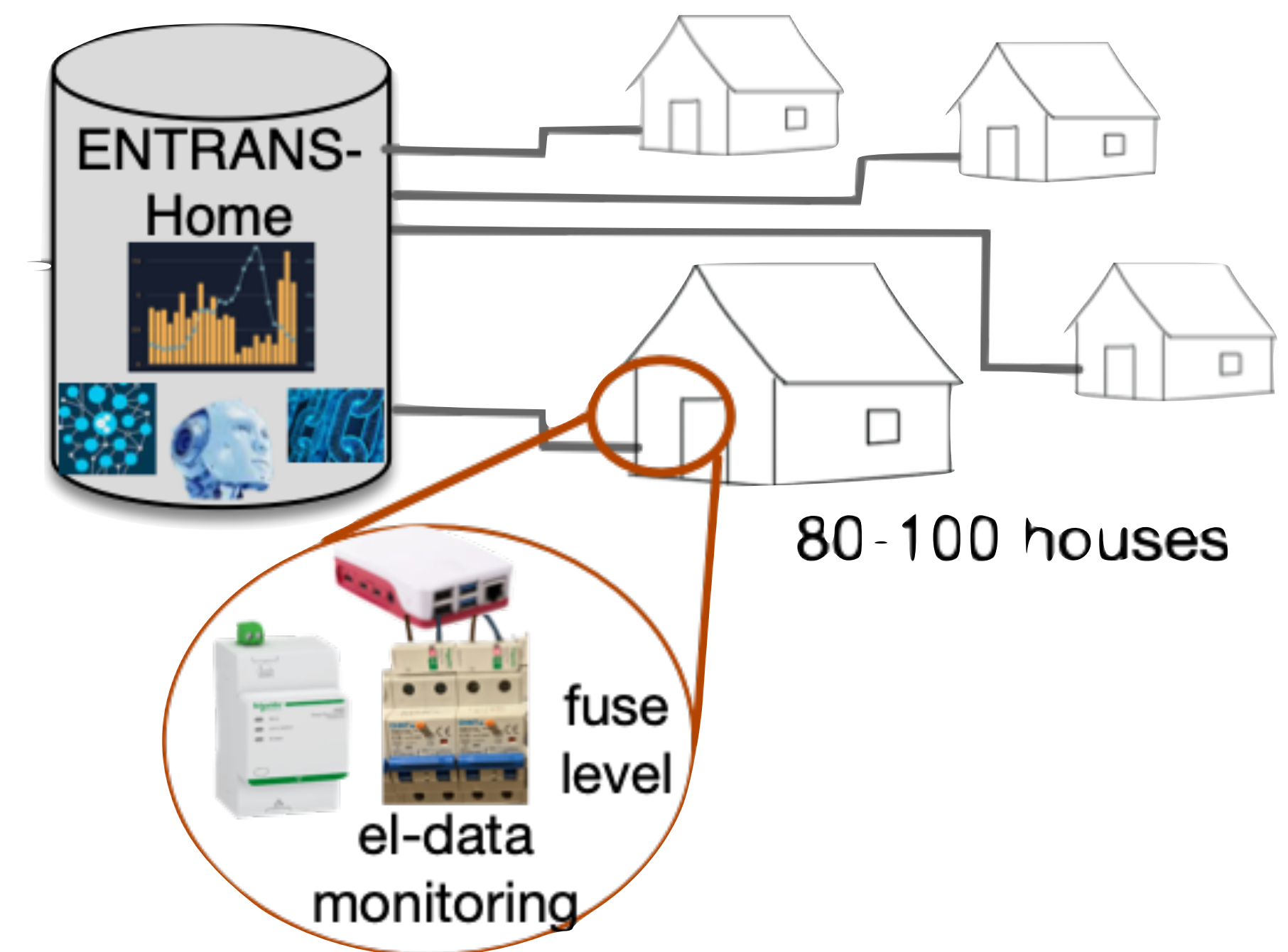
Problem 1: Energy Monitoring & Controlling

- UiO@Kjeller building
 - Smart campus management
 - Energy consumers
 - Meter data
 - Analyze saving possibilities
 - Potential for renewables or efficient use of spill heat/combined energy usage
 - Building automation and communication between buildings



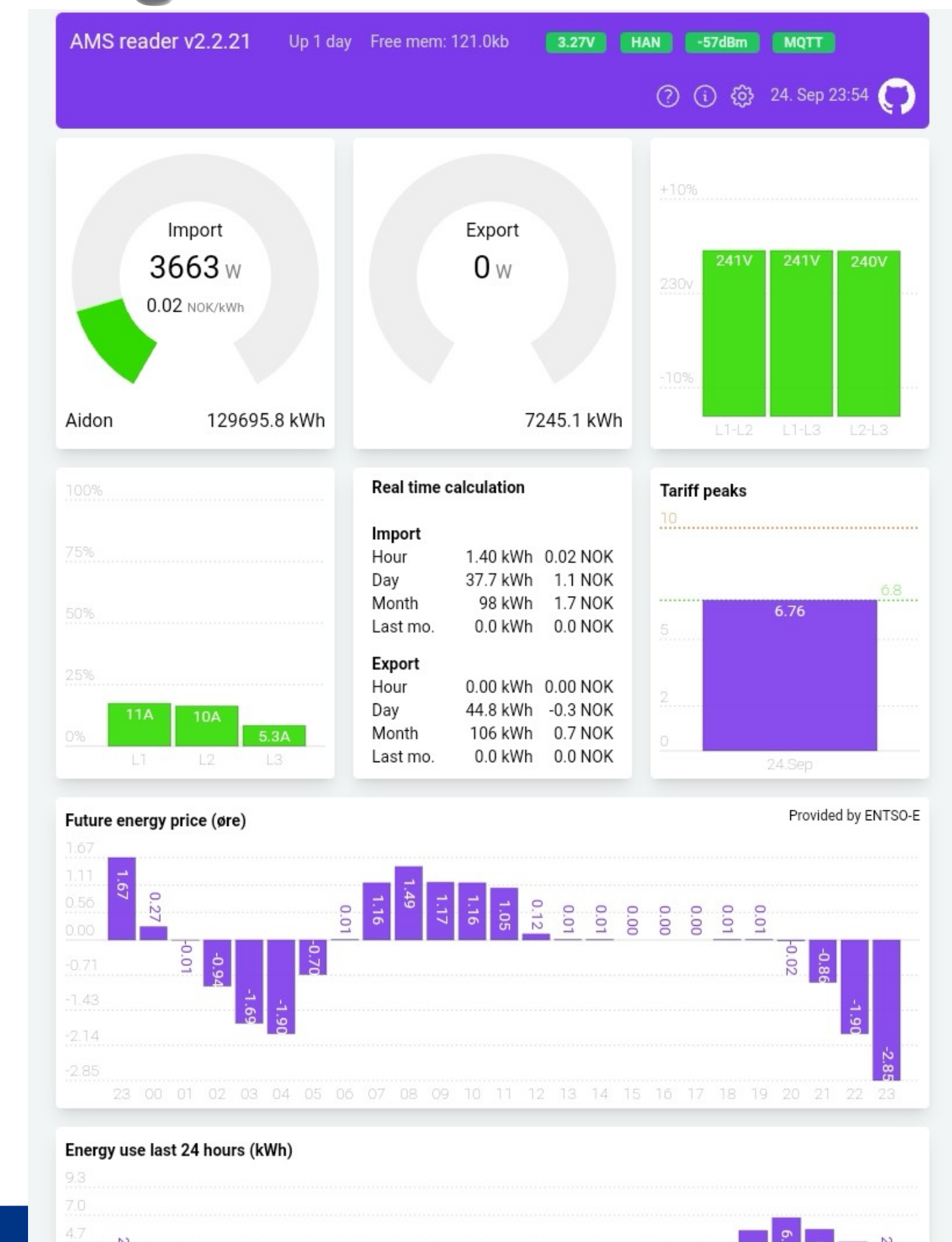
Problem 2: Home automation

- Home energy costs are expected to rise
- Consumption is relatively non-flexible (schedule, convenience, insurance)
- Heterogenous installation with equipment from random vendors
- Smart plugs, meters, app-controlled lamps, heating elements
- Key in large consumers – largest possible benefit:
 - Electric car charging
 - Heat pumps (generally heating, hot water)
- Integration of renewables



Problem 3: Security and Privacy in Home automation

- Challenges to analyze:
 - Identify large consumers, integrate meter readings and introduce some kind of actuators or invest in «smart» device
 - Standards 10 years ago and 10 years from now: future proofing?
- Control beyond «on-off»?
- How to integrate e.g. solar panel production and energy storage
- Smart Meter monitoring & Home Automation & controlling



Problem 3: Building safety

- This time focus only on car charging
 - Lithium batteries are in practice inextinguishable once caught fire
 - Parking cellars, houses are specially at risk
- Sensors for monitoring the charge process:
 - Meters, temperature sensors, charge profile, prediction
 - Alarms, active measures (reduction, cutoff of electric power, CO2)
- Communication
 - Cellars are usually bad for wireless

Problem 4: Farming

- Precise management of farming processes
- Monitoring and predicting needs and events
- Sensors for physical parameters
- Prediction based on historical results and models
- Control of machinery, predictive maintenance
- Safety and security
- Inventory, integrated management of equipment, consumables, chemicals etc.
- Wireless communication



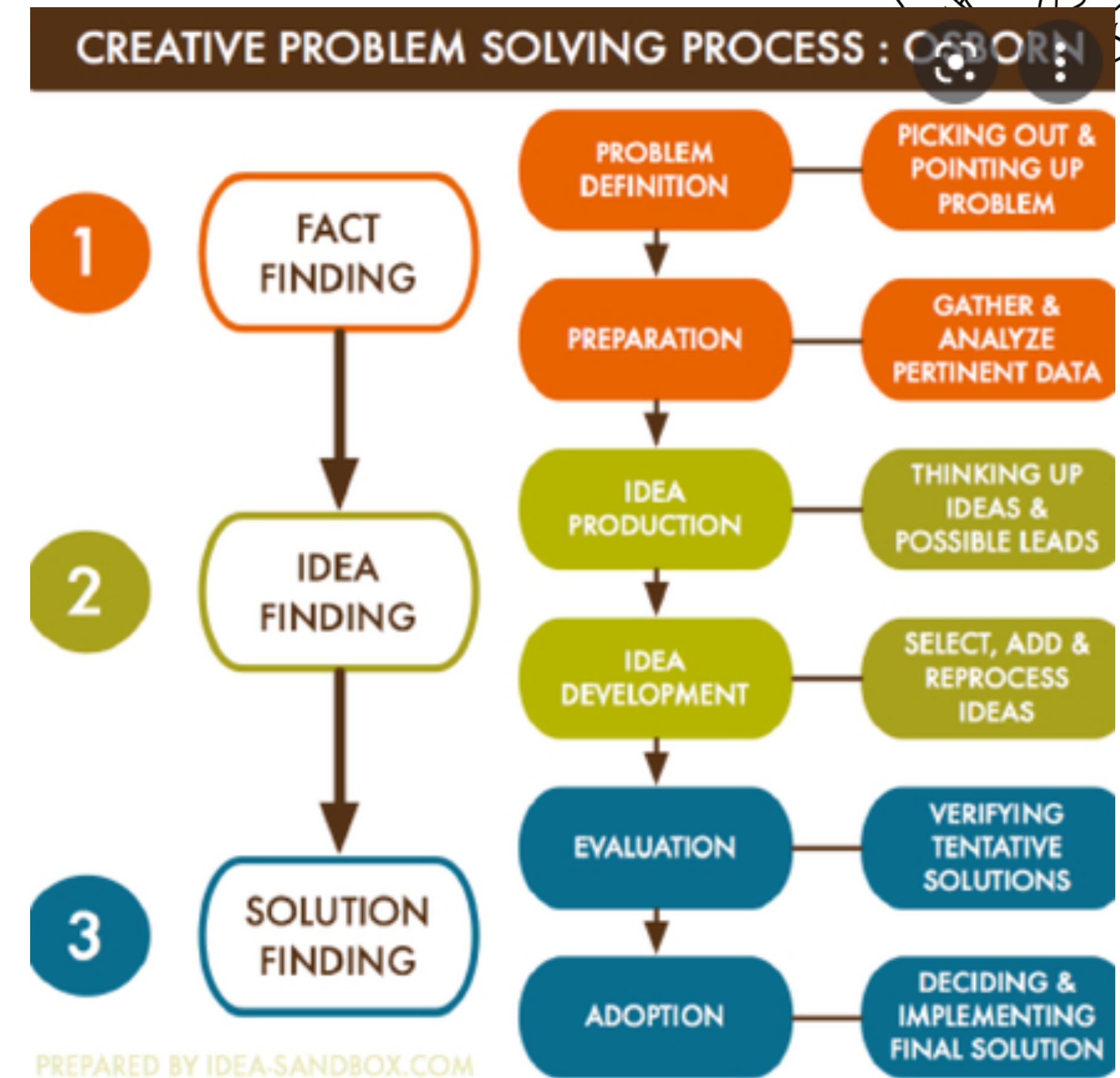
[Source: <https://news.agropages.com/News/NewsDetail---38480.htm>]

Your area of interest?

- for group work evaluation**

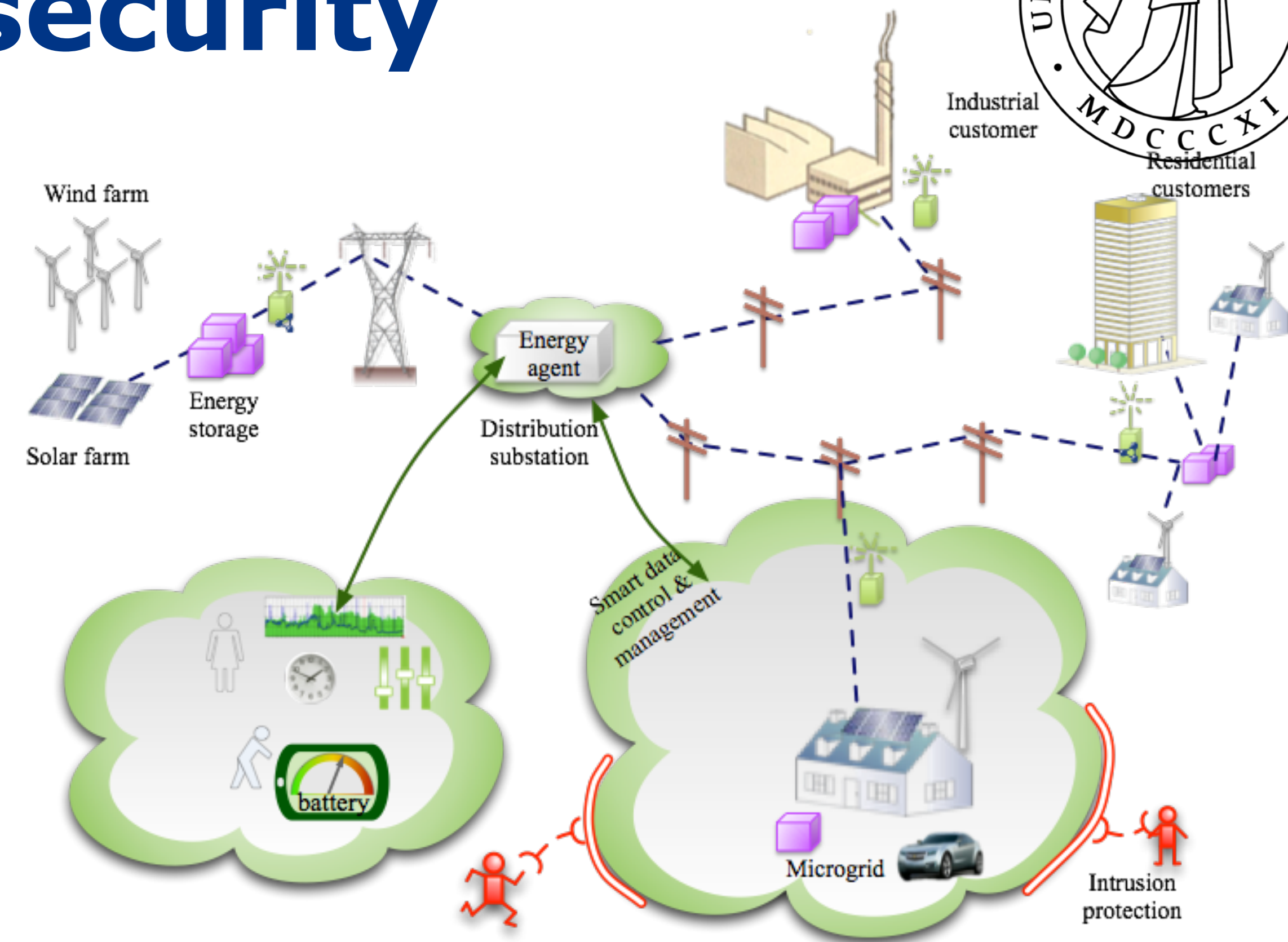
Path to solve problems

- Industrial approach (challenge, knowledge, opportunities, evaluation, solution)



L1 - L3: Introduction to security

- ➔ This first part will provide the introduction into the Internet of Things (Lecture 1 - L2), with industrial examples
 - Smart Grid and automatic metering system (AMS)
 - Smart Homes with sensors
 - Wireless System upgrade of cars
- ➔ Lecture 3 will further address potential security threats, through the example of the smart electricity grid.



- Smart grid with prosumers
- Various control mechanisms
- Attack scenarios
- Critical infrastructure

Internet of Things Security

Energy sector tops list of US industries under cyber attack, says Homeland Security report

12 March, 2015 at 6:38 PM Posted by: Jeremy Cowan

Washington, DC. March 12, 2015 — A report issued today by the US Department for Homeland Security says that in 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents reported by asset owners and industry partners.

The energy sector, says *Jeremy Cowan*, led all others again in 2014 with 79 reported incidents, followed by manufacturing at 65 and worryingly healthcare at 15 reported incidents. ICS-CERT's continuing partnership with the Energy sector reportedly provides many opportunities to share collaborate on incident response efforts.



Power Grid Cyber Attacks Keep the Pentagon Up at Night

A detailed look at why computers running the U.S. electrical infrastructure are so vulnerable to digital threats

By Michael McElfresh and The Conversation | June 8, 2015

The following essay is reprinted with permission from [The Conversation](#), an online publication covering the latest research.

It's very hard to overstate how important the US power grid is to American society and its economy. Every critical infrastructure, from communications to water, is built on it and every important business function from banking to milking cows is completely dependent on it.



Scott Wylie/Flickr

Security and Privacy challenges

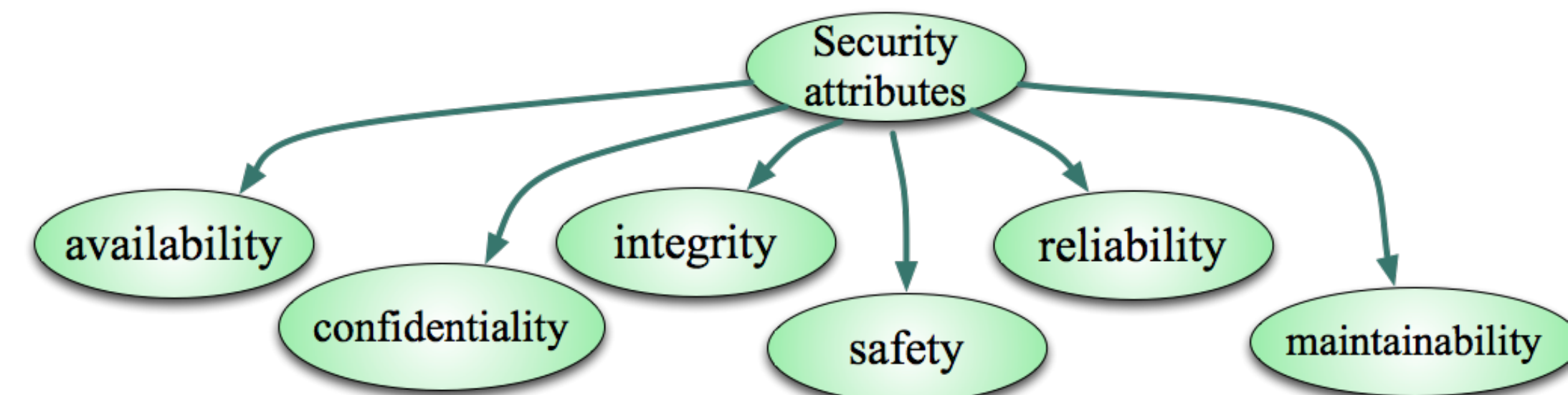
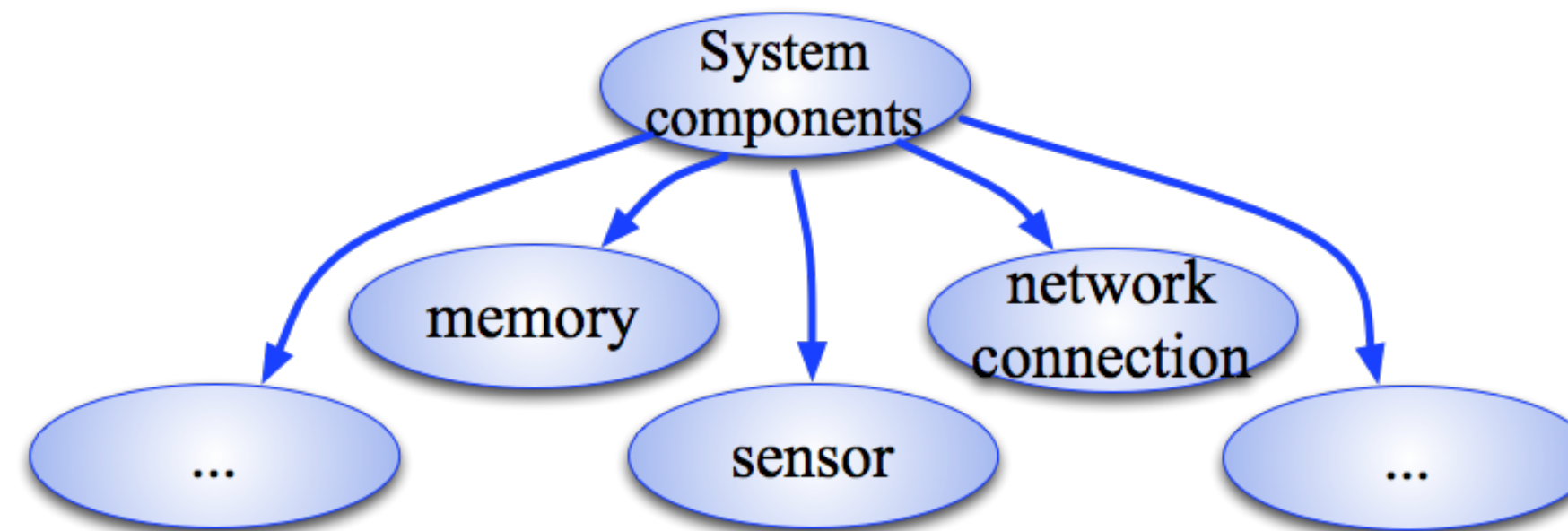
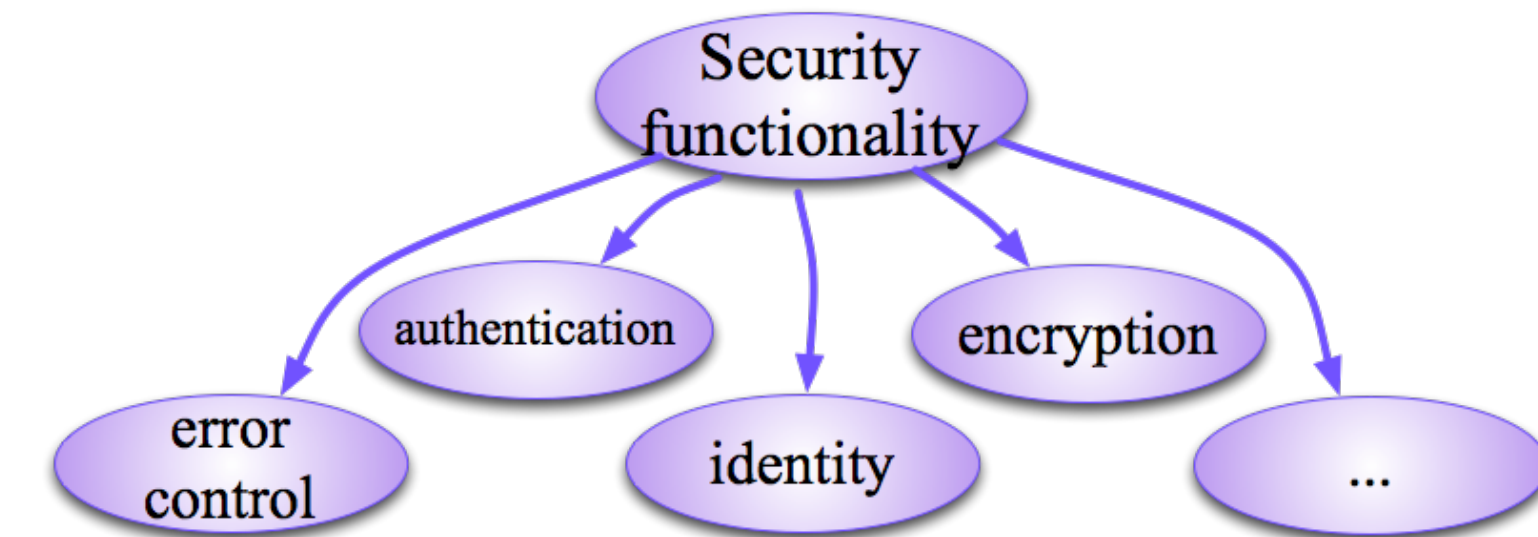
- Example: automatic meter reading (AMR) and -system (AMS) - Insurance
- Mapping from functional requirements towards mapping into technology.
- Example: translation of privacy requirements - can somebody see from my meter reading if I'm at home
- Legislation questions – GDPR and others



[source: seminaronly.com]

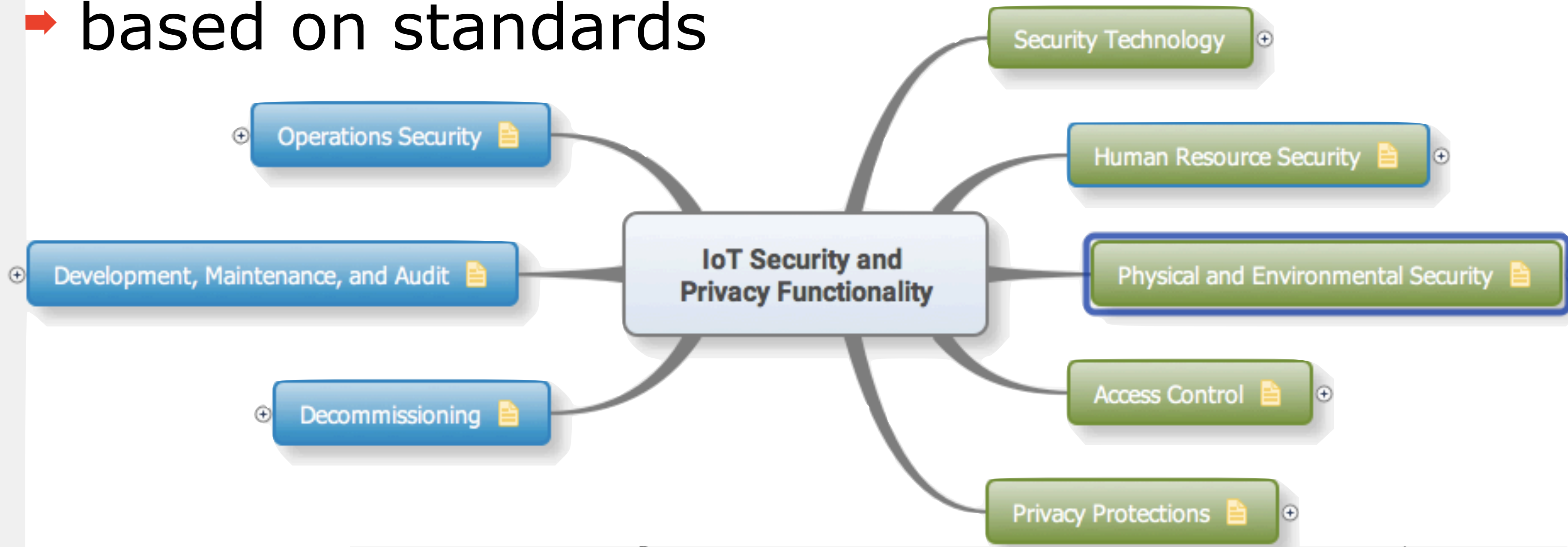
Machine-readable descriptions

- Describe a system based on security attributes
- Introduction to the Semantic Web
 - Ontologies
- Rules & Reasoning
 - make decisions



Security and Privacy Functionality

→ based on standards



References:

https://www.owasp.org/index.php/loT_Security_Guidance

Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

Addressing Measurable Security

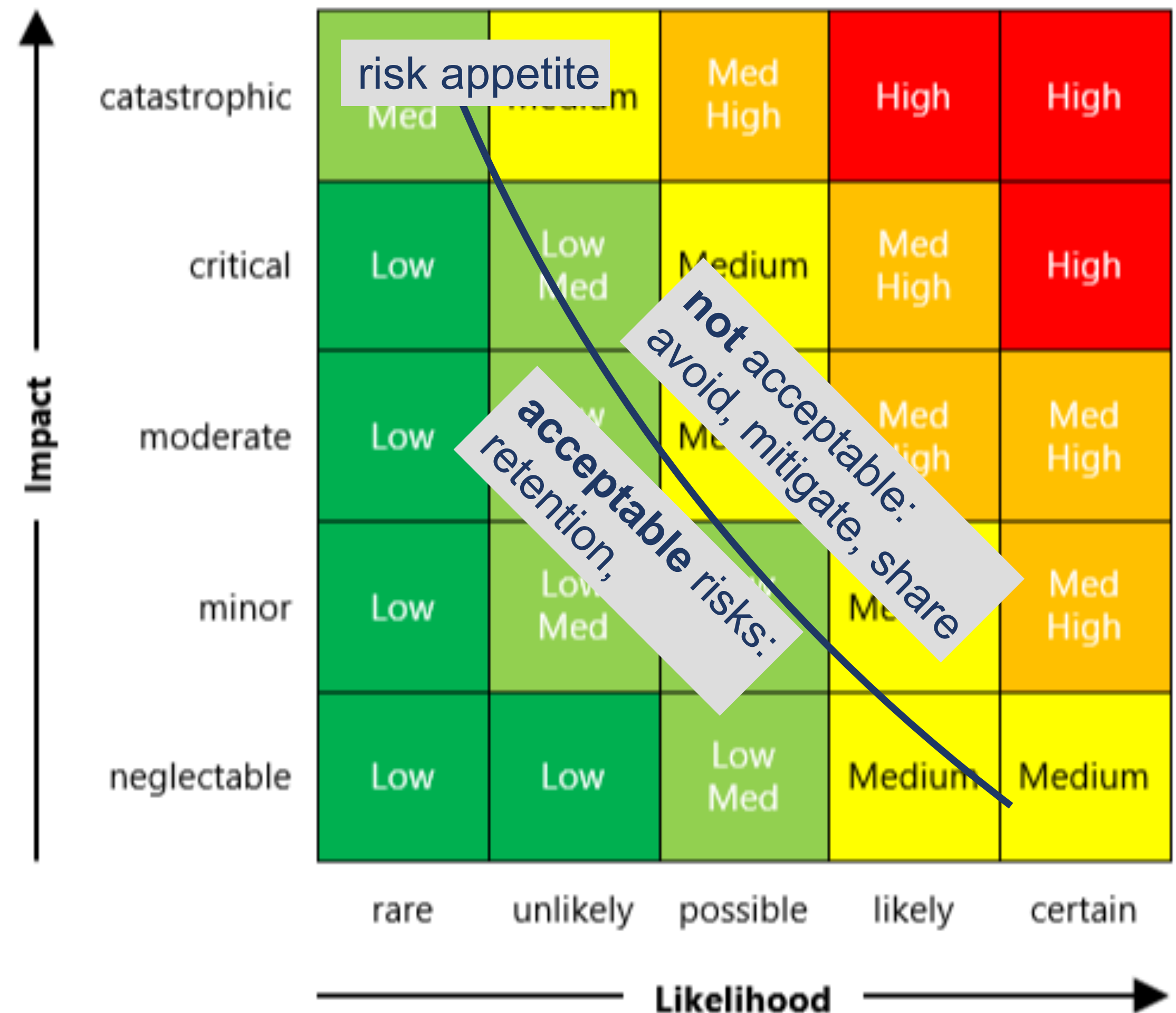
A) Risk analysis for IoT

B) Multi-Matrix analysis

C) Evaluate other IoT Risk Assessment tools

“Measure the Risk” through a Matrix

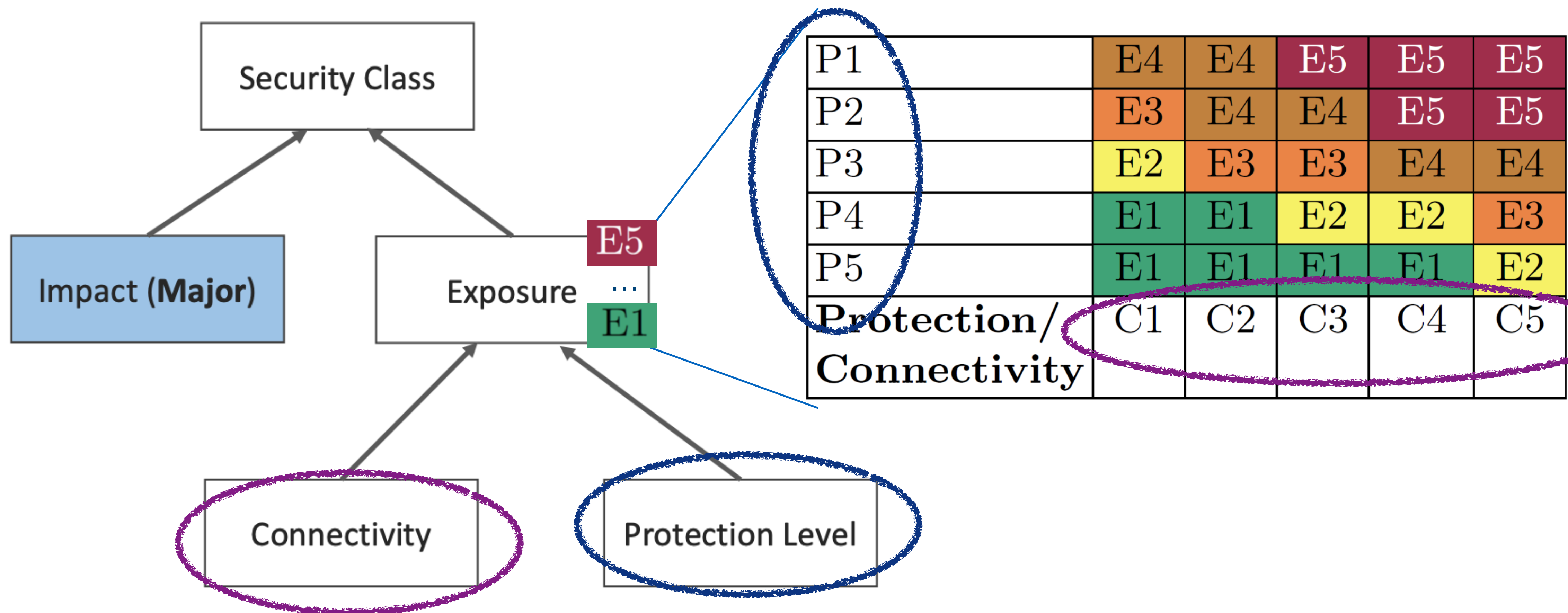
- Traditional approach
 - Likelihood/frequency, e.g. 1/s, 1/c
 - Impact/consequence, e.g. 100 M€
- Risk appetite
 - depends on company
- Challenges
 - not a linear risk behaviour: 1 x 5



[Source: https://b-advisory.ch/risk_matrices.html]

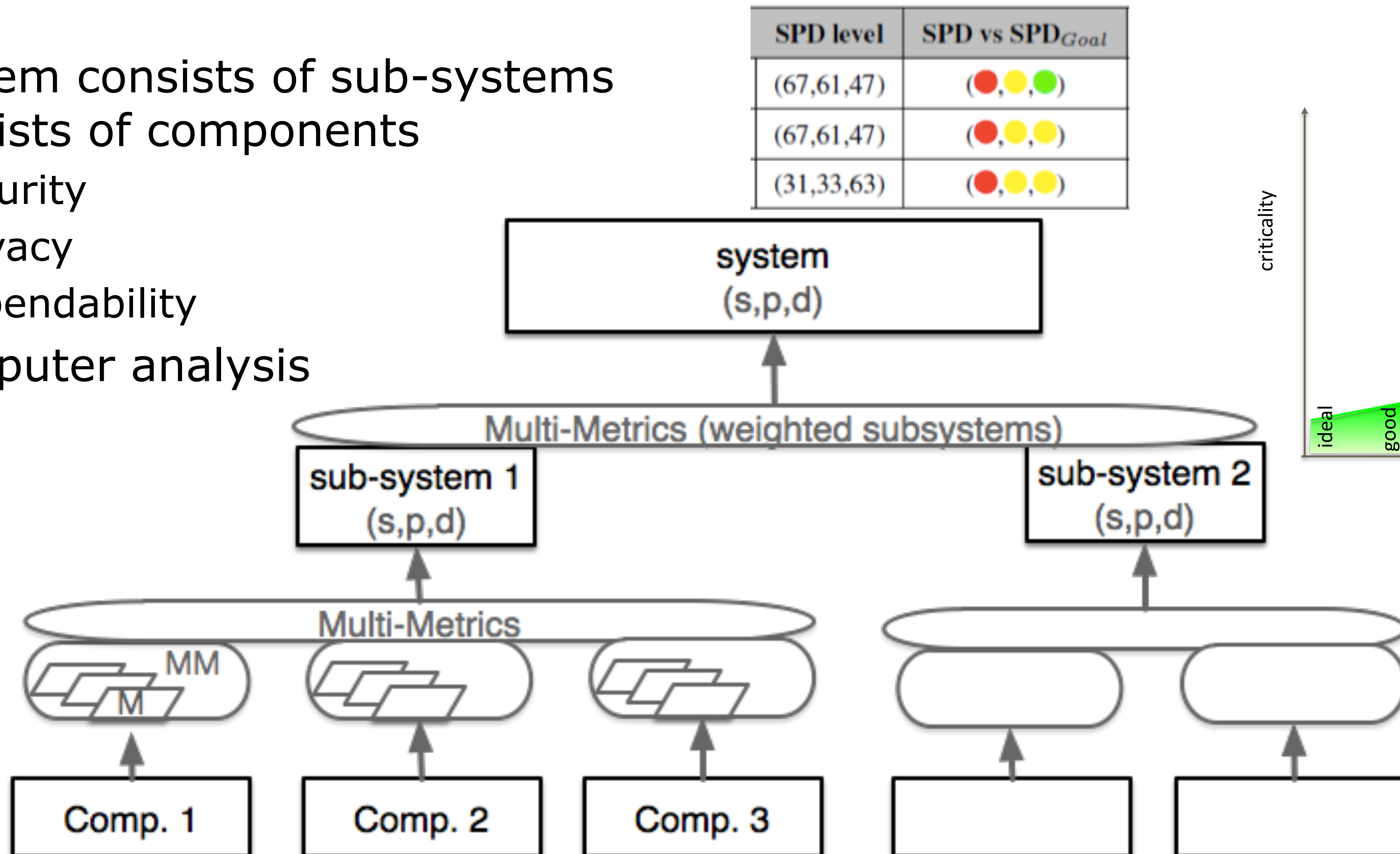
A) Security Class assessment for IoT

→ based on PhD Thesis from Manish Shrestha



B) Multi-Metrics method

- System consists of sub-systems consists of components
 - security
 - privacy
 - dependability
- Computer analysis



C) Industrial Tools analysis

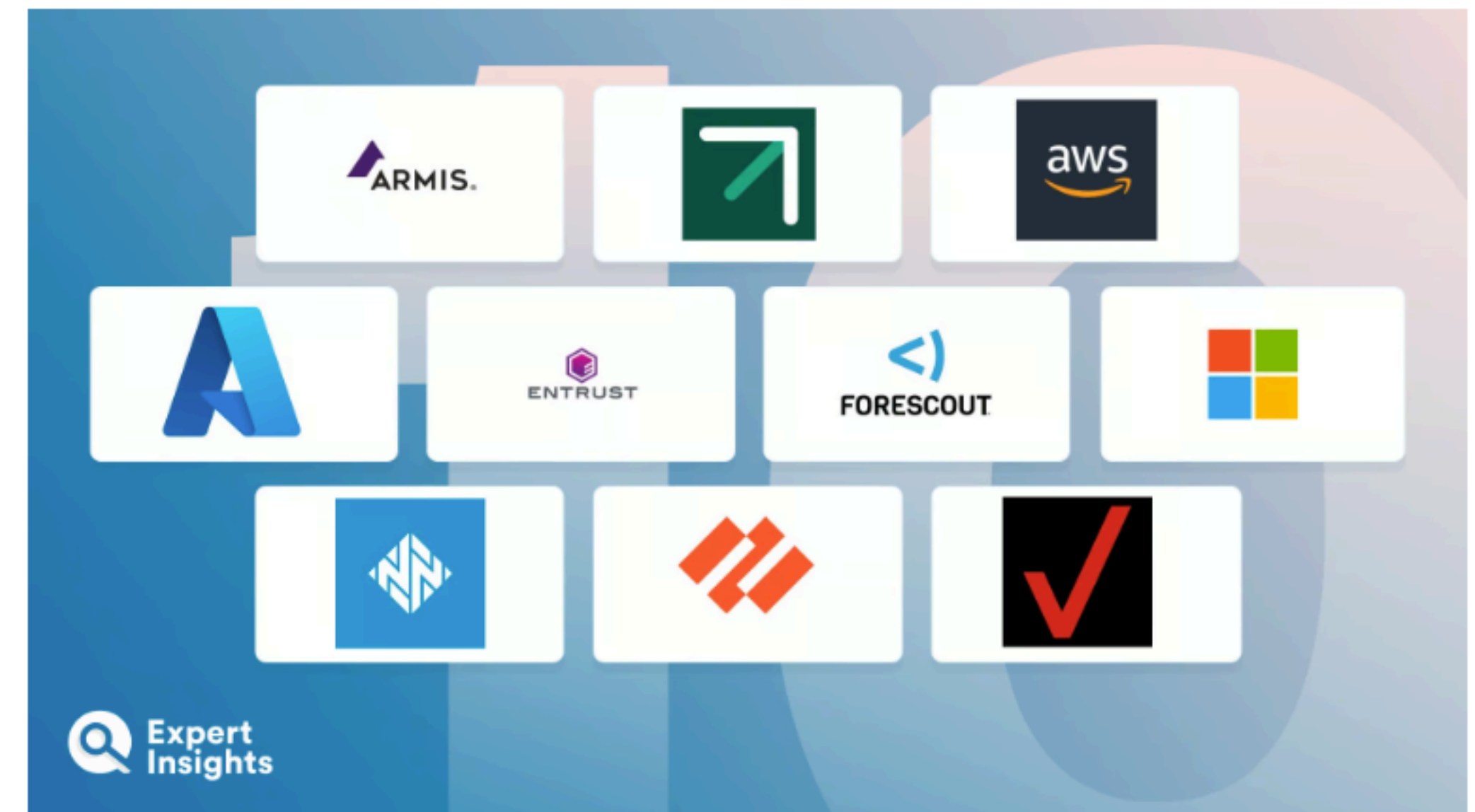
- Evaluate industrial tools
 - assume you are security specialist in an IoT-using industrial company
 - what are your criteria to select a tool
 - perform the evaluation
- <https://expertinsights.com/insights/the-top-10-iot-security-tools/>

The Top 10 IoT Security Tools

Our shortlist of the top IoT tools. Compare features such as device identification, vulnerability scanning, over-the-air patching, behavior monitoring, and encryption.



By Caitlin Jones
Updated Aug 14, 2023



Internet of Things (IoT) and operational technology (OT) devices improve productivity and streamline business operations. IoT devices (such as printers, security cameras, smart

Addressing literature

Paper presentation

→ Methodology:

- Learn AI-based paper search (elicit.org)
- Select (or search) for scientific papers
- Present the paper
- Discuss issues which you find interesting

→ Outcome

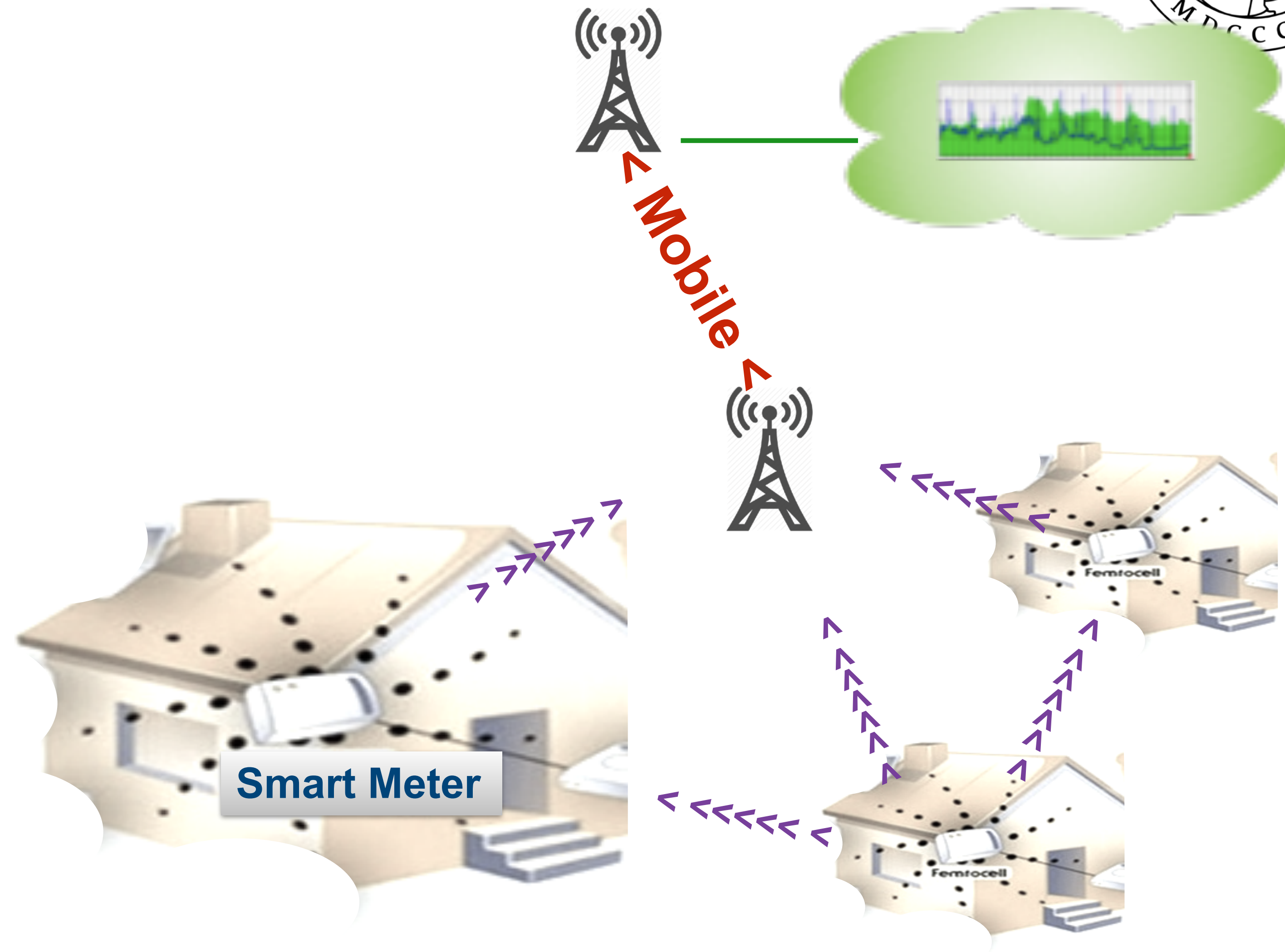
- Personal:
 - Learn to read and present scientific literature with own thoughts
 - Be able to hold a presentation with time limits and active audience
- Course
 - Get a fresh overview of the newest available research challenges and selected surveys of the field of the course
 - Learn from how others are making their presentations
 - Learn to ask questions

Elicit

	Paper title	Abstract summary
Add information about all papers ← Abstract summary ✓ Intervention ✓ Outcomes measured Number of participants Search for paper information What was the...	★ An efficient method for security measurement in internet of things 👤 S. Narang, Tarun Nalwa, T. Choudhury, Nirbhay Kashy... 📅 2018 International Conference on Communication, Comp... 2018 16 Citations DOI	The Internet of Things is exploding in size and complexity.
	★ Hardware Security in IoT era: the Role of Measurements and Instrumentation 👤 IOAN TUDOSA, F. Picariello, E. Balestrieri, L. D. Vito, F.... 📅 2019 II Workshop on Metrology for Industry 4.0 and IoT (...)	Secured IoT applies equally to IoT device-to-device communication, IoT sensing/actuating, and IoT information exchange.

Real World Examples

- ➔ Real world examples
 - taken from industry, e.g. Smart Meter
 - billing,
 - Controlling
- ➔ Service implications on requirements
- ➔ Technology mapping
- ➔ Intrusion detection
- ➔ Communication in automation networks



[source: seminaronly.com]

TEK5530 exam

- The final grade is based on
 - oral exam (100%).

- Group work
 - Keeping the time limits
 - Clear presentation of the topic
 - Own evaluation of the work

- Oral exam
 - Presentation of Group work (8 min)
 - Questions to group work (7 min)
 - Topics of the course (8 min)