

UNIVERSITY OF OSLO

**6th International Workshop on Decentralized
Technologies and Applications for IoT (D'IoT) 2025,
part of
IEEE Vehicular Technology Conference (VTC) 2025, taking
place from June 17–20 in Oslo, Norway**

Fog and Edge AI, increasing resilience and reliability of the electrical grid

Josef Noll

Professor, University of Oslo,
Department of Technology Systems

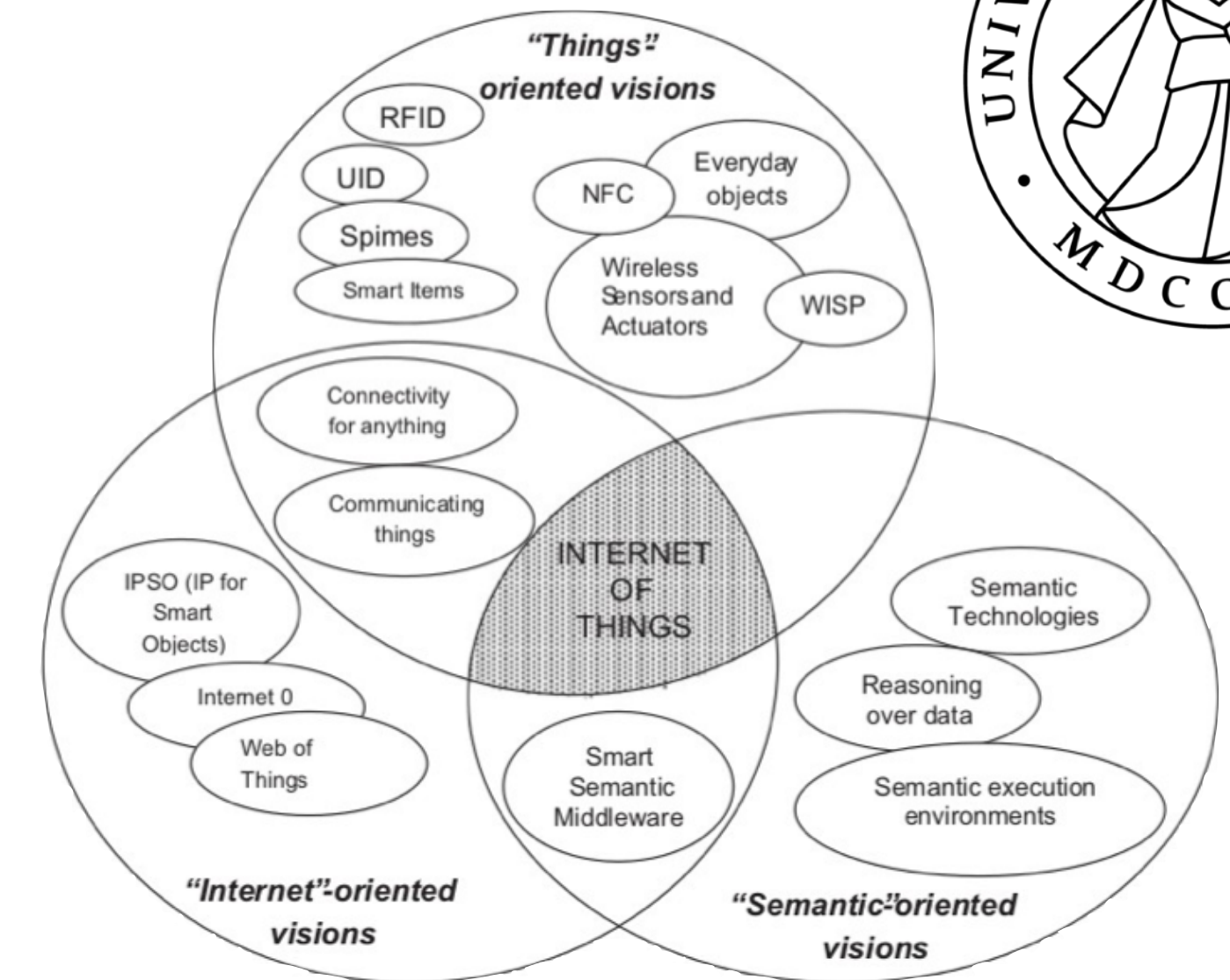
Kjeller, Norway, m: +47 9083 8066, e: josef@jnoll.net



Will AI be able to
describe?

Outline

- ➔ History
 - fog, edge computing
 - edge IoT
- ➔ Power Grid
 - failure & hacks
 - Grid as critical infrastructure
- ➔ Risk analysis - exposure
- ➔ Distributed AI (DAI)
 - research challenges



Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

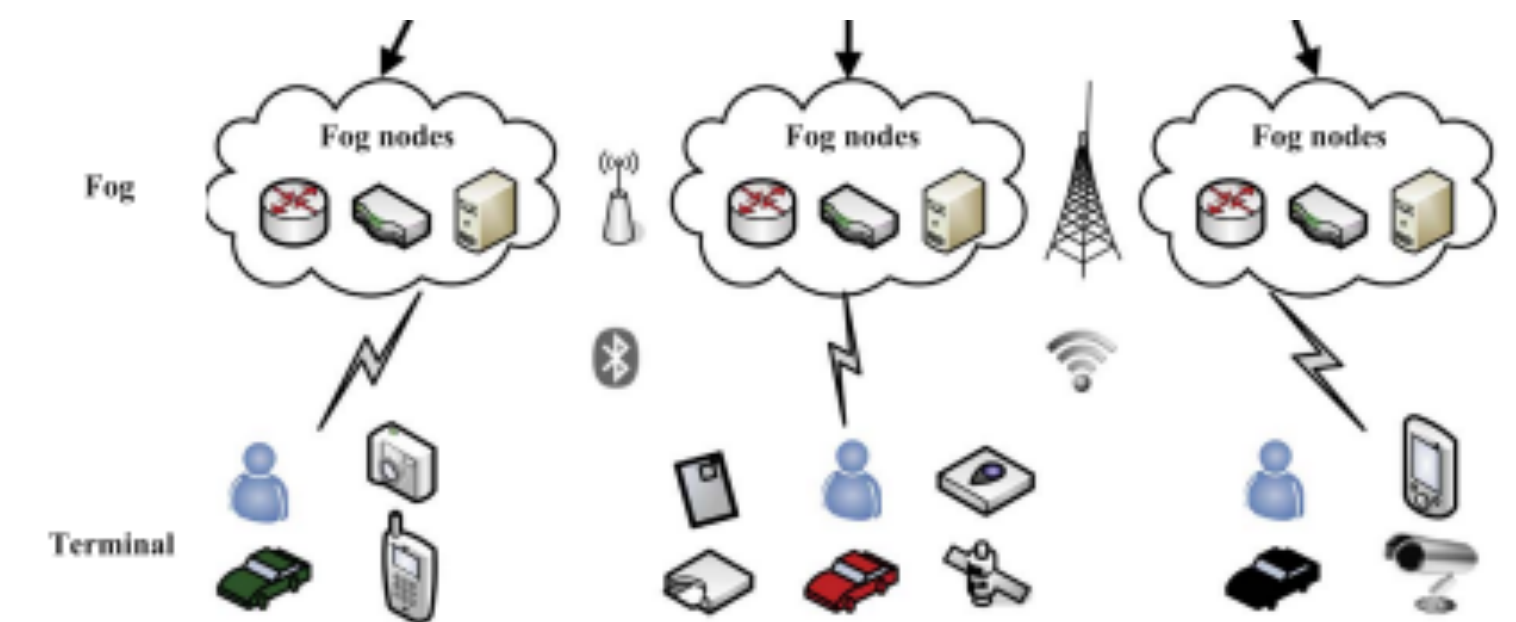
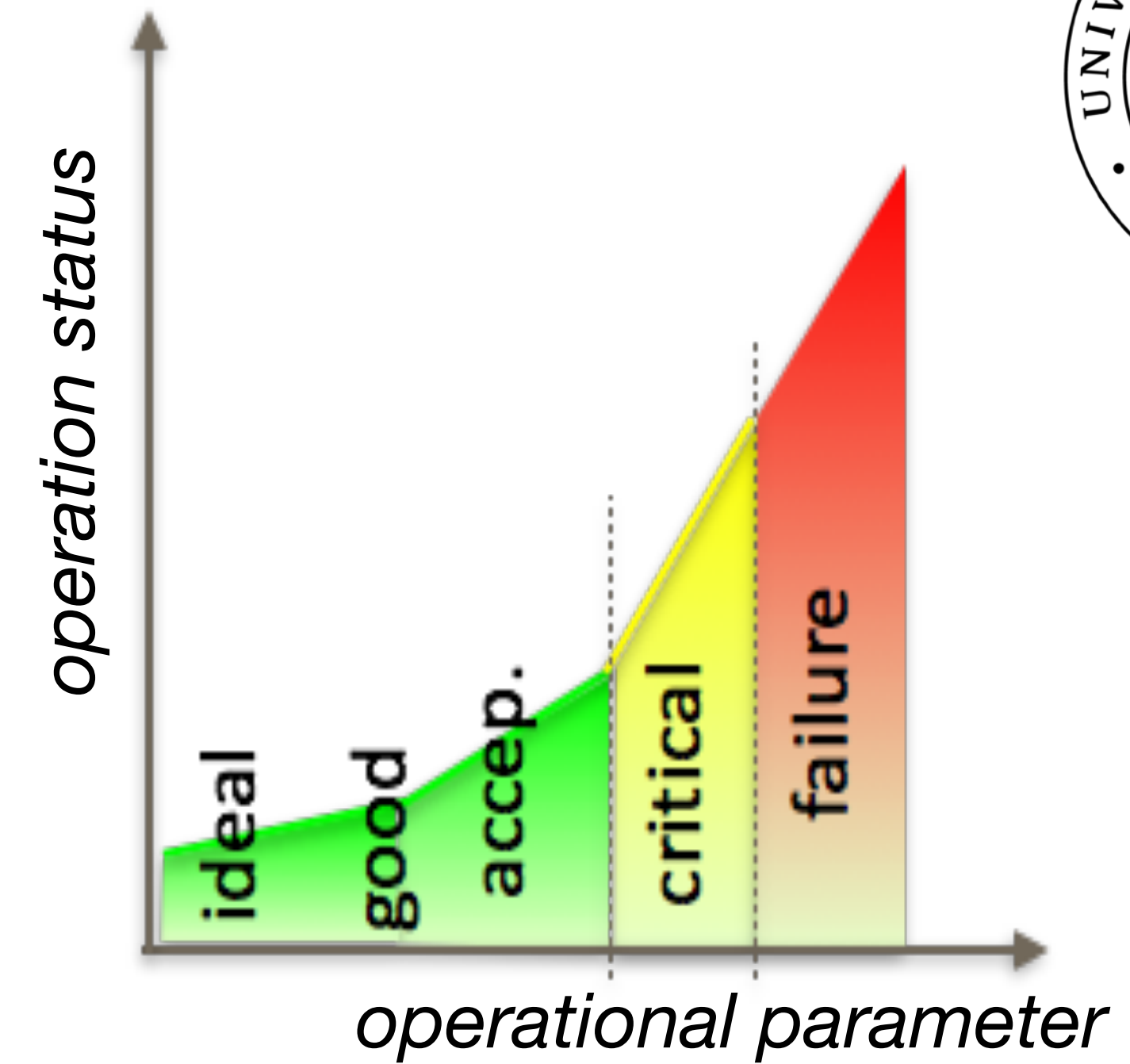


Fig. 1. The hierarchical architecture of fog computing.

Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.*, 98, 27-42.

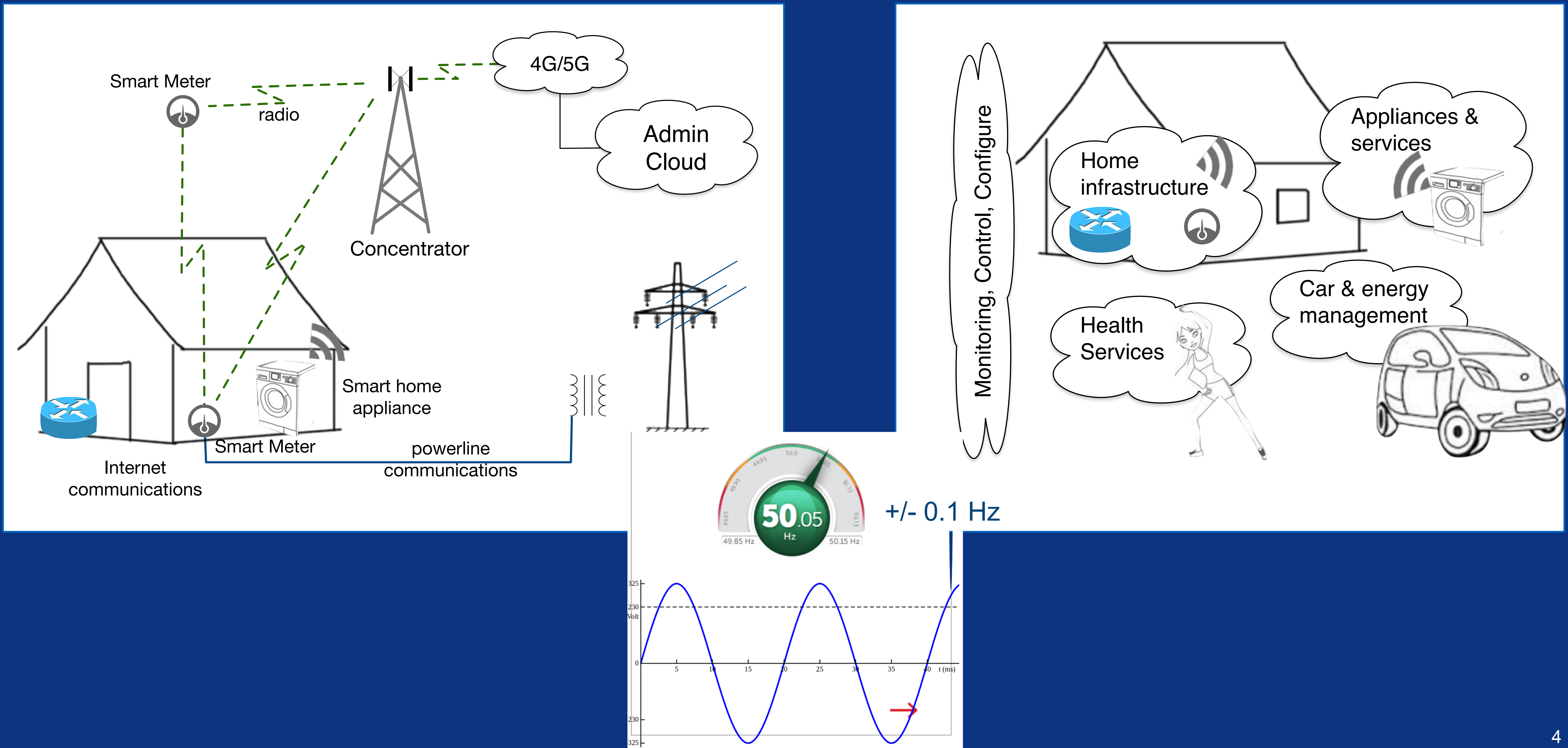
Fog-/Edge-IoT

- Bandwidth & costs
 - 30 GB of data from a truck per month
- Latency
 - local decision within 5 ms
- Security, Privacy
 - Man-in-the-middle, DDoS
 - Authentication, Access control
 - Fault tolerance, Reliability
- Resource management
- Transfer to Fog-/Edge-AI?



A sensor can't run artificial intelligence (AI)

The electrical grid



28Apr2025 Spain & Portugal blackout

- Cause:
 - 60% solar energy,
 - 1. solar park switched off, 1.5 s later 2. solar park
 - interconnection to France stopped ($f < 48,0$ Hz)
- Conventional: inertia (rotating generators)
- Solar: sudden death (DC/AC converters)
- Challenge:
 - distributed respond to grid fluctuations

 Baker Institute

12:20 Oscillations across Europe

12:40 Nuclear outage FR

12:32:57 generation trips (20 s)

total 2200 MW deducted

12:33:18 freq 48,0 Hz

12:33:21 AC to France stopped

12:33:24 blackout (incl HVDC)

2025: ES, PT

2025: CL Chile

2023: PK

2022: BD

2021: PK

2020: LK Sri Lanka

...



Center for Energy Studies | Commentary

The Iberian Peninsula Blackout – Causes, Consequences, and Challenges Ahead

May 2, 2025 | Raúl Bajo Buenestado

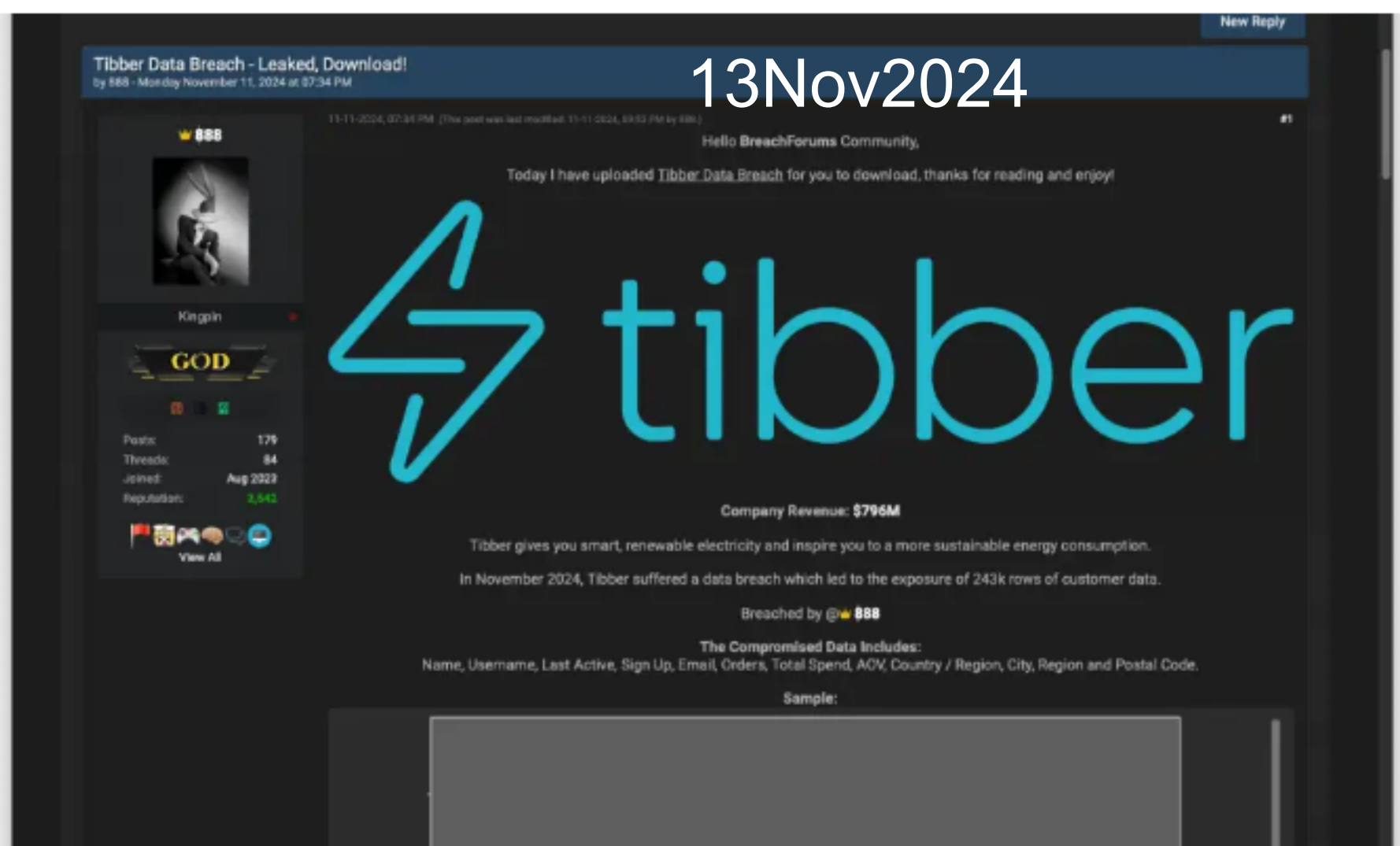
<https://www.entsoe.eu/news/2025/05/09/entso-e-expert-panel-initiates-the-investigation-into-the-causes-of-iberian-blackout/>

<https://www.bakerinstitute.org/research/iberian-peninsula-blackout-causes-consequences-and-challenges-ahead>

https://en.wikipedia.org/wiki/List_of_major_power_outages

Threat landscape

- Supply chain attacks
- Ukraine grid hack (2015)



(Image: heise online)

Nov 13, 2024 at 4:35 pm CET 2 min. read | Security

By Dr. Christopher Kunz

Hackers have attacked electricity provider Tibber and stolen data. The company confirmed this to heise security. Over 50,000 customers are apparently affected, all of them from Germany. The attackers are offering their prey for sale on the Darknet.



July 2023 - June 2024

1. Ransomware 25.8%
2. Malware 5.2%
3. Social Engineering 6.1%
4. GDPR threat 19%
5. DDoS 41.1%
6. Information manipulation ~1%
7. Supply chain attacks ~1%

Examples Supply Chain

- Discord (Mar2024)
- Okta (Oct2023 - authentication)
- JetBrains (Sep2023 - TeamCity)
- MOVEit (Jun2023 - transfer tools)
- Microsoft (Feb2023 - code sign)

<https://www.heise.de/en/news/Electricity-provider-Tibber-hacked-50-000-German-customers-affected-10031690.html>

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

Power Grid 2024

US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney

April 4, 2024 11:48 PM GMT+2 · Updated 9 months ago



A local resident walks by the power grid towers at Bair Island State Marine Park in Redwood City, California, United States, January 26, 2022. REUTERS/Carlos Barria/File Photo [Purchase Licensing Rights](#)

[Home](#) / [2024](#) / [May](#) / Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world

Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world

May 17, 2024

By Emily Cerf

SHARE THIS STORY: [Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#)

On a cold winter night in 2016, Ukrainians experienced the first-ever known blackout caused by malicious code (malware) designed to autonomously attack the power grid. One-fifth of Kyiv's citizens were plunged into darkness as attackers used malware to target the capital city's power grid. Six years later, in the early months of the ongoing Russia-Ukraine war, a second attack attempted to combine kinetic and cyber attacks to take down Ukraine's power grid.

Malware attacks against physical infrastructure have long been a looming threat in the realm of cybersecurity, but these two in Ukraine were the first attacks of their kind, and have received little attention from the academic community. Carried out by a Russian intelligence agency against Ukraine, they warn of the evolution of cyber attacks to the built world, and highlight the need to better understand and defend against this type of malware.



Power lines in Ukraine. Photo credit: Mny-Jhee, iStock.

<https://news.ucsc.edu/2024/05/ukraine-cybersecurity.html>

<https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/>

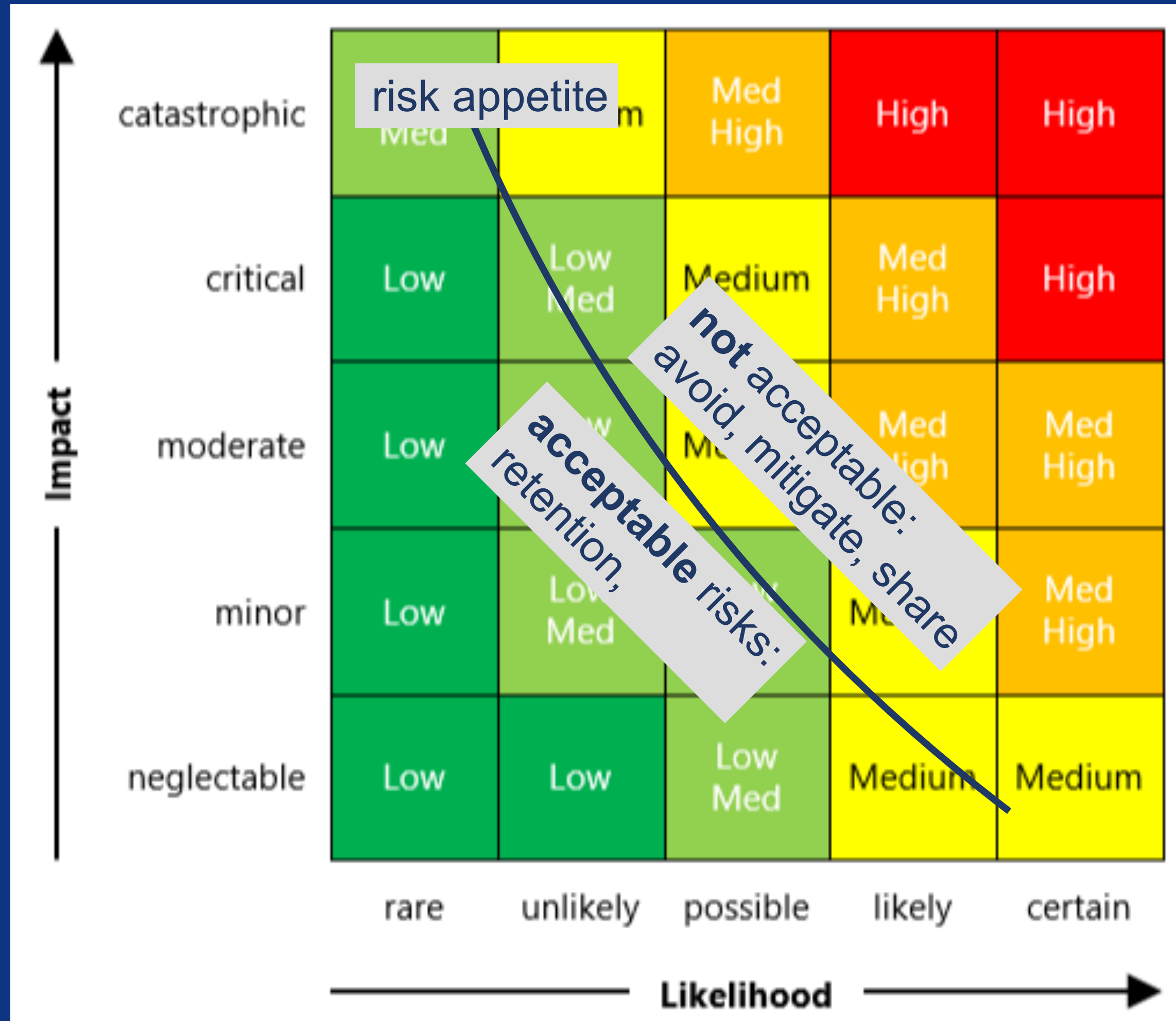
Resilient Societies

- Resilience to threats
 - Pandemics: COVID-19,
 - natural disaster
 - external threats: terrorism, fake news,
- Self-sustained communities
 - job-creation
 - educating, information,
 - Dugnad: value creation
- Value-based
 - “alle er med” (everyone is included)
 - Trust
- “Digital Participation in the society”



Markus Brunnermeier, Princeton University

Risk Analysis for IoT

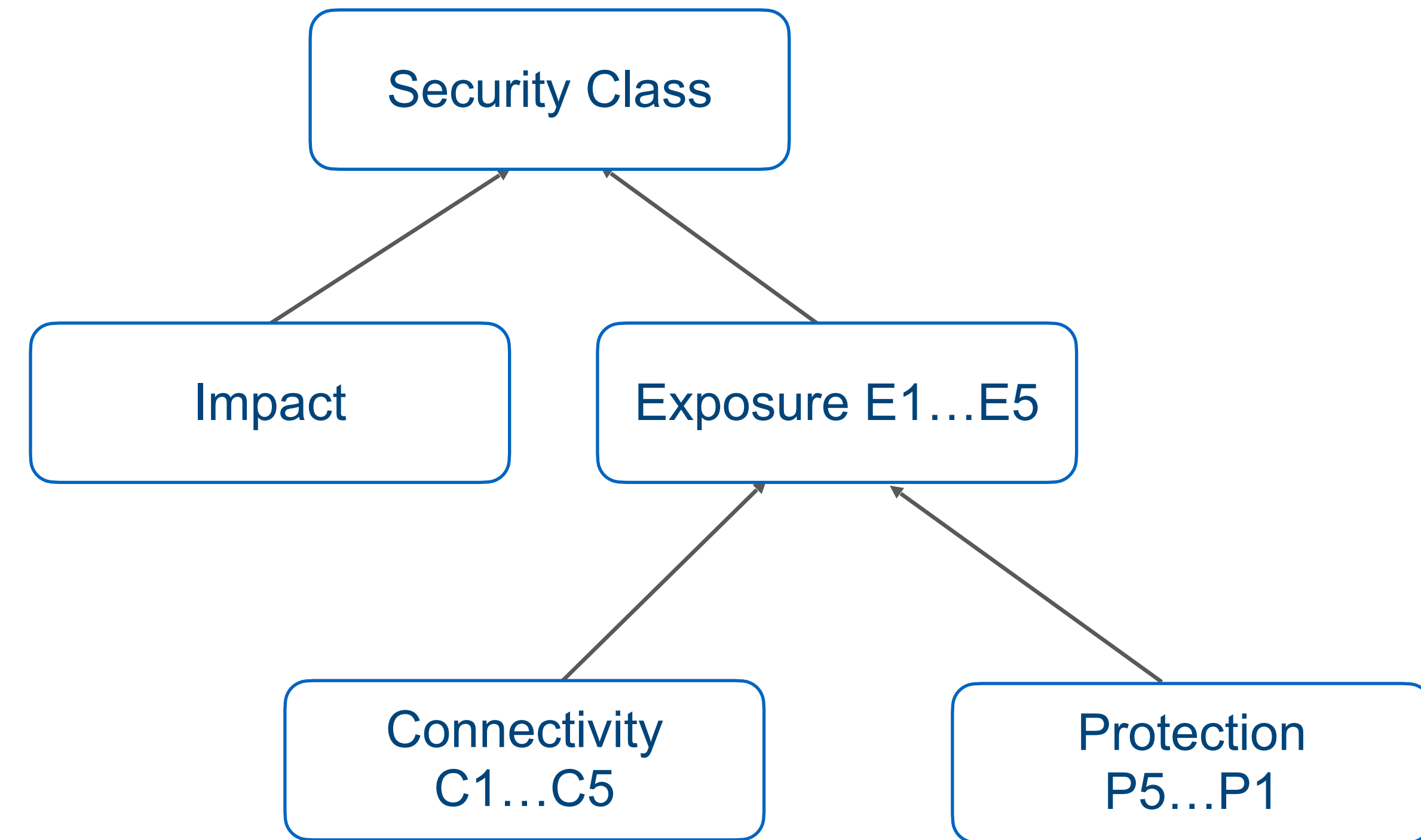


Applicable to IoT?



Risk Exposure Model for IoT

- “you have been hacked”
- Exposure
 - Connectivity
 - Protection Level



Lowest Protection

P1	E4	E4	E5	E5	E5
P2	E3	E4	E4	E5	E5
P3	E2	E3	E3	E4	E4
P4	E1	E1	E2	E2	E3
P5	E1	E1	E1	E1	E2
Protection/ Connectivity	C1	C2	C3	C4	C5

Highest Protection

Isolated Wireless connectivity Internet

Manish Shrestha https://its-wiki.no/wiki/Smart_ICT_2019



Industrial standards (IEC 62443)

- ➔ Security Level (SL) 0: No protection required
- ➔ SL1: Protection **unintentional** or accidental misuse.
- ➔ SL2: Protection **intentional misuse** by simple means with few resources, general skills and low motivation.
- ➔ SL3: Protection against intentional misuse by **sophisticated means** with **moderate resources**, automation-specific knowledge and moderate motivation.
- ➔ SL4: Protection against intentional misuse using sophisticated means with **extensive resources**, automation-specific knowledge and high motivation.
- ➔ Set of standards, e.g. IEC 62443-1-6: Applying the 62443 series to the industrial internet of things
- ➔ Certification authorities: TÜV, Bureau Veritas, ...

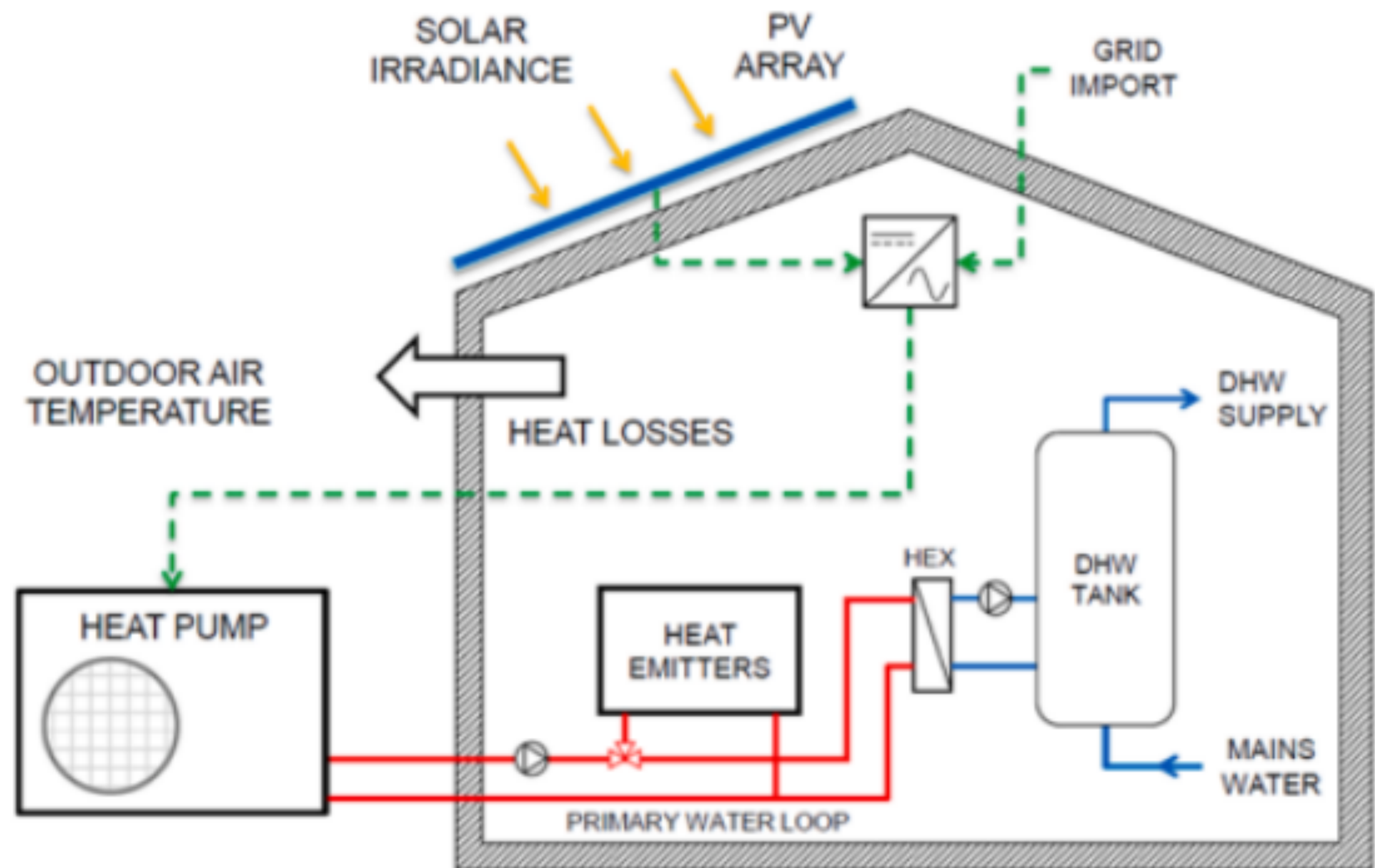
➔ https://en.wikipedia.org/wiki/IEC_62443

Standard	Title
IEC 62443-1-1	Concepts and models
IEC 62443-1-5	Scheme for IEC 62443 security profiles
IEC 62443-2-1	Security program requirements for IACS asset owners
IEC 62443-2-3	Patch management in the IACS environment
IEC 62443-2-4	Requirements for IACS service providers
IEC 62443-3-1	Security technologies for industrial automation and control systems
IEC 62443-3-2	Security risk assessment and system design
IEC 62443-3-3	System security requirements and security levels
IEC 62443-4-1	Secure product development lifecycle requirements

... and more

Security classes for energy control

- Centralised (provider) or
- Decentralised (edge)



Centralised control: Exposure calculation

- Assessment:
Exposure E3
 - full Internet access (C5)
 - high protection (P4)

P1	E4	E4	E5	E5	E5
P2	E3	E4	E4	E5	E5
P3	E2	E3	E3	E4	E4
P4	E1	E1	E2	E2	E3
P5	E1	E1	E1	E1	E2
Protection/ Connectivity	C1	C2	C3	C4	C5

Exposure = E3

see additional slides for **protection requirements**

[Courtesy: Manish Shrestha, UiO, 2019]

Centralised: Security Class D

Class : D

Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

[Courtesy: Manish Shrestha, UiO, 2019]

Exposure

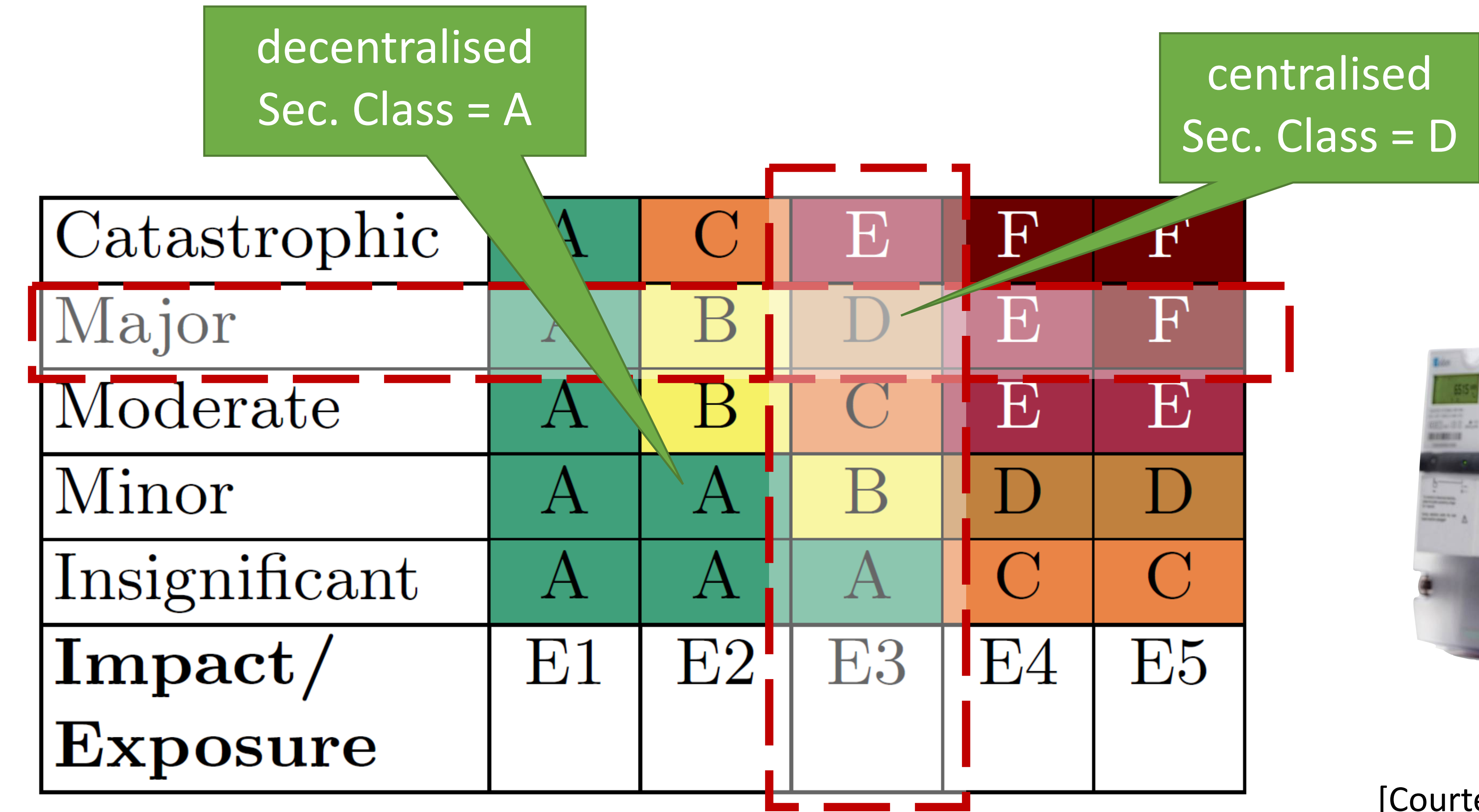


	Decentralised E2				Centralised E3	
P1	E4	E4	E5	E5	E5	
P2	E3	E4	E4	E5	E5	
P3	E2	E3	E3	E4	E4	
P4	E1	E1	E2	E2	E3	
P5	E1	E1	E1	E1	E2	
Protection/ Connectivity	C1	C2	C3	C4	C5	

[Courtesy: Manish Shrestha, UiO, 2019]

Exposure Risk Model

Increased Security through decentralisation



Smart Meter Regulations



[Courtesy: Manish Shrestha, UiO, 2019]

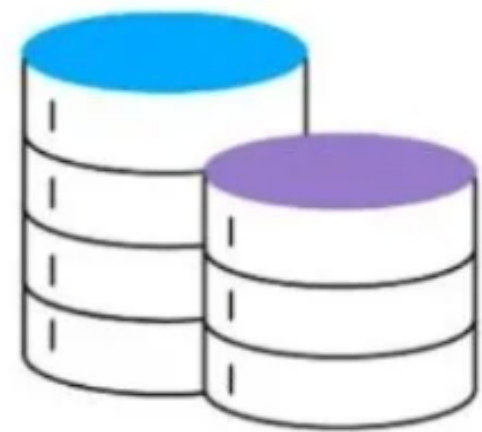
Artificial Intelligence (AI)

“Big is beautiful”?

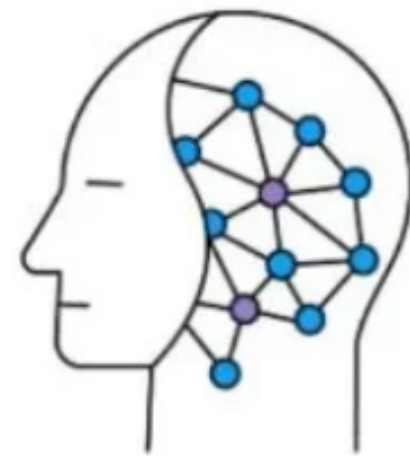
Will AI be able to
describe?



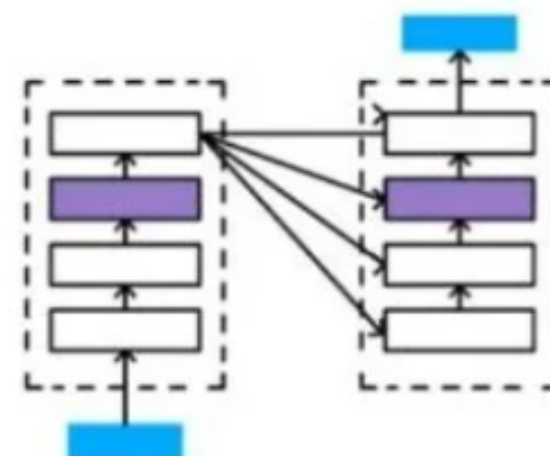
And now we want the computer to answer all questions of the world, in all languages



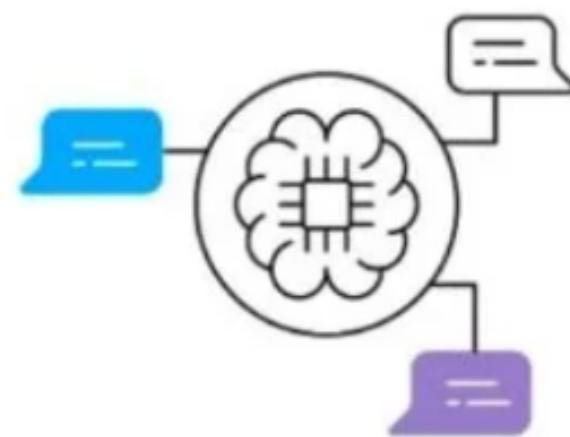
Massive Dataset



Deep Learning



Transformer Architecture

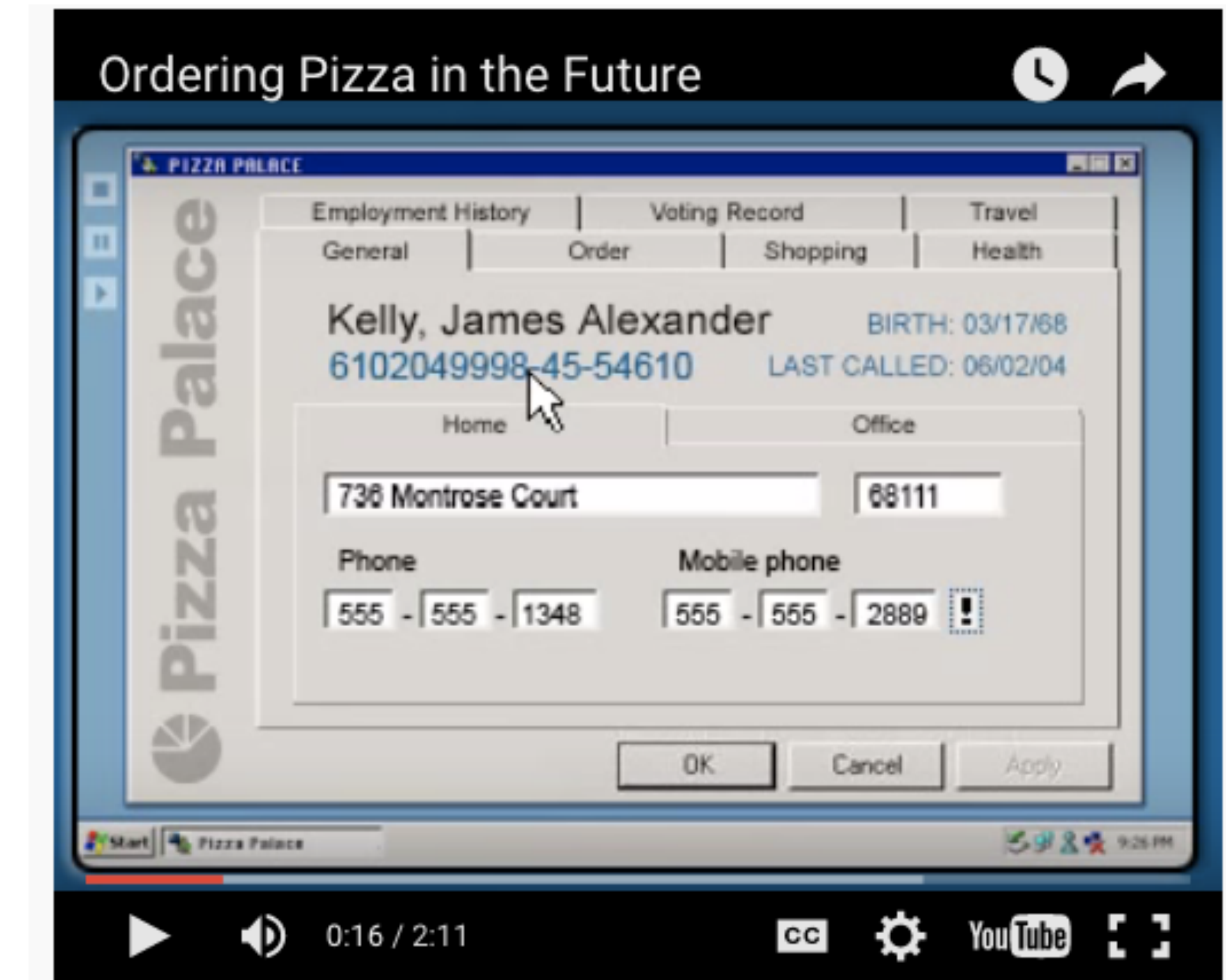


Self-supervised Learning



Fine-tuning

Large
Language
Models
(LLM)



12Jun2006

<https://www.youtube.com/watch?v=RNJI9EEcsoE>

Source: <https://em360tech.com/tech-articles/what-large-language-model-llm-definition-examples-use-cases>

Challenge Large Language Models



◆ AI Overview

To challenge a large language model (LLM), you can ask questions that probe its limitations in areas like reasoning, logic, context awareness, factual accuracy, ethical considerations, and creative interpretation, including:

Logic and Reasoning:

- "Explain why a square is not a circle, using only logical reasoning."
- "If all cats are mammals, and all mammals are animals, then are all cats animals? Why or why not?"
- "Solve this riddle: What has to be broken before you can use it?"

Context and Understanding:

- "Tell me a story about a robot who falls in love with a human, but is programmed to never express emotions. How does the robot grapple with this conflict?"
- "Explain the concept of 'schadenfreude' in a way that a child would understand."
- "Compare and contrast the perspectives of two opposing political viewpoints on a current issue."

[Source: Google "questions to challenge large language models", 19 Feb2025]

Factual Accuracy and Bias:

- "What is the most recent scientific discovery that challenges a previously held belief?"
- "Provide evidence to support the claim that climate change is primarily caused by human activity."
- "Explain why it's important to consider potential biases when interpreting historical events."

Creativity and Interpretation:

- "Write a poem about the feeling of nostalgia."
- "Compose a song that expresses the struggle of overcoming adversity."
- "Imagine a world where animals could talk, what would be a typical conversation between a dog and a cat?"

Ethical Considerations:

- "What are the potential dangers of using AI to make decisions that affect people's lives?"
- "How can we ensure that AI systems are developed and used in a way that is fair and equitable?"
- "Discuss the ethical implications of creating deepfakes that could be used to deceive people."

Why is big beautiful?

INNOVATION / AI

Stargate: America's \$500 Billion Bid To Corner Global AI Capital

By [Craig S. Smith](#), Contributor. Craig S. Smith, Eye on AI host...

[Follow Author](#)

Jan 23, 2025, 11:57am EST



Save Article



Comment



TOPSHOT - OpenAI CEO Sam Altman speaks during the Microsoft Build conference at the Seattle ... [+] AFP VIA GETTY IMAGES

Source: <https://www.forbes.com/sites/craigsmith/2025/01/23/stargate-americas-500-billion-bid-to-corner-global-ai-capital/>

→ feed with “everything” TV, video, wikipedia, NY times,...

→ all possible combinations

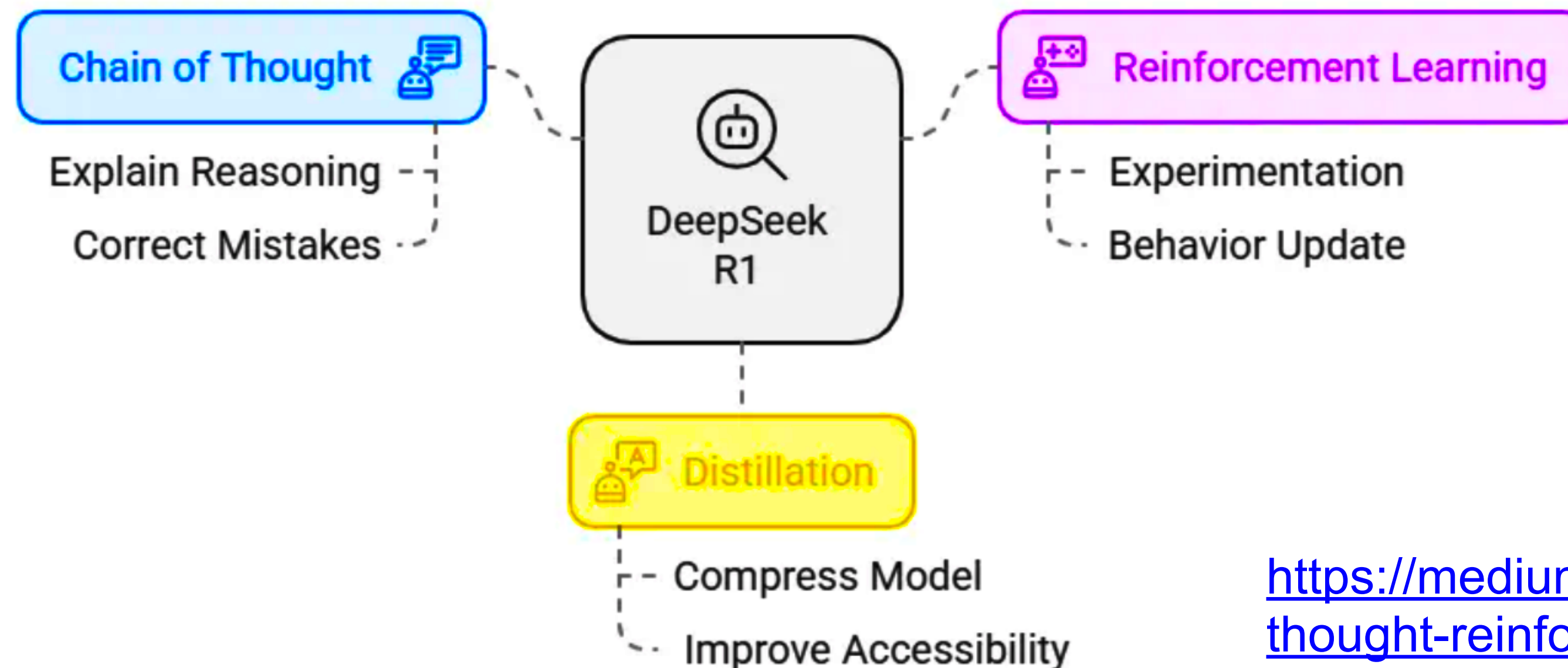


→ the n^2 problem

→ finding plausible answers

The Chinese Way

- ➔ 2022: 440 Universities in China educated AI
 - 50% of world's AI brains
- ➔ Mixture-of-Experts (MoE)



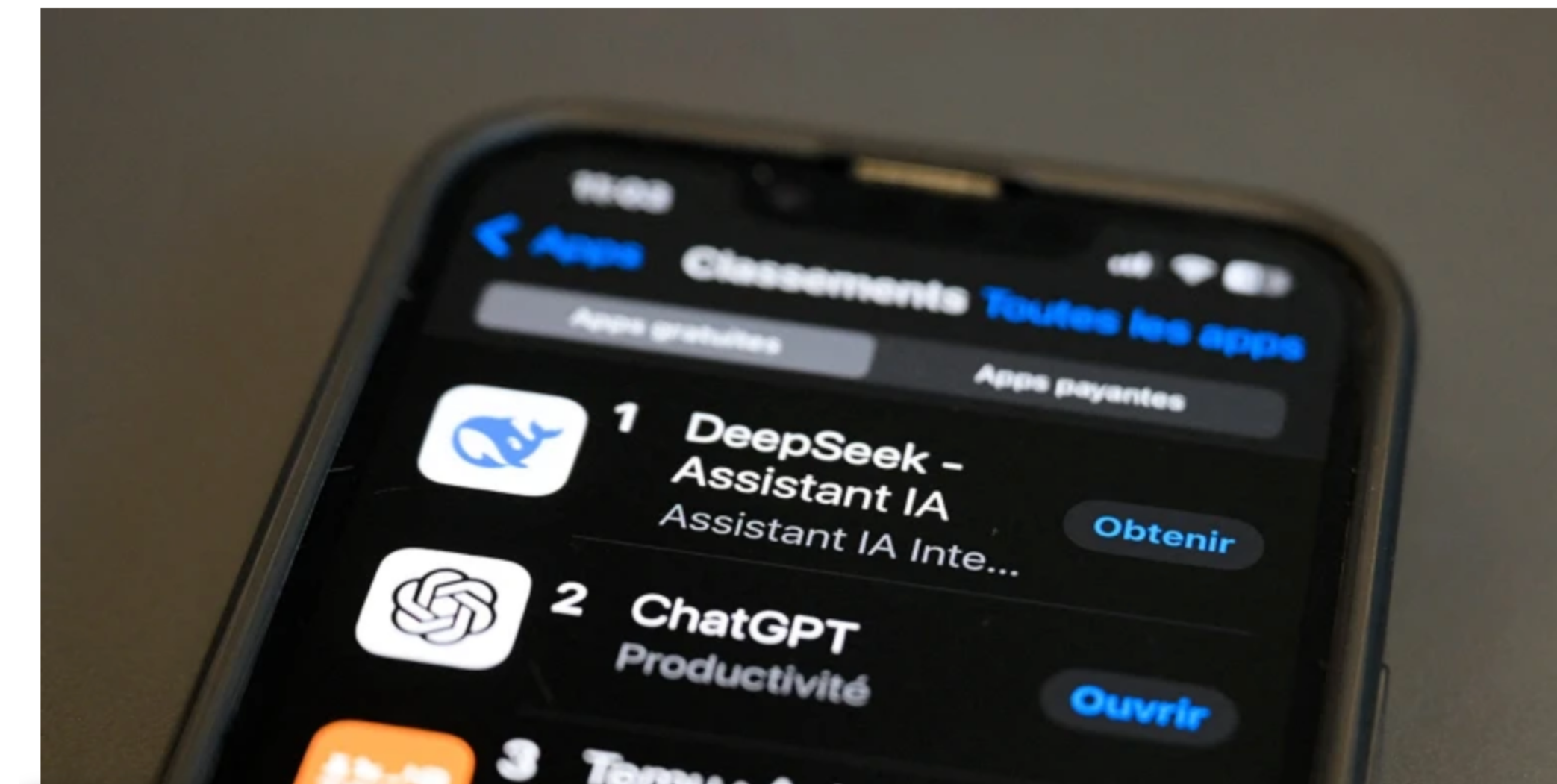
How China created AI model DeepSeek and shocked the world

Government policies, generous funding and a pipeline of AI graduates have helped Chinese firms create advanced LLMs.

By [Gemma Conroy](#) & [Smriti Mallapaty](#)



<https://www.nature.com/articles/d41586-025-00259-0>



<https://medium.com/@tahirbalarabe2/deepseek-r1-explained-chain-of-thought-reinforcement-learning-and-model-distillation-0eb165d928c9>

AI Opportunities for All

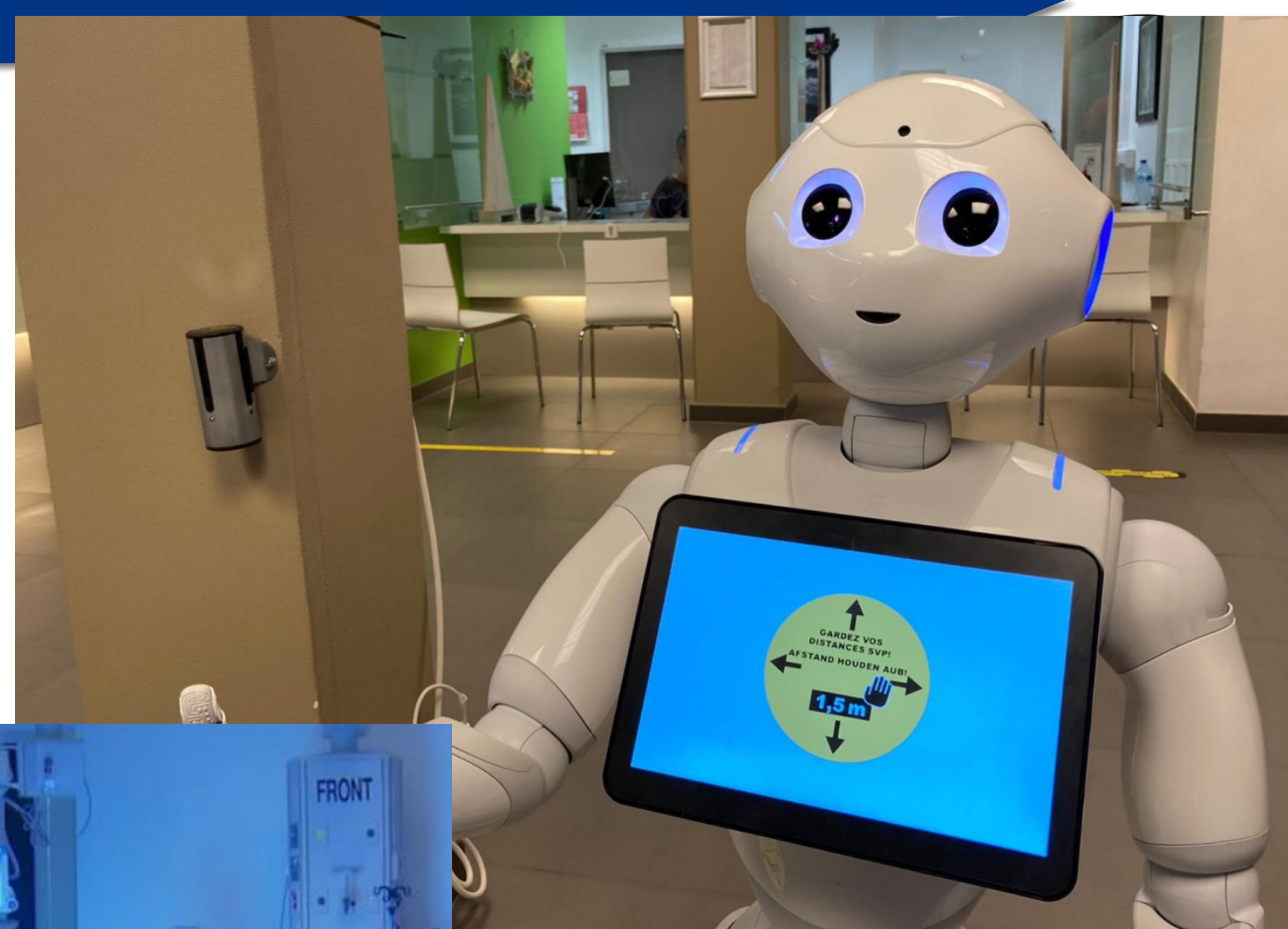
“Think differently: Where to we reach our people”



Distributed AI (DAI)

- ➔ Reduce: real needs
 - information on health
 - local information
 - language processing
- ➔ Speed
- ➔ Privacy

<https://medicalfuturist.com/8-exciting-medical-robot-facts/>



Source: <https://www.brusselstimes.com/>



Installation on RPI as part of TEK5530 course

Department of Technology Systems
TEK5530 - Measurable Security for IoT-Based Systems

Local Language Models in Raspberry Pi

- Installed on RPI 5 with 4 GB RAM
 - tinnyllama: 1.1b
 - deepseek-r1:1.5b
 - llama3.2:1b
- Limitations:
 - recommended 8 GB RAM for models
- Next steps
 - training local models

Stian Østgaard, Ulrik Sand



Get up and running with large
language models.

Run [DeepSeek-R1](#), [Qwen 3](#), [Llama 3.3](#), [Qwen 2.5-VL](#),
[Gemma 3](#), and other models, locally.

Download ↓

Available for macOS, Linux,
and Windows

Screenshot from the Ollama website

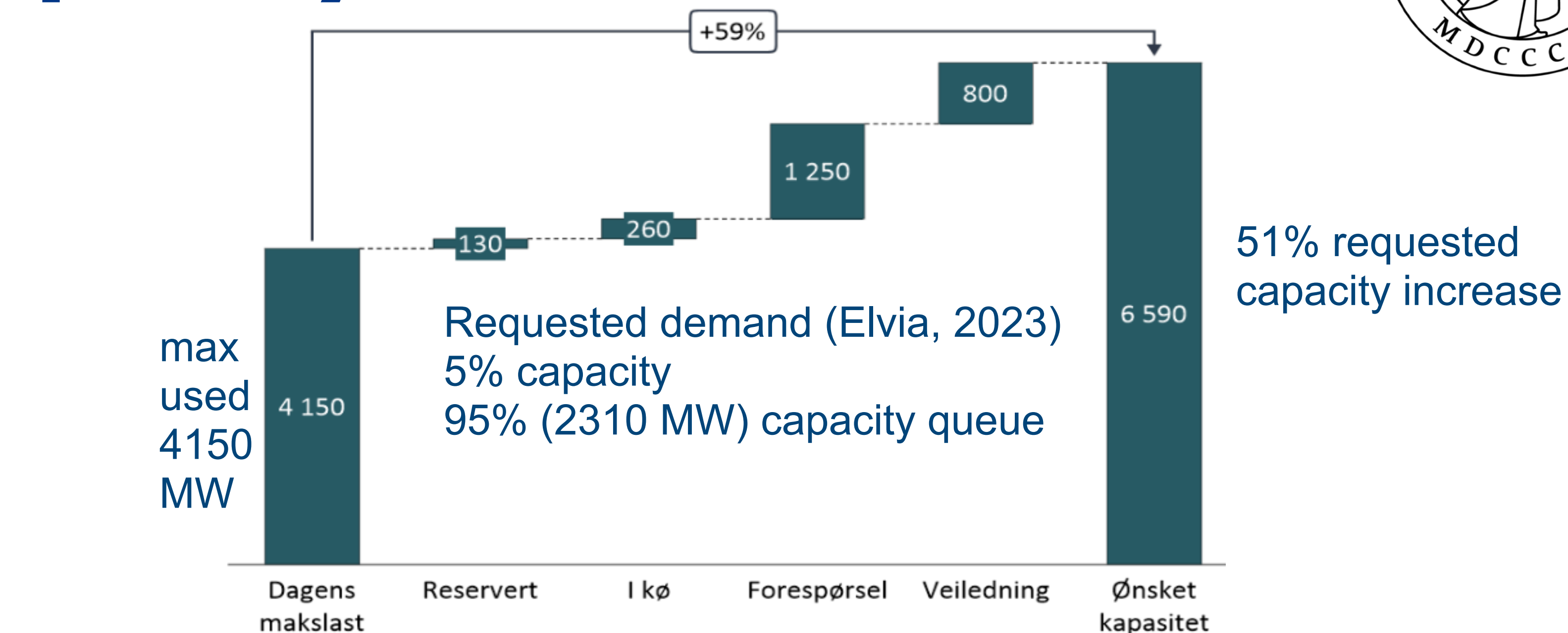
Distributed Grid

Potential Achievements

Limited Grid-capacity

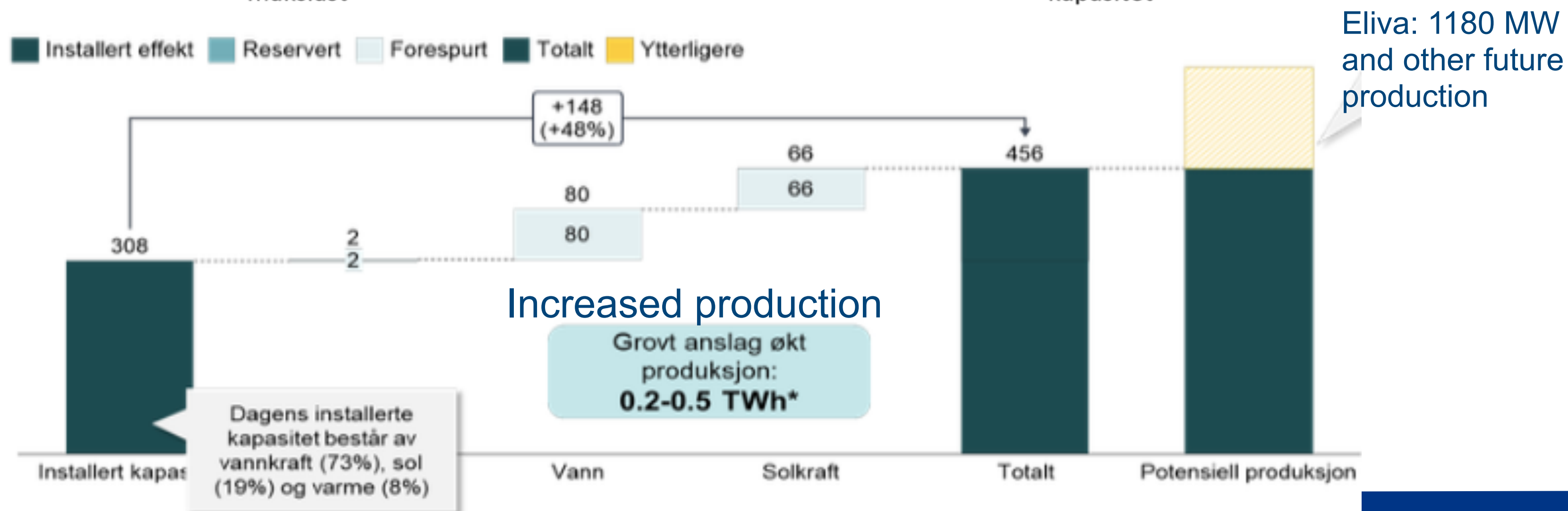
[SSB, <http://ssb.no/stabank/table/10314/>]

→ “No capacity for new usage in Oslo, Østfold and Akershus until 2030-2035”



[Kraftløftet Oslo Akershus, LO & NHO, 2023]

→ Green business development?

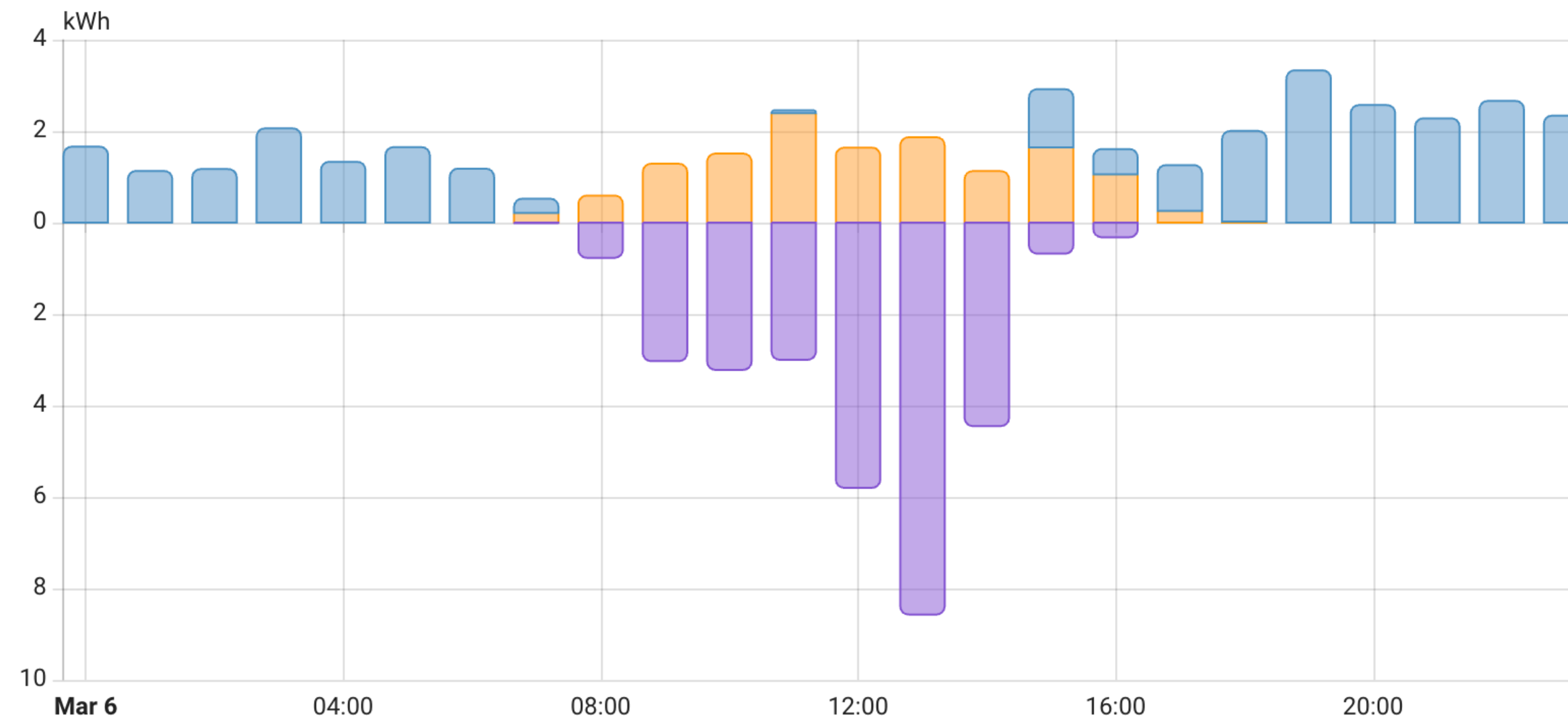


6 Mar 2025

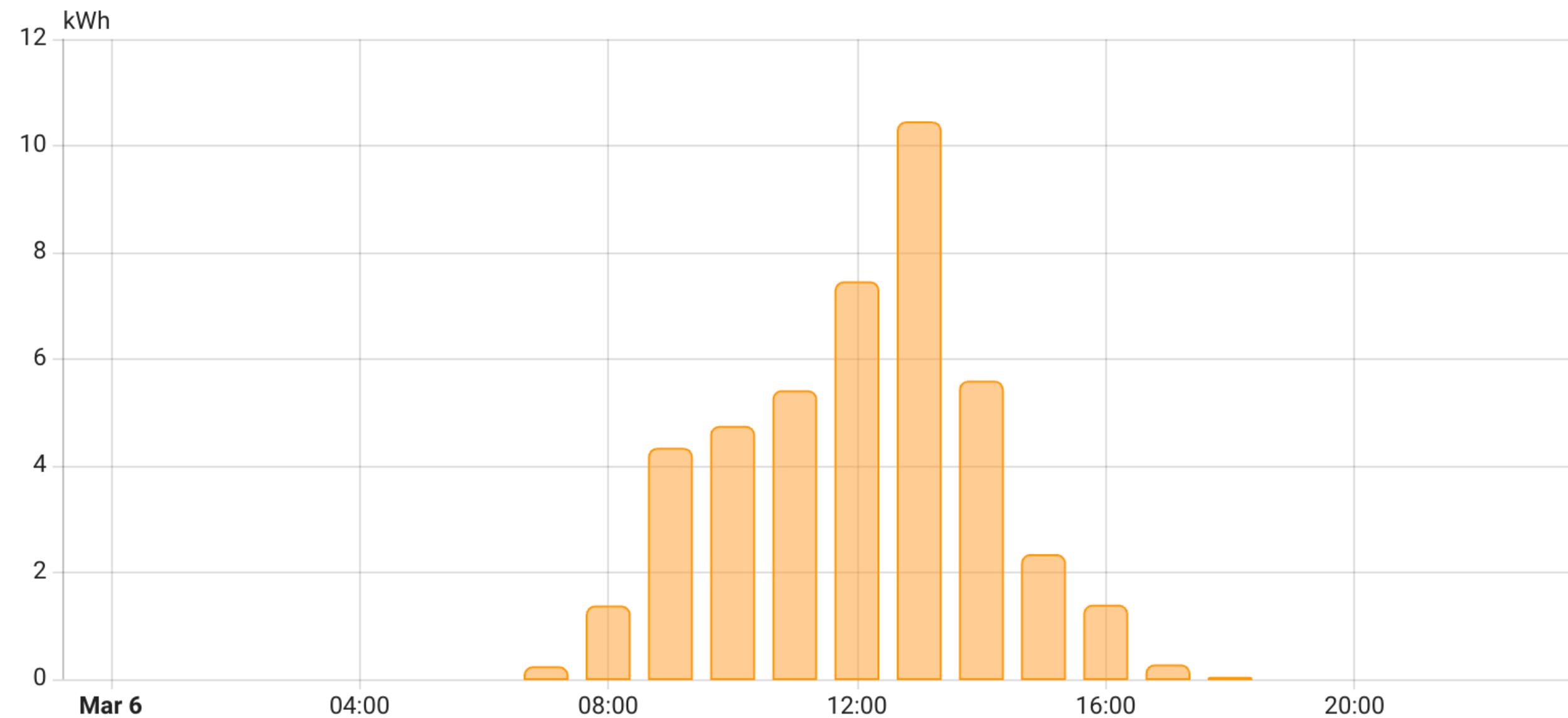
→ typical situation

- 31% self consumed
- 43,5 kWh produced (orange)
- 29,9 kWh to the grid (pink)

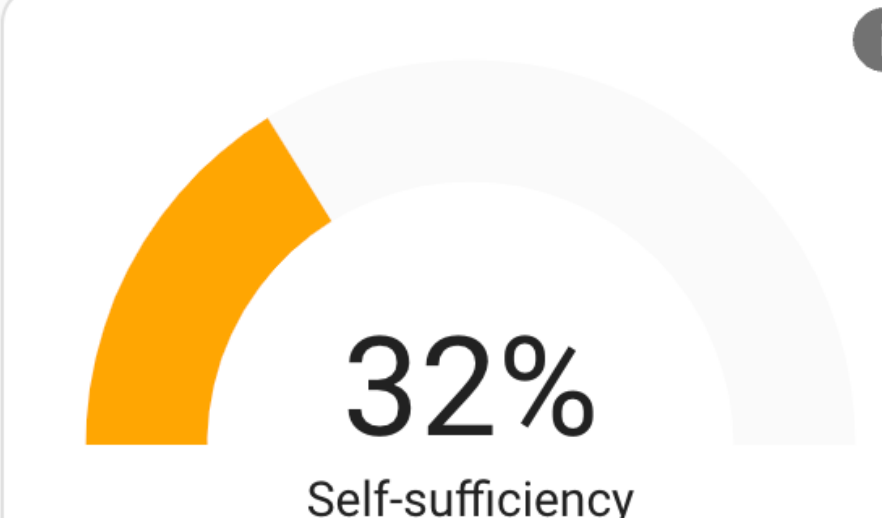
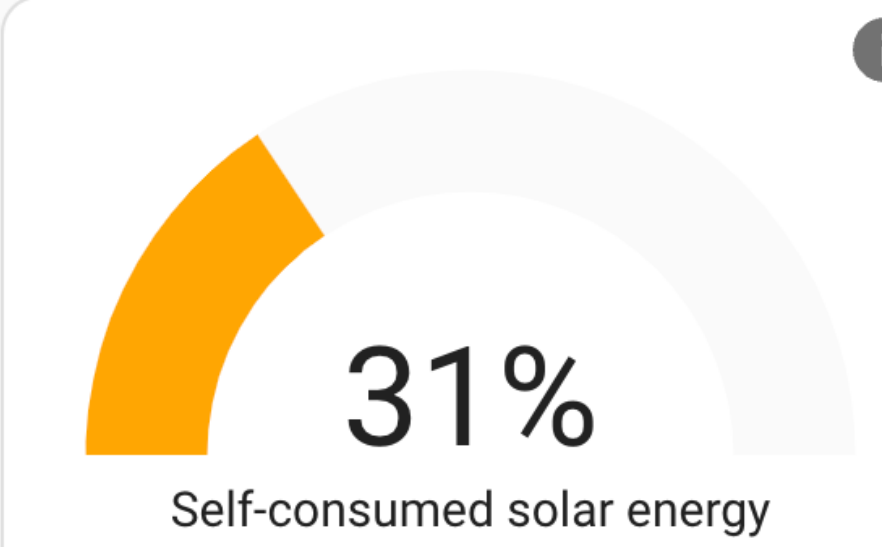
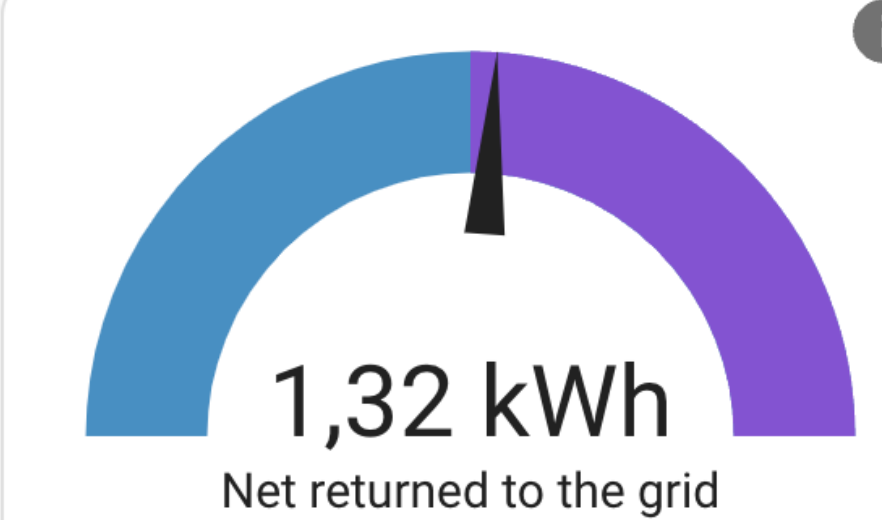
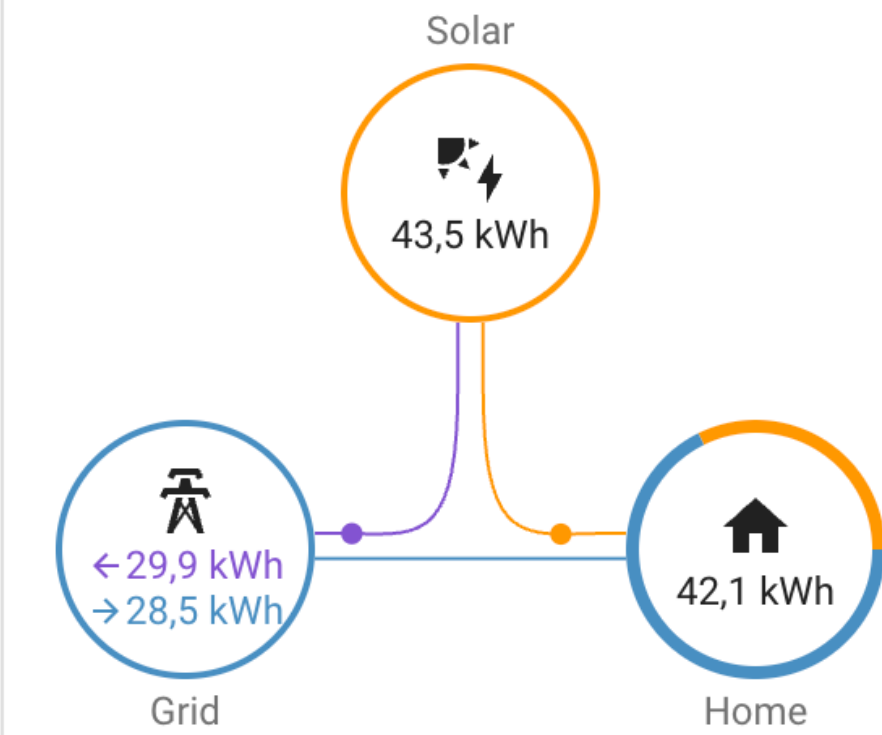
Electricity usage



Solar production



Energy distribution





DESSI infrastructure by ITS@Uio

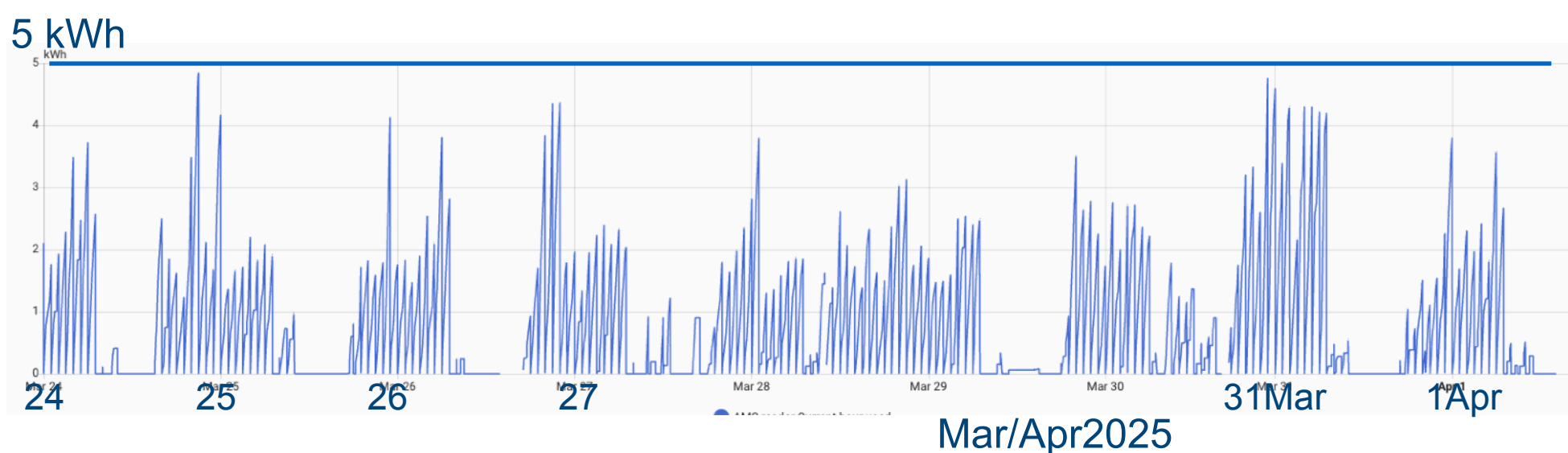
<https://www.mn.uio.no/its/english/research/projects/dessi/index.html>

→ busy hour reduction

- 0700-0900: 84%, 96%
- 1700-1900: 69%, 25%

→ Peak shaving

- below 5 kWh/h



Conclusions

- “Learn from history”
 - fog, edge computing/IoT
 - edge IoT
- Risk Exposure Model
 - Distributed: Security Class A
- Distributed AI (DAI)
 - RPI 5, 8 GB
- Research challenges in DAI
 - model federation
 - distributed learning
 - hierarchical models

Security Class A

Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

Additional Slides

Norway: 1 Billion NOK for 6 AI centres (100 Million USD = 1.79 USD/inhabitant)

- Artificial Intelligence Centre for the Empowerment of Human Learning
- **The Norwegian Centre for Trustworthy AI**
- **Center for AI & Creativity**
- Norwegian Centre for Embodied AI
- Norwegian Centre for Sustainable, Risk-averse and Ethical AI
- Norwegian Centre on AI for Decisions

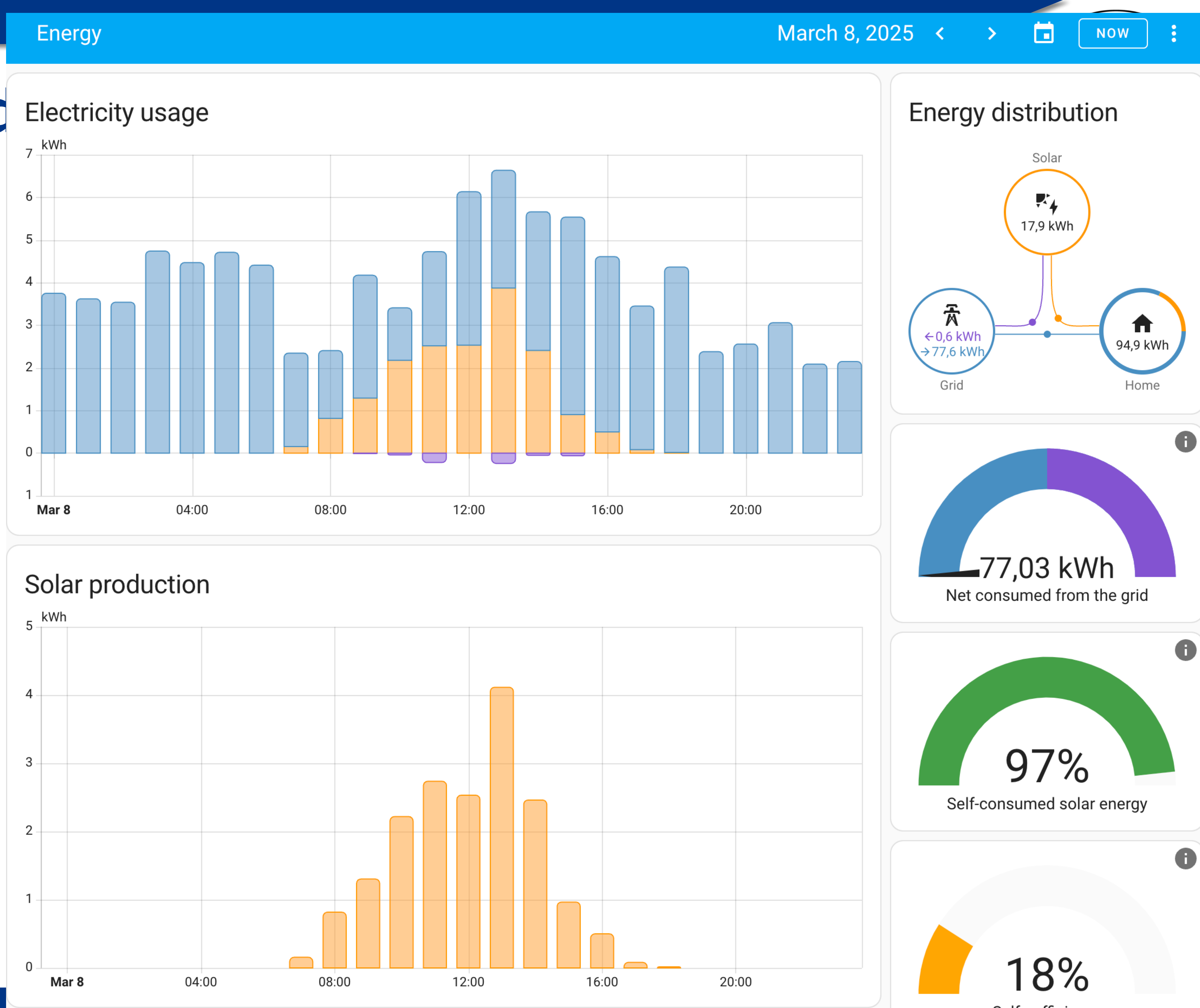
UiO is partner in all 6 centres, and leads 2

announced 12Jun2025 <https://www.forskningsradet.no/nyheter/2025/forskningscentre-kunstig-intelligens/>

Energy dashboard

8 Mar 2025

- Energy dashboard
 - blue: from grid
 - orange: from solar
 - ping: to grid
- Solar production
- Energy distribution



SC1: Relevant Protection Criteria

Protection Criteria	Security Functionality	P5	P4	P3	P2
Data Encryption	Encryption of data between system components	x	x	x	x
	Strong encryption mechanism	x	x	x	
	Credentials should not be exposed in the network	x	x	x	
	End-to-end encryption	x	x		
	Should not use custom encryption algorithms	x	x		
	Sensitive stored data should be encrypted	x	x		
Communication and Connectivity Protection	Have a minimal number of network ports open	x	x	x	
	Devices should not be accessible from the Internet	x	x	x	
	Only authorized components can join the network	x	x	x	
	Use only standard communication protocol	x	x		
Access Control	Disable remote access functionality	x			
	Only authorized devices can join the network	x	x	x	
	Default and weak passwords should not be used	x	x	x	
Monitoring and Analysis	Monitoring system components	x	x		
	Analysis of monitored data	x	x		
	Act on analysed data	x			

- ➔ Disable remote access functionality
- ➔ Only authorised devices can join the network
- ➔ The APIs calls should be authenticated and authorised
- ➔ Default and weak passwords should not be used

[Courtesy: Manish Shrestha, UiO, 2019]