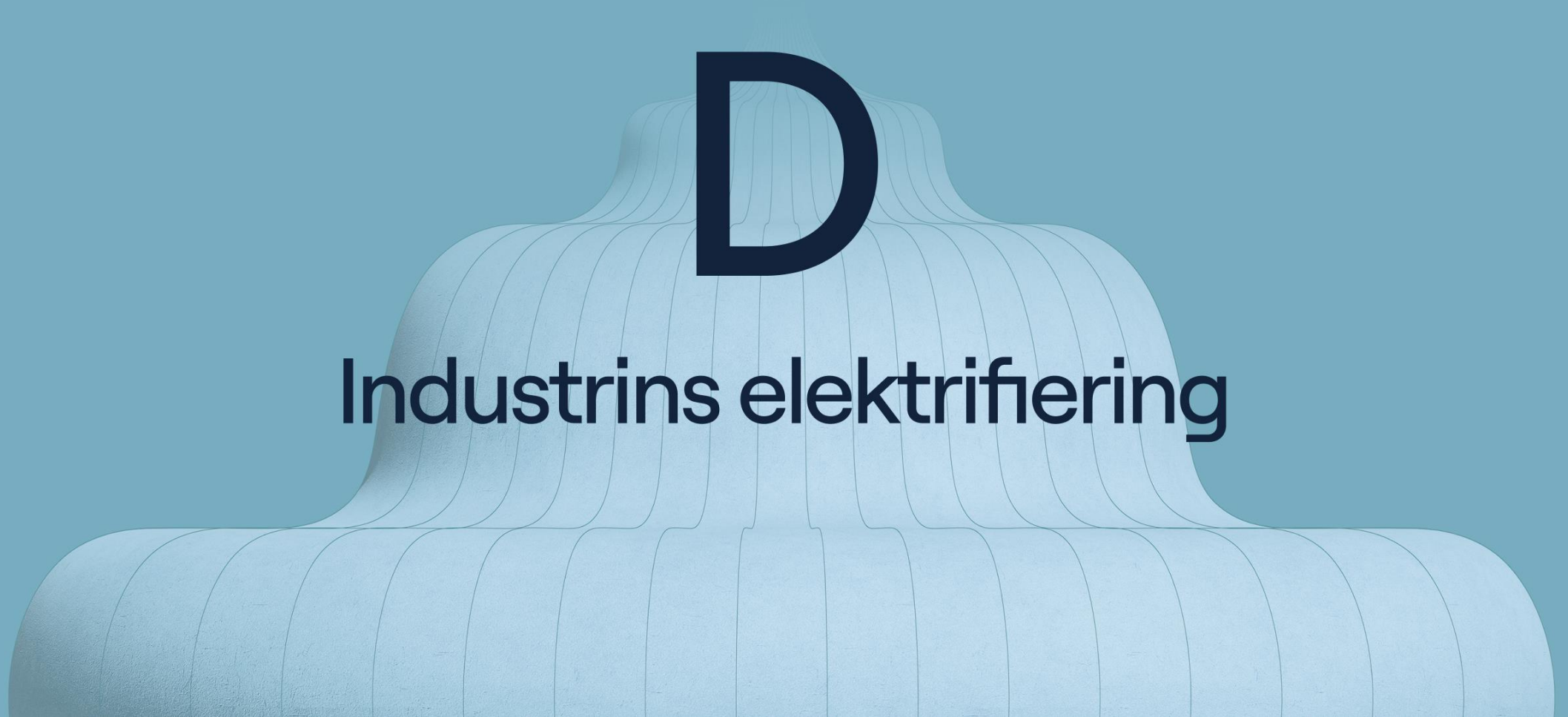
Välkommen till

D

Industrins elektrifiering



Agenda spår D

11.00 – 12.00

- Välkommen - del 1
- ACE CyberSafe (Christer Åhlund, LTU)
- SID: Säker datahantering för industriell digitalisering (Henrik Abrahamsson, RISE)
- AI mjukvara för planering och rapportering av elnätsutbyggnad (Elias Hartvigsson, Endre)
- Cybersecurity for Energy Communities of the Future (Mikael Asplund, LiU)
- Summering

12.00 - 13.00 LUNCH, entréplan

13.00 – 15.00

- Välkommen - del 2
- Den flexibla fabriken (Johan Tavast, Billerud)
- AIDE – Avancerad Industri, digitalisering & elektrifiering (Magnus Kuschel, Innovatum Science Park)
- Gruppdialog
- Summering

Projekt

ACE CyberSafe

Christer Åhlund, LTU


Arctic
Center of
Energy

ACE CyberSafe

An experimental test bed for increased cyber security in connected buildings

IN PARTERSHIP WITH

Skellefteå Municipality
Luleå University of Technology
Skellefteå Kraft
Th1ng
Bravida
ABB

POWERED BY
Avancerad Digitalisering
Vinnova

Arctic Center of Energy

ACE CyberSafe

- Syfte
  Att stärka cybersäkerheten i framtidens uppkopplade fastigheter med samexisterande IoT-system för olika funktioner i ett byggnadsautomationssystem (BAS), där cybersäkerheten i delsystem monitoreras och orkestreras utifrån de säkerhetslösningar varje delsystem tillämpar.

- Resultat
  Resultat av projektet kommer att tillgängliggöras i form av en testbed utrustad med state-of-the-art teknologi med flertalet IoT-system som kommunicerar mot en BAS funktionalitet med tillgänglighet till dataset, ML/AI-metoder och visualisering/dash-board som möjliggör anpassade utökningar för experiment

- Effekter
  Ett motståndskraftigt samhälle genom ökad kunskap och förståelse om cybersäkerhet i uppkopplade fastigheter med heterogena system genom anomalidetektering, autentisering och integritetskotroll av funktioner och data.


Arctic
Center of
Energy

Arctic
Center of
Energy

37.8% of computers managing smart building automation systems facing malicious attacks in the first half of 2019 originates from a **Kaspersky Lab report** published in 2019. The report analyzed the cybersecurity threats to smart buildings and building automation systems (BAS)

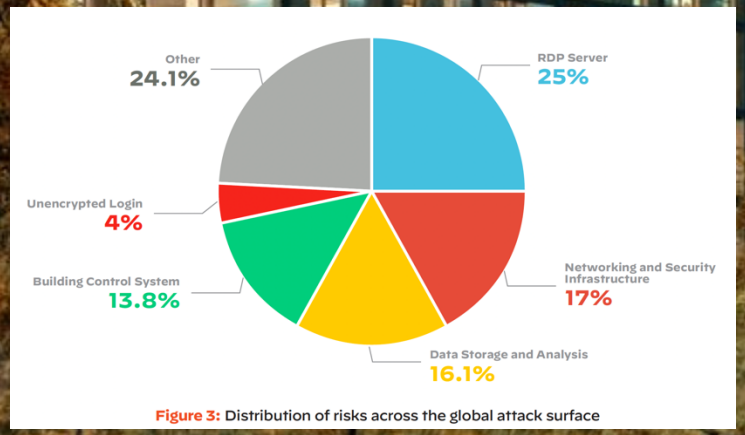
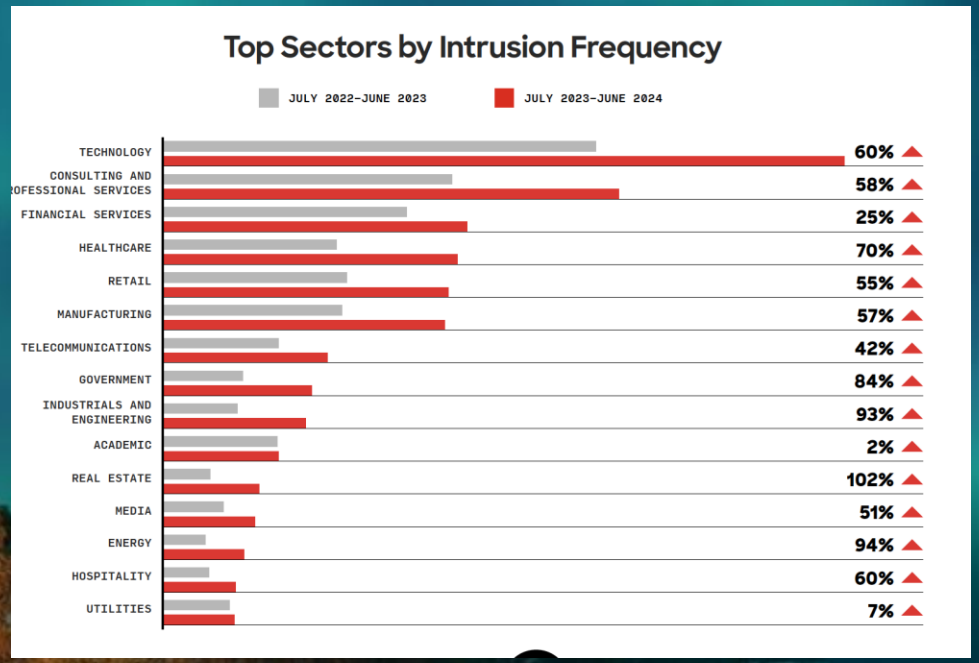


Figure 3: Distribution of risks across the global attack surface

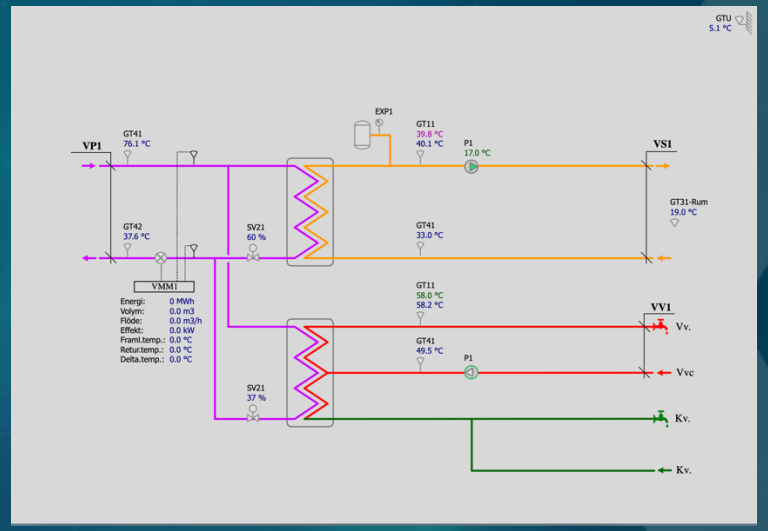
Source: Palo Alto, 2022 Cortex Xpance Attack Surface Threat Report

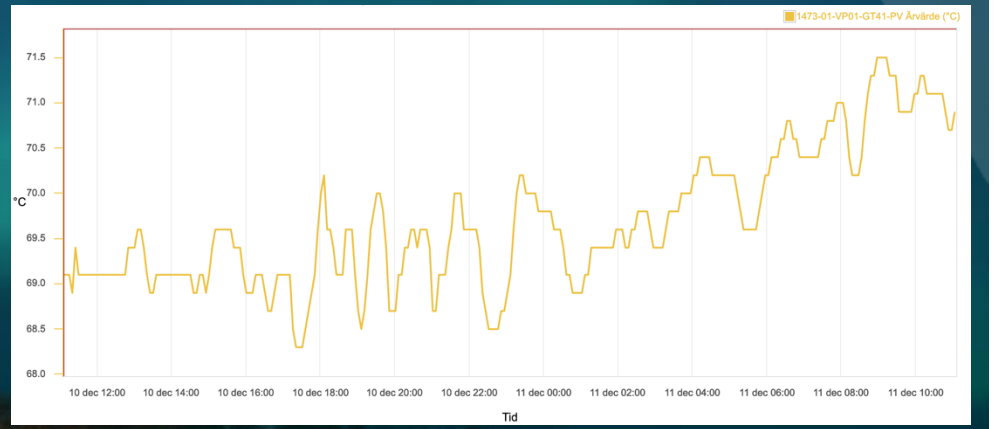


Source: Crowdstrike, 2024 Threat Hunting Report

Arctic Center of Energy

BAS monitorering…

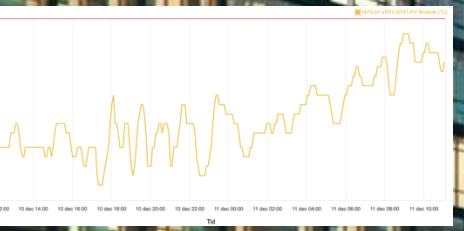




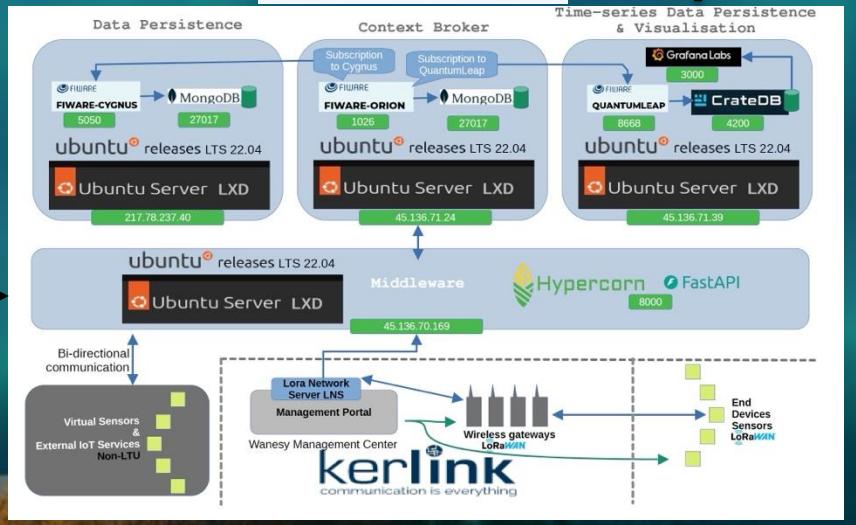
Arctic Center of Energy

…. samt monitorering av delsystemskommunikation

IoT Open



Schneider ? BMS systems



Snotra IoT-platform

Arctic Center of Energy

Frågor

Projekt

SID: Säker datahantering för industriell digitalisering

Henrik Abrahamsson, RISE

Secure data sharing for Industrial Digitalization

Henrik Abrahamsson, RISE

Mötesplats Avancerad Digitalisering
Göteborg, 2024-01-23

We are funded by the innovation and research program Advanced Digitalisation

Project SID: Secure data sharing for Industrial Digitalization

bron. RI.SE SENSATIVE VINNOVA Sveriges innovationsmyndighet

We are funded by the innovation and research program Advanced Digitalisation

Project SID: Secure data sharing for Industrial Digitalization

Two-year project, started in November 2023.

We are funded by the innovation and research program Advanced Digitalisation

Project SID: Secure data sharing for Industrial Digitalization

Two-year project, started in November 2023.

The goal is to enable Swedish industry to use privacy-preserving techniques for data sharing and data analysis to a greater extent and avoid the obstacles and pitfalls that exist today

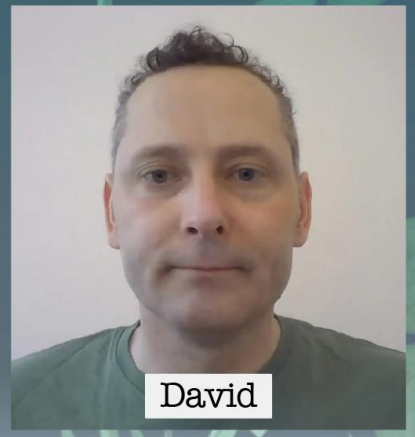
We are funded by the innovation and research program Advanced Digitalisation

Who we are

RISE


Henrik


Sima


David


Mohammadreza

Bron Innovation


Johan

Sensative


Sara


Fredrik

bron.

RI. SE

SENSATIVE

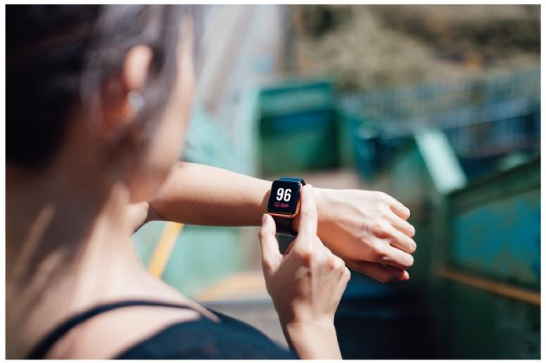
VINNOVA
Sveriges innovationsmyndighet

We are funded by the innovation and research program Advanced Digitalisation

Background and context

Digital transformation

- The digital transformation of industry and society increases data collection
- Data has become an important asset
- There is often a need to share data between processes and stakeholders



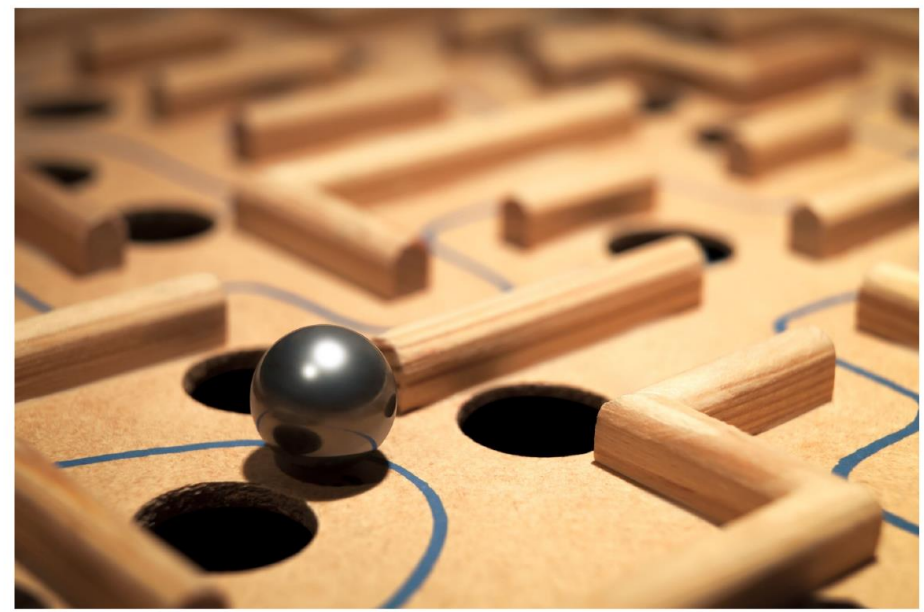
Data analysis and machine learning

- More data collection and combined data flows from multiple systems open up **great opportunities for data analysis and machine learning**

- For instance for: decision support, automation, optimization, anomaly detection, or new services

RI.
SE

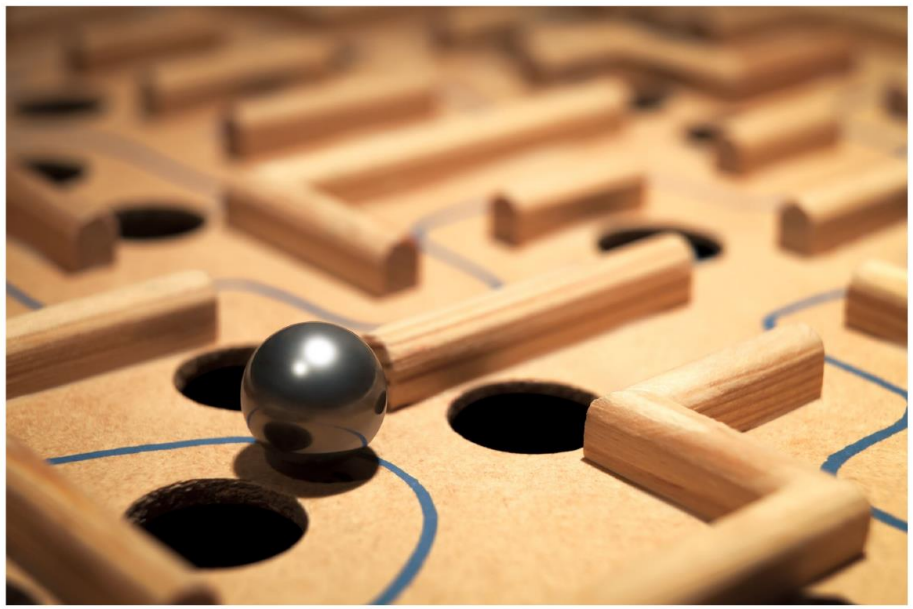
But there is an obstacle!



RI.
SE

But there is an obstacle!

Data is often sensitive to share between different stakeholders and between companies and customers



RI.
SE

But there is an obstacle!

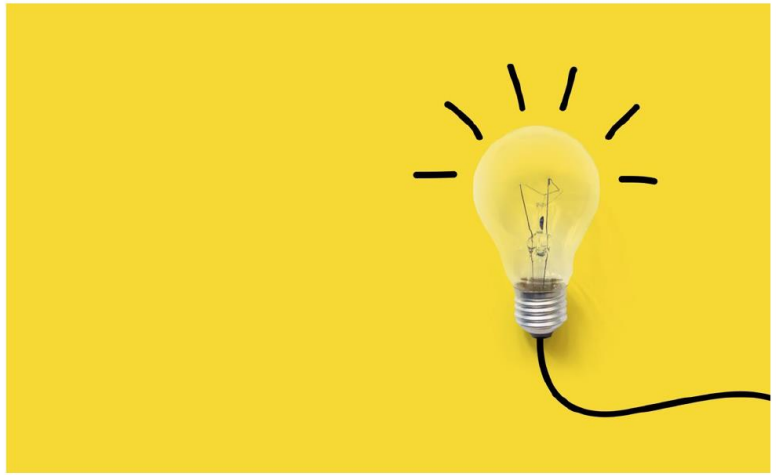
Data is often sensitive to share between different stakeholders and between companies and customers

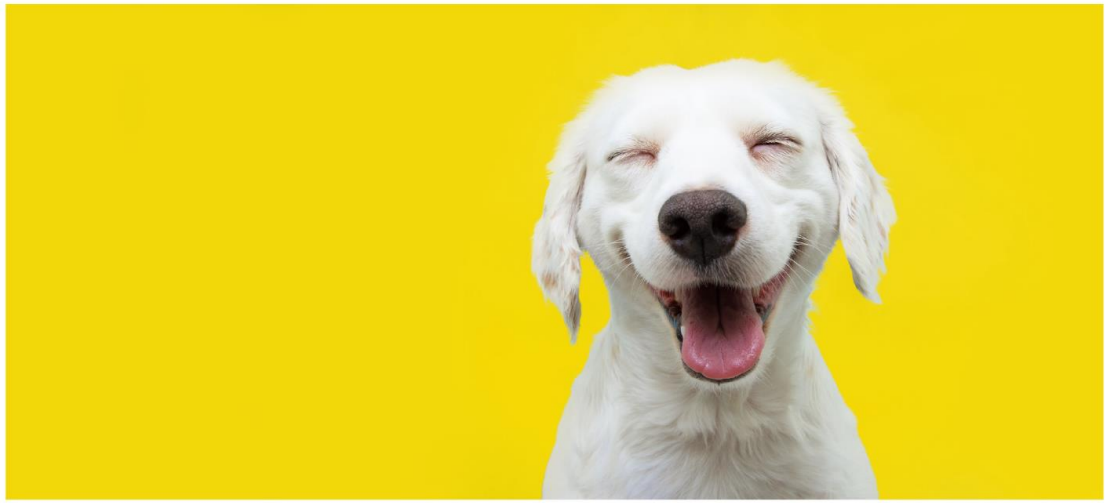
This prevents the use of data

RI.
SE

The good news

- There are promising methods for privacy-preserving data analysis available today
- For example, differential privacy and federated learning
- Methods that make it possible to analyze and gain insights from data but at the same time protect sensitive information

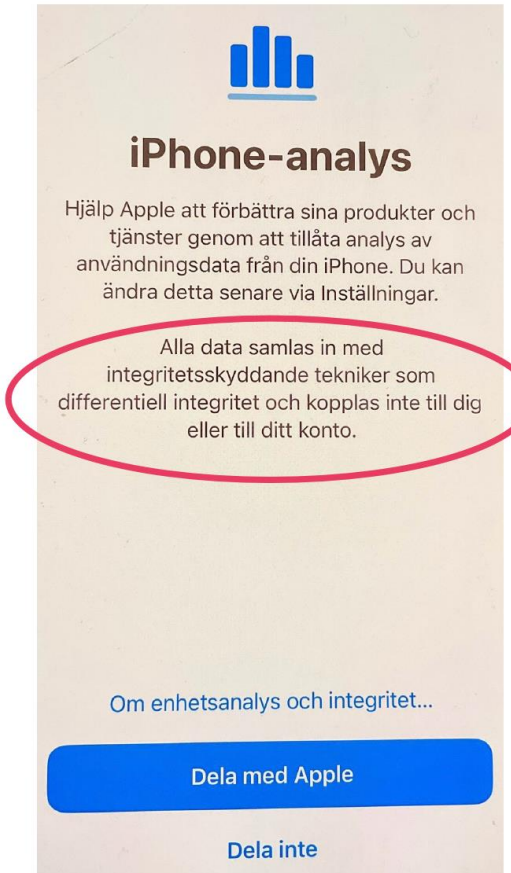


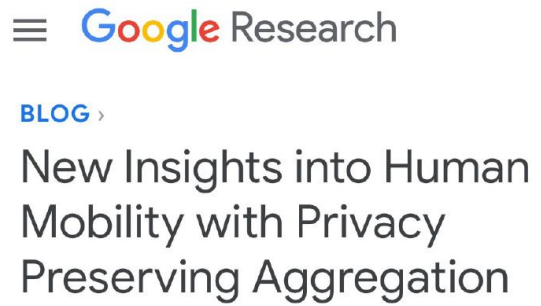


RI.
SE

Differential privacy

- Differential privacy is a popular and promising method to provide privacy to personal data
- Many big tech companies, such as Google and Apple, use differential privacy when collecting user data.
- Core idea: it should not be possible to tell if a particular individual is part of the data or not.
- Inject changes to individual data that do not change the statistics of interest for the group





Differential privacy

- Trade-off between how well the data is protected and how useful it is for analysis.
- Misuse and confused applications of differential privacy may give the impression that data is protected when it is not.
- Guidelines are needed

DOI:10.1145/3433638 Josep Domingo-Ferrer, David Sánchez, and Alberto Blanco-Justicia

Viewpoint

The Limits of Differential Privacy (and Its Misuse in Data Release and Machine Learning)

Differential privacy is not a silver bullet for all privacy problems.

COMMUNICATIONS OF THE ACM, July 2021.

csrc.nist.gov

Guidelines for Evaluating Differential Privacy Guarantees

Documentation Topics

Date Published: December 11, 2023

https://doi.org/10.6028/NIST.SP.800-226.ipd

RI. SE

Federated learning

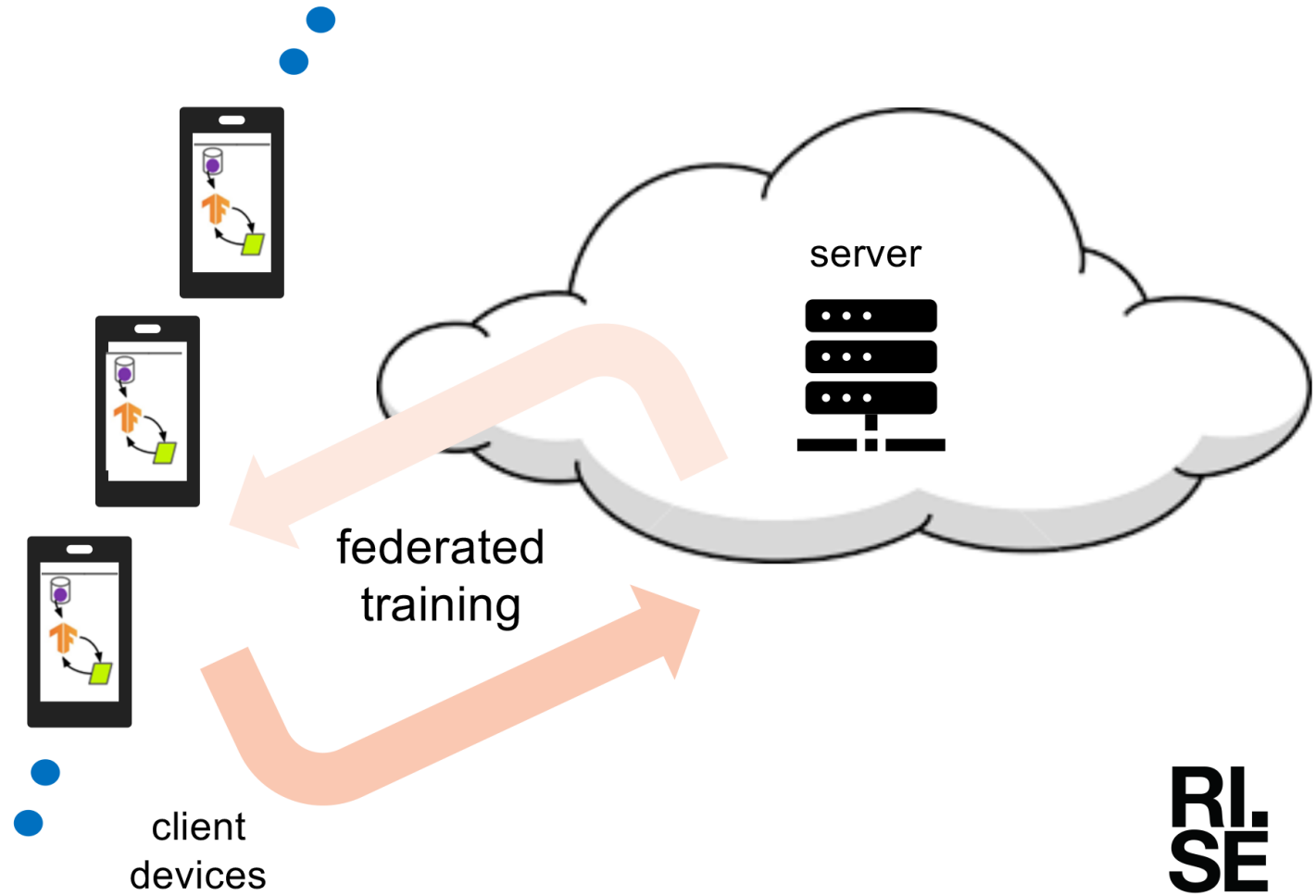
- Federated learning promotes privacy by keeping data local and enables machine learning models to be trained directly on user devices or edge servers

- Federated learning shares model parameters and updates rather than the raw data.

- Federated learning can be combined with techniques like differential privacy or encryption to protect leakage of sensitive information.

Federated Learning

- Data is generated locally and remains decentralized.
- Each client stores its own data and cannot read the data of other clients.
- Data is not independently or identically distributed.
- The clients can vary between use cases from IoT devices and mobile devices to data centers in different geographic regions



The SID-project has two complementary themes

Applied research

- From a scientific perspective, the project will **contribute to new knowledge, methods, and models.**
- We will **conduct privacy-, utility- and performance analysis** of differential privacy, federated learning and also federated learning combined with differential privacy and homomorphic encryption.
- We will **publish the results in scientific papers with open access.**

Industry collaboration

- The project objective is to enable Swedish industry to use privacy-preserving techniques to share and analyze sensitive data and avoid the obstacles that exist today.
- **Case studies with real-world data sets**
- **Workshops** to inform about privacy-preserving techniques, discuss use cases and experiences of using privacy-preserving techniques on real-world use cases.
- **Guidelines and Reports:** "A practical guide to how to use privacy-preserving methods and how to avoid pitfalls" (Oct. 2024, Aug. 2025)

Examples of case studies

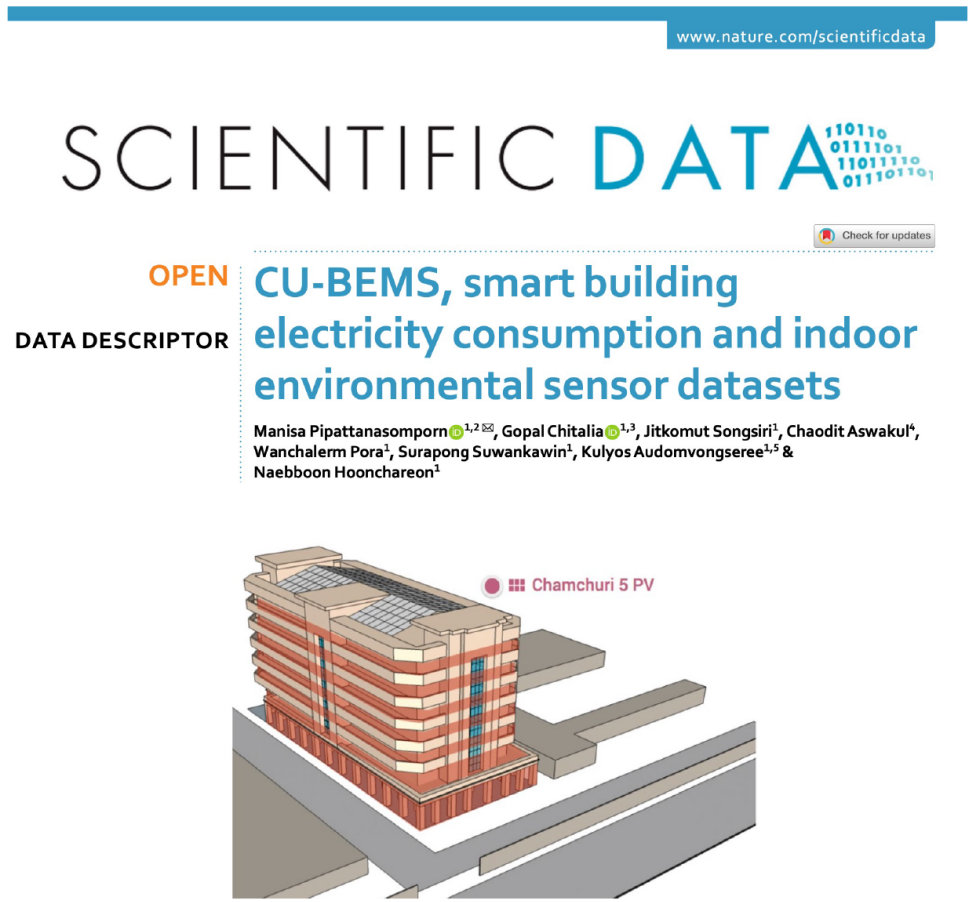
Three ongoing case studies

- We are currently working on three case studies with different types of data
  - Forecasts of electricity consumption in smart buildings (sensor data, timeseries)
  - Image analysis and object detection in construction environments (images)
  - Analysis of mobility and location data (positions, timeseries)

RI.
SE

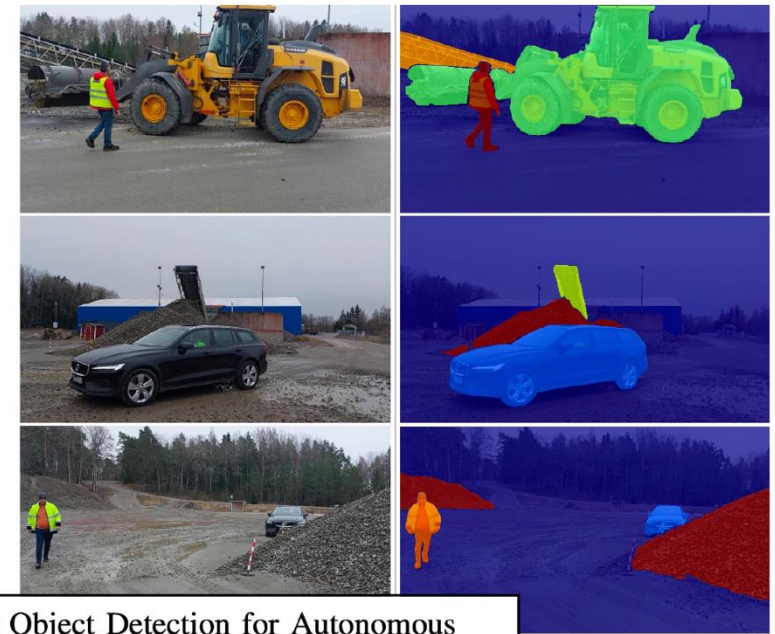
Case study 1: Forecasts of electricity consumption in smart buildings

- Forecasts useful for anomaly detection or optimization
- Data about electricity consumption might be sensitive
- Study using privacy enhancing Federated Learning
- Public data set (CU-BEMS)
  - time-series with sensor data,
  - energy consumption and outdoor temperature



Case study 2: Object Detection in Construction Environments

- Collaboration with Volvo CE
- Want to train an object detection model with images from diverse environments and different weather conditions.
- However, the images might reveal business sensitive information and cannot be shared between customers.
- The solution is to use federated learning to train a model across decentralized devices, without sharing the raw data



Enhancing Object Detection for Autonomous Machines in Private Construction Sites Through Federated Learning

Mohammadreza Mohammadi[a*], Maghsood Salimi[b*], Mohammad Loni[b], Sima Sinaei[a]
[a] RISE Research Institutes of Sweden
Email:{mohammadreza.mohammadi, sima.sinaei}@ri.se
[b] School of Innovation, Design and Engineering, Mälardalen University, Sweden
Email:{maghsood.salimi, mohammad.loni}@mdu.se
* Equal Contributions.

***Abstract*—A critical enabler of autonomous construction equipment is object detection, a computer vision task integral to navigation, task execution, and safety. However, challenging conditions at construction sites, such as mud splashes, dirt, and vibrations, can degrade object detection performance by causing sensor occlusions and image blurriness. Traditional adversarial training methods, which enhance model robustness by using perturbed data, are limited in construction environments due to the scarcity of diverse real-world adversarial data and the dynamic nature of these sites. Additionally, privacy concerns and site-specific data variability hinder data sharing across different construction sites. To overcome these challenges, this paper explores federated learning as a solution to enhance the robustness and adaptability of object detection models while preserving data privacy. FL enables continuous online learning without direct data exchange, offering a scalable and privacy-preserving approach to training models across diverse construction environments. Experimental results demonstrate that our approach improves model performance on the ConstScene**

nificant vibrations that can result in blurry camera images [5]. Therefore, leveraging object detection models in construction sites require additional considerations to provide robust and reliable predictions.

Adversarial training methods [6], [7] are popular for defending against adversarial examples and noisy inputs. These approaches involve using intentionally perturbed data to train the model to resist such manipulations. The perturbed image data for adversarial training can be obtain either from (i) real environment, or (ii) using generative models such as generative adversarial networks (GANs) [8] or diffusion models [9]. However, the real perturbed data collected from a single construction site lacks diversity, as construction sites often concentrate on specific tasks. In other words, certain types of adversarial inputs, such as dirty lens, might be rarely encountered in forestry sites compared to mines and quarries.

Case study 3: Analysis of mobility and location data

- Case study illustrating some of the pitfalls of differential privacy.
  - In particular, we look at the size of ϵ, utility and the unit of privacy.
- Public data set with records of taxi trips in New York City from 2009 to the present (2024).
  - pick-up and drop-off dates, times and locations as well as trip distance, fare amount and passenger counts.

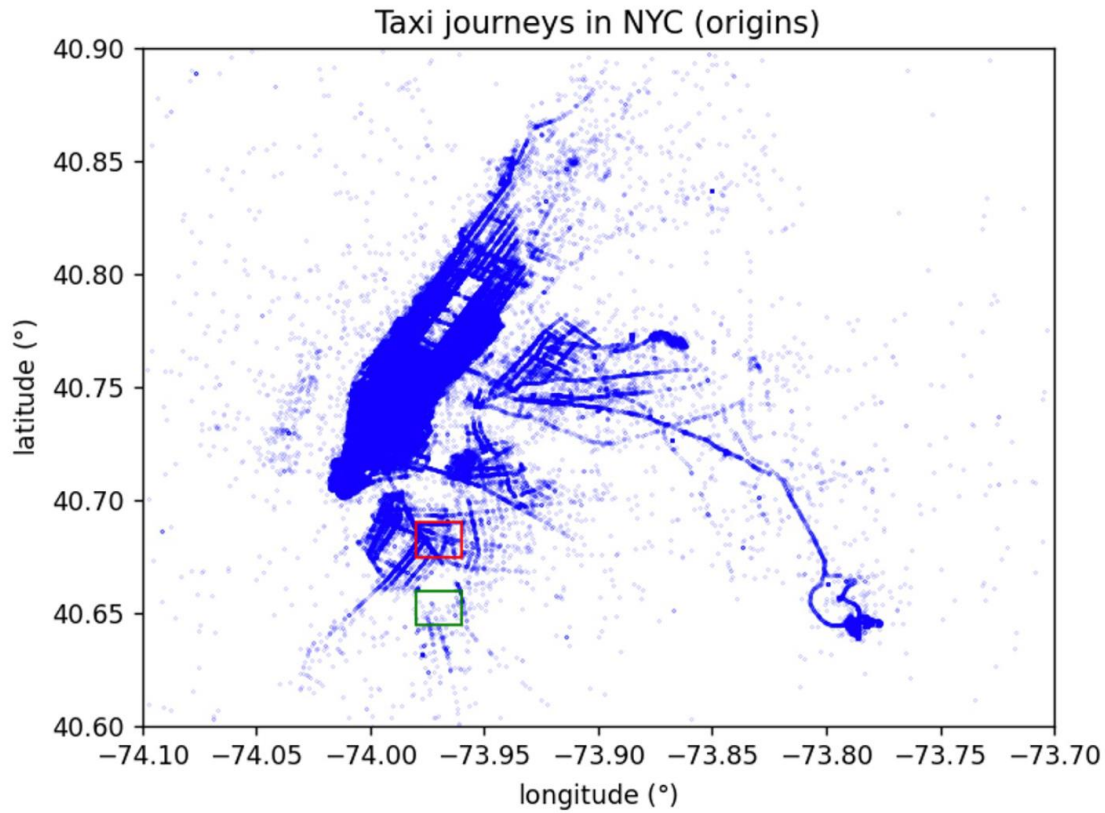


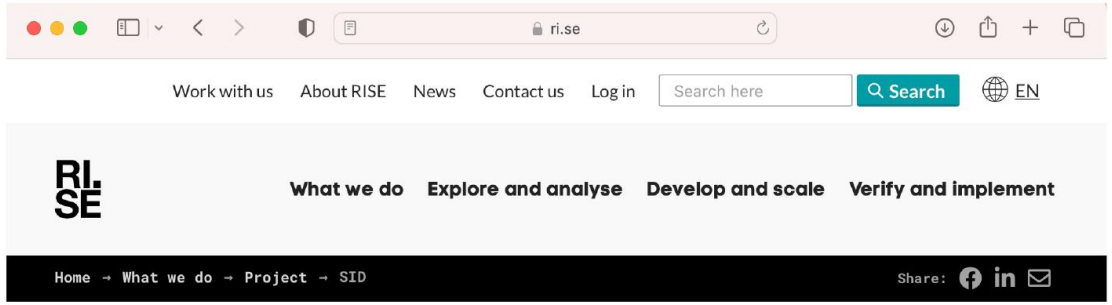
Figure 1: Scatter plot of origin of taxi trips.

RI. SE

Take away message about the SID-project

- The project is about privacy-preserving methods to share, analyse, and gain insights from data, while protecting sensitive information

- Research project with industry collaboration
  - Workshops and information about privacy-preserving methods.
  - Reports and guidelines how to use the methods
  - Case studies with real-world data sets



https://www.ri.se/en/what-we-do/projects/sid-secure-data-sharing-for-industrial-digitalization

Contact: henrik.abrahamsson@ri.se

Projekt

AI mjukvara för planering och rapportering av elnätsutbyggnad

Elias Hartvigsson, Endre

endre

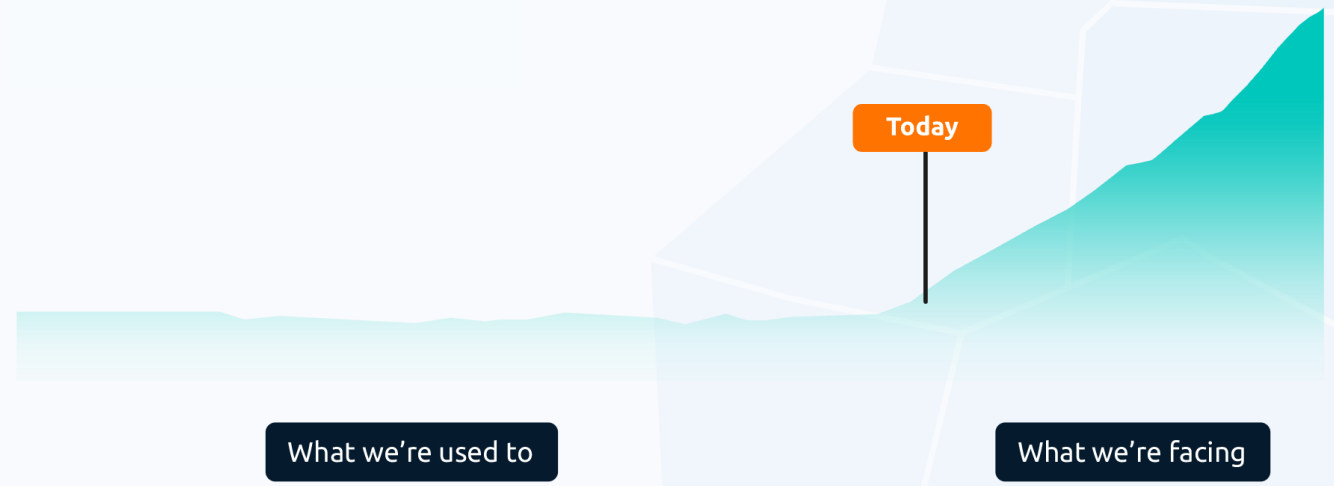
SMARTER GRID PLANNING USING SOCIETAL INSIGHTS

Elias Hartvigsson, PhD, CTO

Insights

As the world becomes electrified, society is changing

Which places completely new demands on our power grids



endre

Problems

For grid operators, this results in risk and uncertainties

Electric vehicles

What are the transportations future requirements on the grid?

New production

Where and what will be the impact of new production?

Grid congestions

Can my grid handle this new future?

Urbanization

Will my area increase or decrease in size?

Electrification of industry

Can, and will, industries is my area electricity?

endre

Problems

For grid operators, this results in risk and uncertainties

Electric vehicles

What are the transportations future requirements on the grid?

New production

Where and what will be the impact of new production?

Urbanization

Will my area increase or decrease in size?

Electrification of industry

Can, and will, industries is my area electricity?

Grid congestions

Can my grid handle this new future?

endre

Meet Endre

Smarter Grid Planning Using Societal Insights

endre

How?

Electric Vehicles

How large is demand and flexibility from heavy truck charging?

The old way

Manual

Manually collect historical records guessing charging demand.

Outcome

Reactive since demand or flexibility is not known beforehand, resulting in larger errors and higher investment risk.

The Smarter, Endre way

Outcome

Proactively know demand, and flexibility for heavy vehicle charging leading to better planning, and lower risks, using less resources.

Benefit

More reliable insights, faster.

endre

THANK YOU

endre

Projekt

Cybersecurity for Energy Communities of the Future

Mikael Asplund, LiU

CyREC

Cybersecurity for Resilient Energy Communities of the Future

Cybersäkerhet för framtidens resilienta energigemenskaper

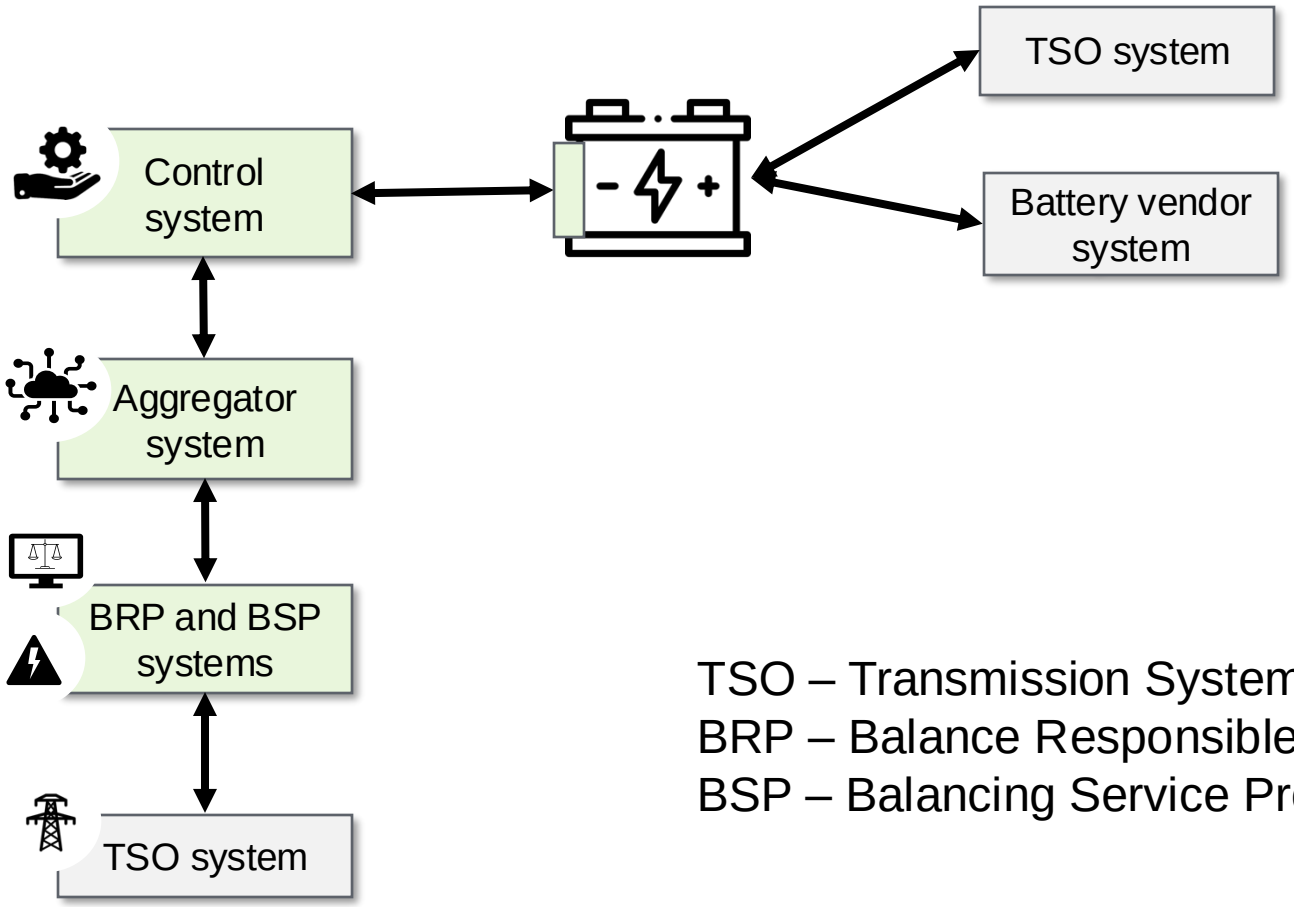
LINKÖPINGS UNIVERSITET RI.SE UKEAB SECTRA EMULATE

Energigemenskaper (Energy Communities)

- “an effective and cost-efficient way to meet citizens' needs and expectations regarding energy sources, services and local participation”[1]
- decentralisering – många aktörer
- fysiska eller virtuella
- möjliggörare för flexibilitet

[1] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU

Exempelscenario



TSO – Transmission System Owner
BRP – Balance Responsible Party
BSP – Balancing Service Provider

Frågeställningar

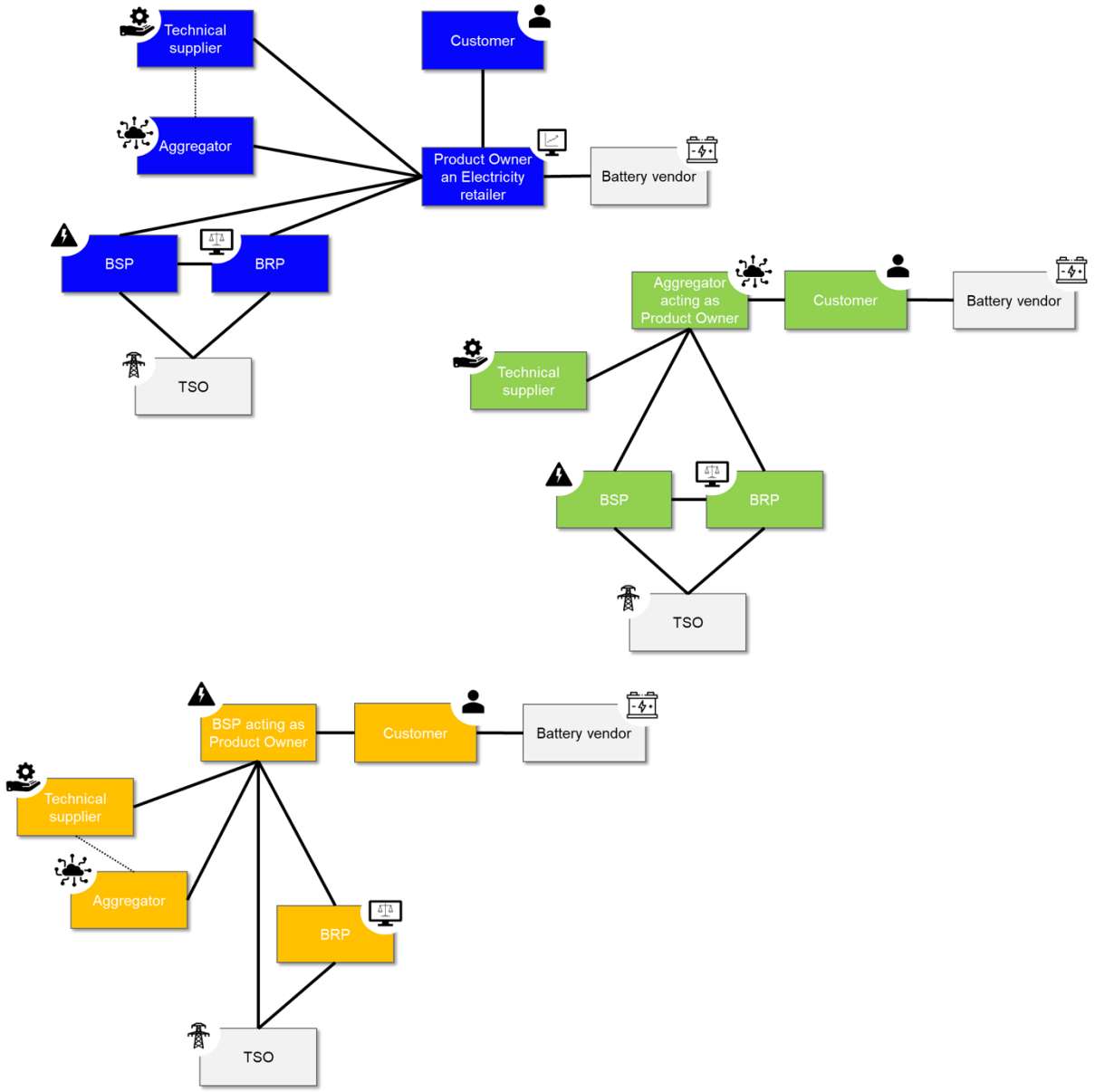
- Vad är möjliggörare och hinder för nya teknologier kopplat till energigemenskaper?
- Hur kan vi modellera effektiva samarbeten kring säkerhet i en miljö med många aktörer?
- Hur kan vi kombinera nya digitala plattformar med kritisk infrastruktur?
- Hur anpassar vi metoder för hot- och riskanalys?
- Hur kan vi utvärdera energigemenskapers förmåga att motstå cyberattacker?

Frågeställningar

- Vad är möjliggörare och hinder för nya teknologier kopplat till energigemenskaper?
- **Hur kan vi modellera effektiva samarbeten kring säkerhet i en miljö med många aktörer?**
- Hur kan vi kombinera nya digitala plattformar med kritisk infrastruktur?
- **Hur anpassar vi metoder för hot- och riskanalys?**
- Hur kan vi utvärdera energigemenskapers förmåga att motstå cyberattacker?

Modeller för samarbete

- flera modeller möjliga
  - beror på lagstiftning och affärsmodeller
- olika intressen/agendor från existerande aktörer
  - nya aktörer introduceras
- idag framväxande: hybrider av olika modeller
- stor osäkerhet vad gäller riskansvar och lösningar



Hot- och Riskmetoder

- identifierar risker där IT och OT möts
  - hur säkrar vi nya plattformar och dess kontroll av styrsystem
- tar hänsyn till både cybersäkerhet och funktionssäkerhet
- kontinuerlig riskhantering
  - uppdateras allt eftersom nya kända sårbarheter identifieras
- hur kan de involverade parterna identifiera och belysa risker
  - skall enkelt kunna integreras i befintliga processer

Kort om projektet i övrigt

- Nuvarande status
  - Månad 15 av 24
  - Avslutas november 2025
- Andra resultat
  - 4 exjobb (1 avslutat)
  - Säkerhetsmodeller för attacksimulering och intrångsdetektering
- Total budget: 10Mkr
- Partners
  - Emulate Energy
  - Linköpings universitet (LiU)
  - Utvecklingsklustret Energi AB
  - RISE Research Institutes of Sweden
  - Sectra

Lunch

Entreplan, vi ses kl 13