Välkommen till

E

Cybersäkerhet och resiliens

Agenda spår E – del 2

13.00 – 13.20	Inspirationstalare – Jan-Åke Larsson, Linköpings universitet
13:20 – 14.00	Projektpresentationer
14.00–14.14	Mingel i rummet
14.14 -14:53	Projektpresentationer
14.53–15.00	Summering

Inspirationstalare

Kvantkrypto

Jan-Åke Larsson, Linköpings universitet

Projekt

ACE CyberSafe

Christer Åhlund


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)

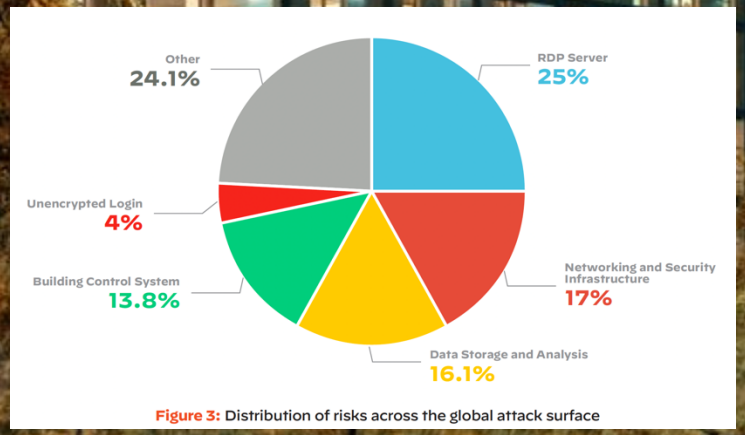
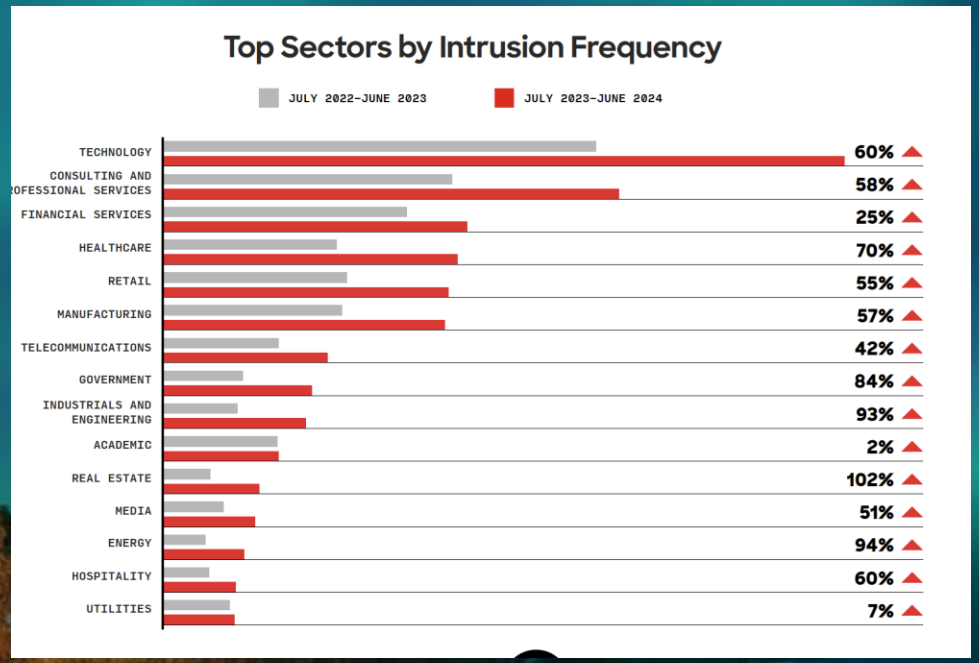


Figure 3: Distribution of risks across the global attack surface

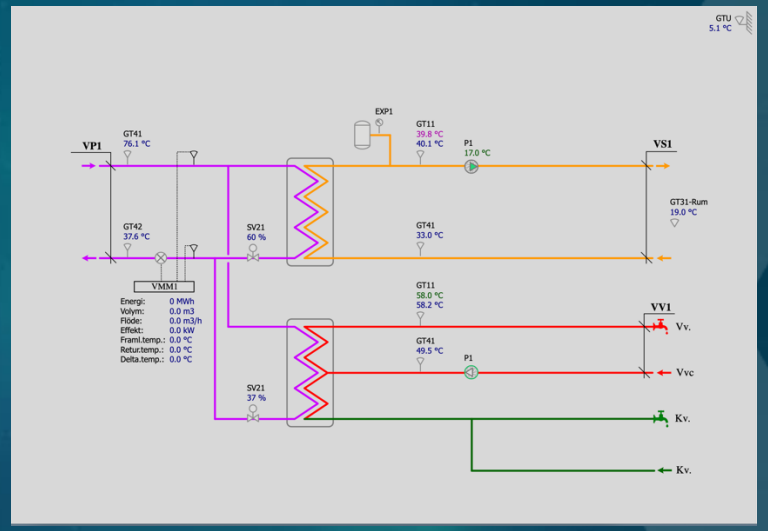
Source: Palo Alto, 2022 Cortex Xpance Attack Surface Threat Report

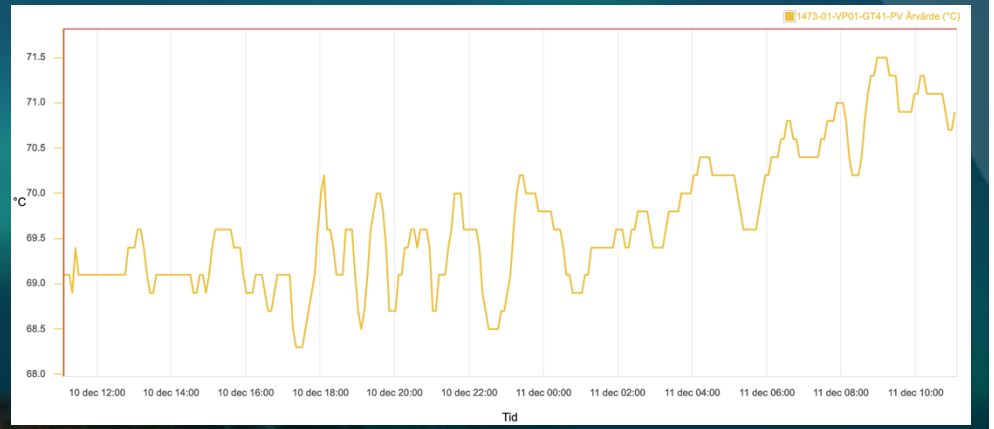


Source: Crowdstrike, 2024 Threat Hunting Report

Arctic Center of Energy

BAS monitorering…

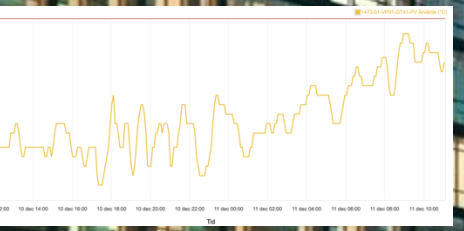




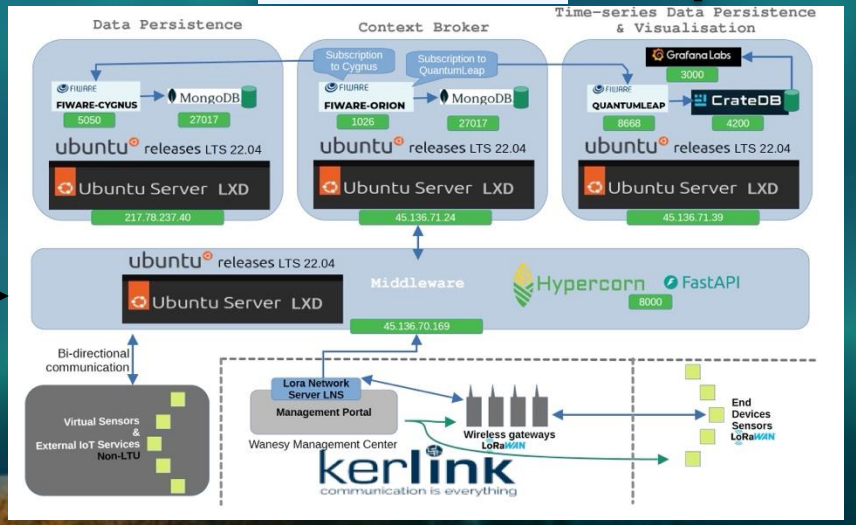
Arctic Center of Energy

…. samt monitorering av delsystemskommunikation

IoT Open



Schneider ? BMS systems



Snotra IoT-platform

Arctic Center of Energy

Frågor

Projekt

SEAS (Sustainable Energy with Adaptive Security)

Pierre Kleberger

SEAS
Sustainable Energy with Adaptive Security

Hållbar energi med adaptiv säkerhet

LINKÖPINGS UNIVERSITET RI.SE UKEAB SECTRA

Publicerat: 2023-10-31 09:30

Nu blir det enklare för variabla resurser att delta på stödtjänstmarknaderna

Under nästan två år har en pilotstudie för resurser med variabel produktion och förbrukning pågått för att möjliggöra för dessa typer av resurser att delta på stödtjänstmarknaden. Nu har förkvalificeringsprocessen förtydligats för variabla resurser och därmed avslutas pilotstudien.

Nyhet: Nya föreskrifter om incitament för kvalitet och effektivt nätutnyttjande i intäktsramsregleringen

Nu finns nya föreskrifter publicerade om incitament för kvalitet och effektivt nätutnyttjande i intäktsramsregleringen. Föreskrifterna träder i kraft den 15 november 2023.

Fler bytte till timprisavtal och installerade solceller

För att själva kunna påverka sina elkostnader genom att flytta sin elanvändning till tider då priset är lägre, var det många som ville byta till timprisavtal. Många ville också installera solceller. Under 2022 ökade installationerna av solceller med nästan 50 procent jämfört med året innan.

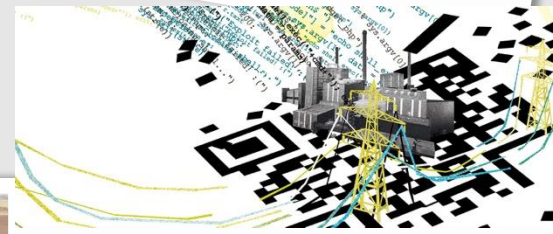
Freja Offshore ansöker om tillstånd för havsvindpark på Sveriges östkust

Publicerad: 31 oktober 2023 11:29

Nyhet: Höga elpriser ledde till ökat intresse och fler flexibla kunder på elmarknaden

Under 2021 och 2022 steg elpriserna kraftigt i Sverige. Konsumenterna ifrågasatte den svenska elmarknaden samtidigt som de högre priserna fick fler att vilja göra medvetna val.

Insats för IT- och OT-säkerhet inom energisektorn start oktober 2022. Motiveringen till insats: "*I och med ett **ansträngt säkerhetspolitiskt läge** i Sveriges närområde där **energi är en del av konflikten och IT-incidenter mot energisektorn har observerats** har MSB beslutat att starta upp en samverkansgrupp rörande cyberfysiska system kopplat till energi. Syftet med denna gruppering är att proaktivt dela information och i händelse av incidenter samordna, varna och stödja.*"



Så ska energibranschen klara de ökade cyberhoten

CYBERSÄKERHET It-hoten mot energibranschen har ökat under senare år. Nu är flera initiativ på gång för att stärka cybersäkerheten i branschen. Detta ställer större krav på samtliga energibolag. Men att tolka alla nya direktiv och

Volvo Cars startar ny affärsenhet – ska tjäna pengar på laddningen

Volvo Cars skapar en ny affärsenhet för produkter och tjänster som rör laddning åt båda håll. "Batteriet i våra bilar är en energikälla som kan användas till mer än körning", säger Alexander Petrofski, chef för nya Volvo Cars Energy Solutions.

EU:s energisystem behöver bli mer flexibelt enligt ny rapport

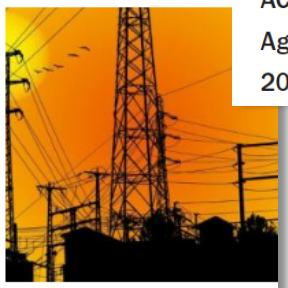
En ökning av förnybar energi från sol och vind ställer krav på ett mer flexibelt energisystem. Det skriver EU-myndigheten ACER* och Europeiska miljöbyrån (European Environment Agency (EEA)) i en gemensam rapport som publicerades den 20 oktober.

Uppsala planerar kombinerad energilösning för stärkt krisberedskap

Uppsala kan gå i bräschen för en ny kombination av energikällor som kan stärka stadens krisberedskap och påskynda övergången till fossilfri energi. En förstudie av Uppsala Vatten och Avfall AB och BioDriv Öst föreslår att kombinera biogas, vätgas...

OX2 och Nordkalk gör förstudie om e-bränsleproduktion på Gotland

Europas framtida energiutmaningar - Flexibilitet som hörnsten för förnybar energiövergång



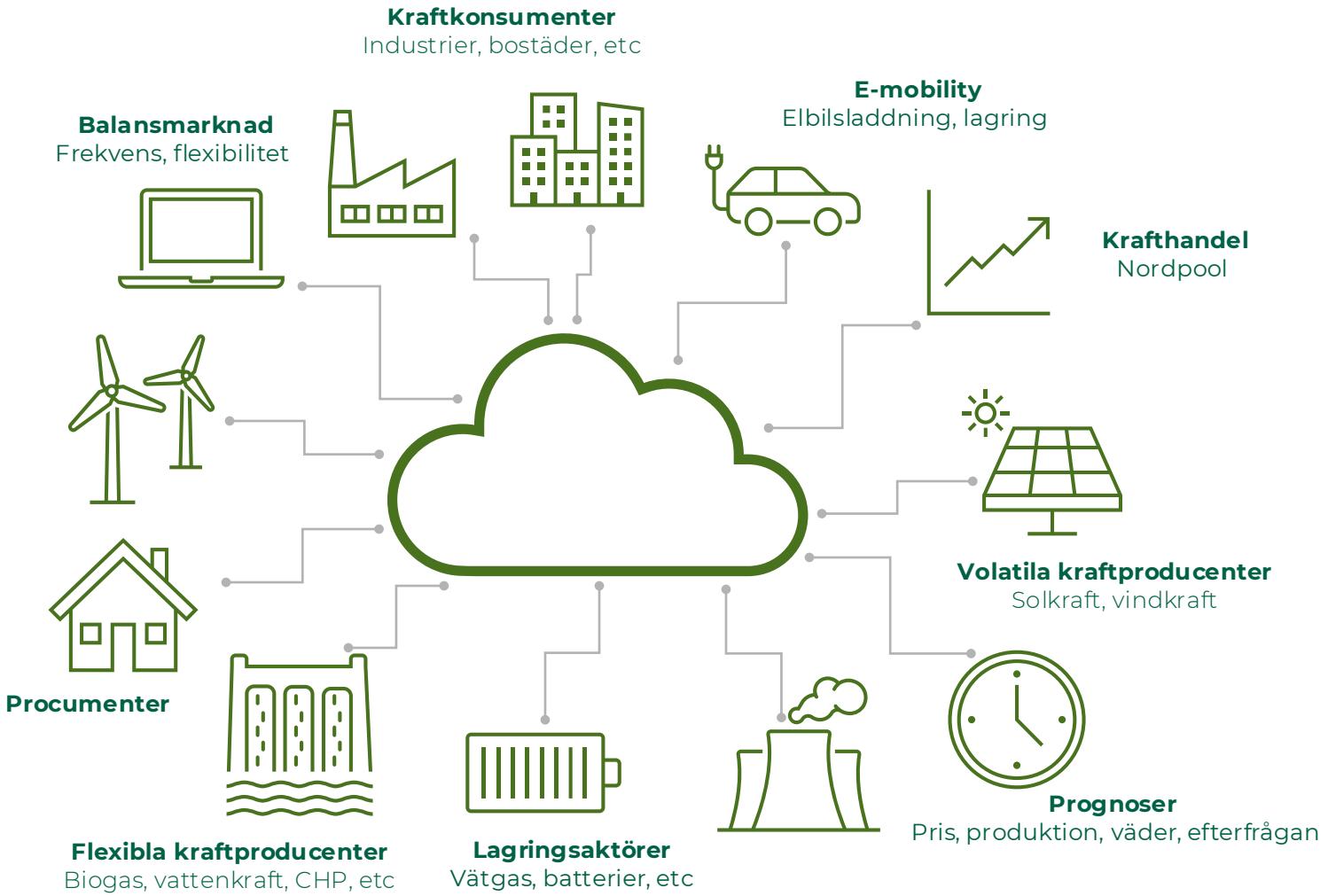
Svenska kraftnät varnar - Vattenkraftens miljöanpassning hotar energisystemet

Ekosystem av molnbaserade styr- och kontrollsystem

Nätverk av decentraliserade uppkopplade

- effektgenererande enheter
- flexibla effektanvändare
- lagringssystem

Mer diversifierat, mer distribuerat



Om projektet

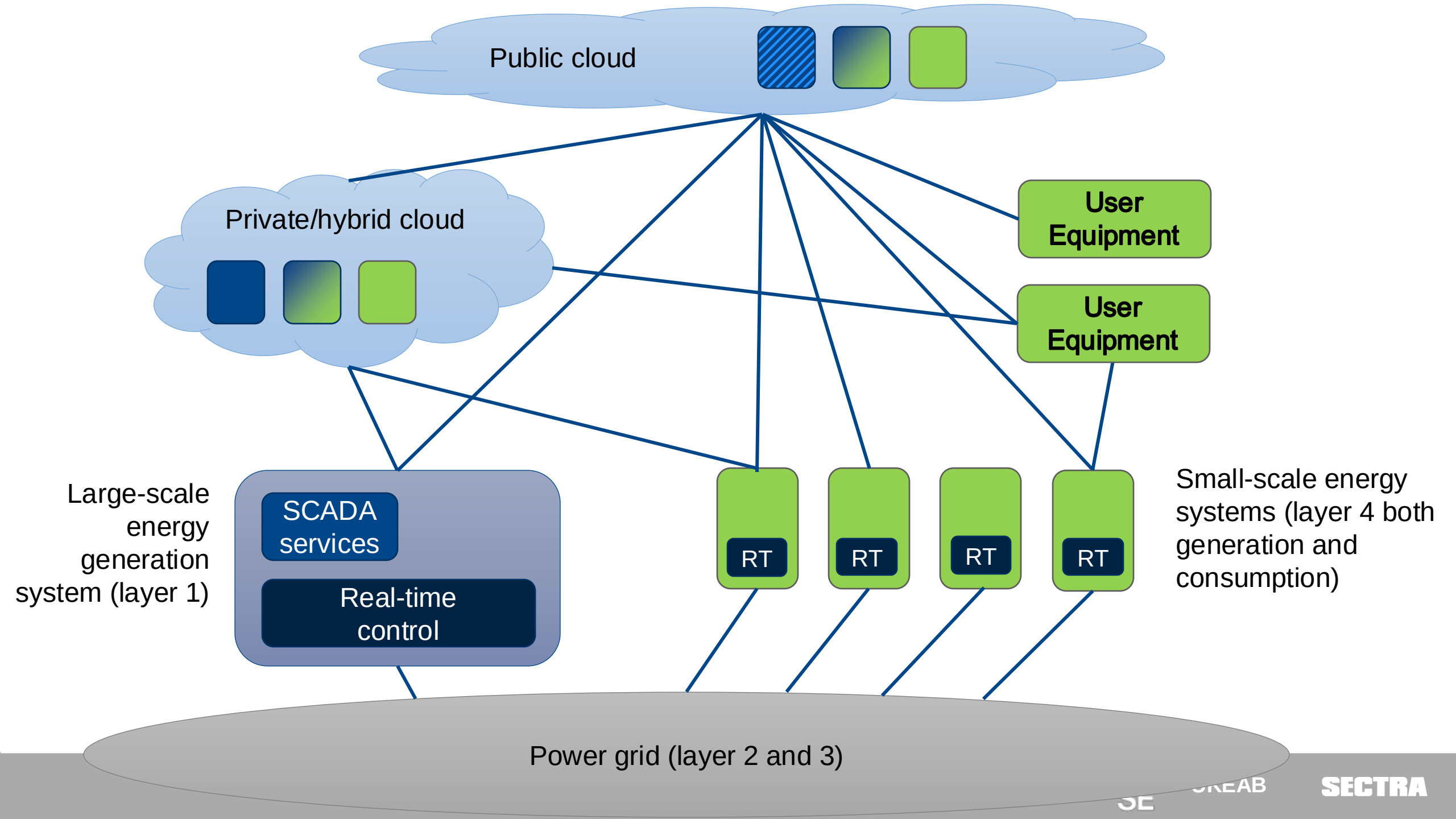
- Finansierat av Vinnova
- Partners
  - Linköpings universitet (LiU)
  - Utvecklingsklustret Energi AB
  - RISE Research Institutes of Sweden
  - Sectra
- Period: 2021-2023
- Vi vill kunna **möjliggöra omställningen** till förnybar energi genom förbättrad **riskhantering** och **adaptiv säkerhet**

SEAS

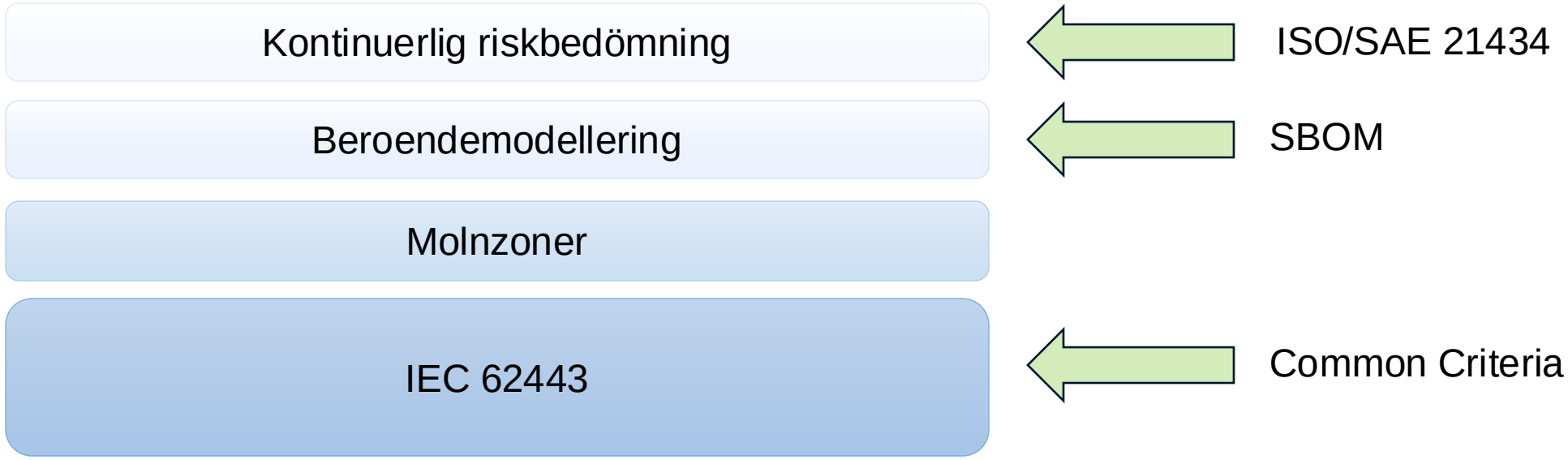
Sustainable Energy Adaptive Security

Resultat från projektet

- Utvecklade och demonstrerade use-cases för energy clouds
- Nya metoder för hotanalys och riskhantering för dessa system
- Riktlinjer för cybersäkerhet i energy clouds


Public cloud
Private/hybrid cloud
User Equipment
User Equipment
Large-scale energy generation system (layer 1)
SCADA services
Real-time control
RT
RT
RT
RT
Small-scale energy systems (layer 4 both generation and consumption)
Power grid (layer 2 and 3)

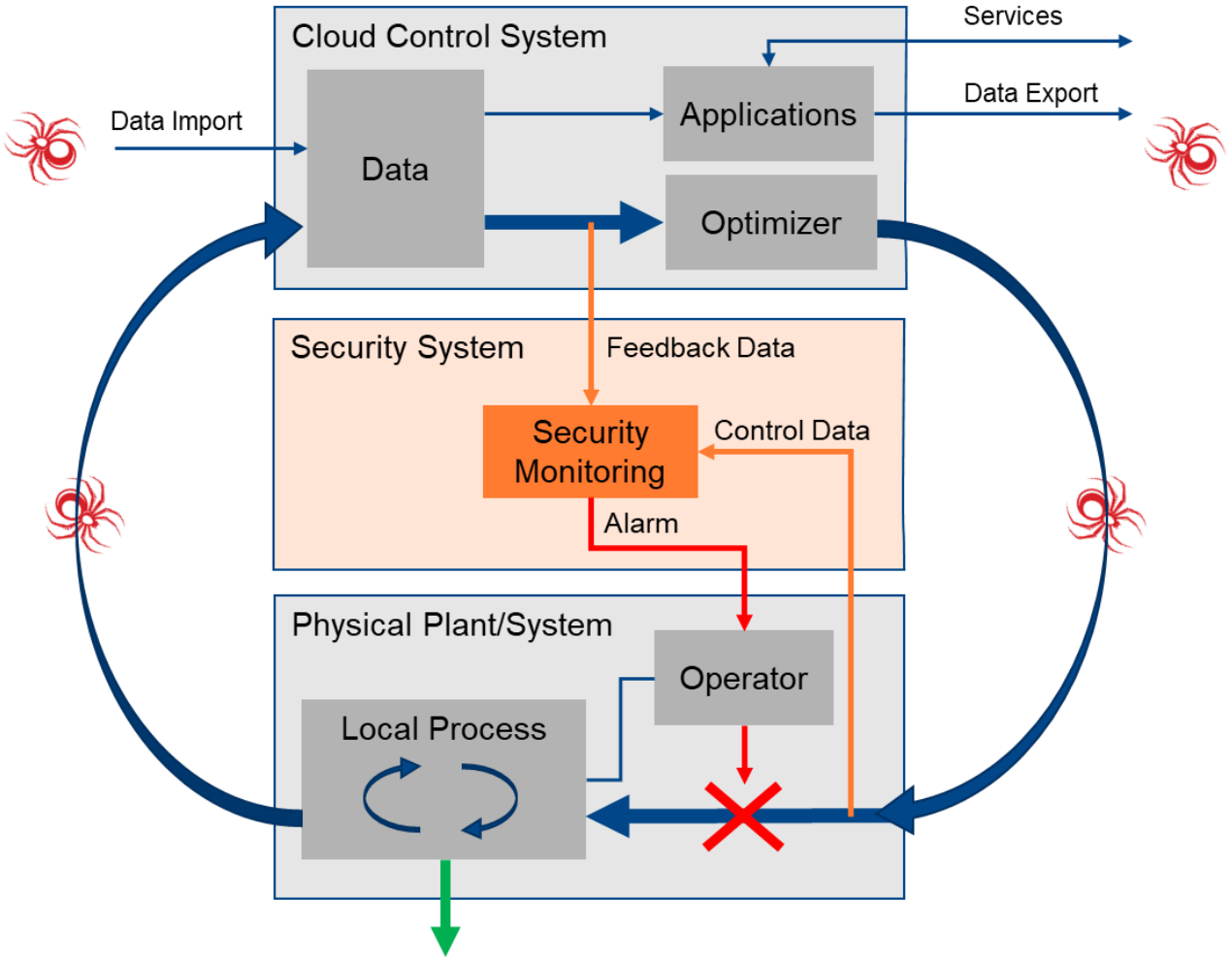
SEAS riskmetod - sammanfattning



Modell för säkerhetsövervakning av:

Molnbaserade styr & kontrollsystem

- Övervaka kontroll-loopar
  - Feedbackdata
  - Styrdata
- Inför felsäkert tillstånd
  - Liknar ödrift
- För mer information kring säkerhet och risker
  - Se rapporten från projektet



Lärdomar

- Molntjänster starkt ökande inom energisektorn
- Nya risker i molnbaserade styr & kontrollsystem
  - Robusthet mot cyberattacker - en central faktor
  - Krävs mer förståelse för olika attackmodeller
- Riskhanteringsmetoder från relaterade teknikområden anpassningsbara
  - Kombination av metoder från IEC 62443 och ISO/SAE 21434 fungerar med viss anpassning
  - Behov av automatiserade verktyg
- Samarbeten med många parter kräver en kontinuerlig närhet i frågorna
  - Tydliga modeller (inkl. säkerhetsfrågor) för samarbete saknas

Projekt

CyREC (Cybersecurity for Resilient Energy Communities of the Future)

Pierre Kleberger

CyREC

Cybersecurity for Resilient Energy Communities of the Future

Cybersäkerhet för framtidens resilienta energigemenskaper

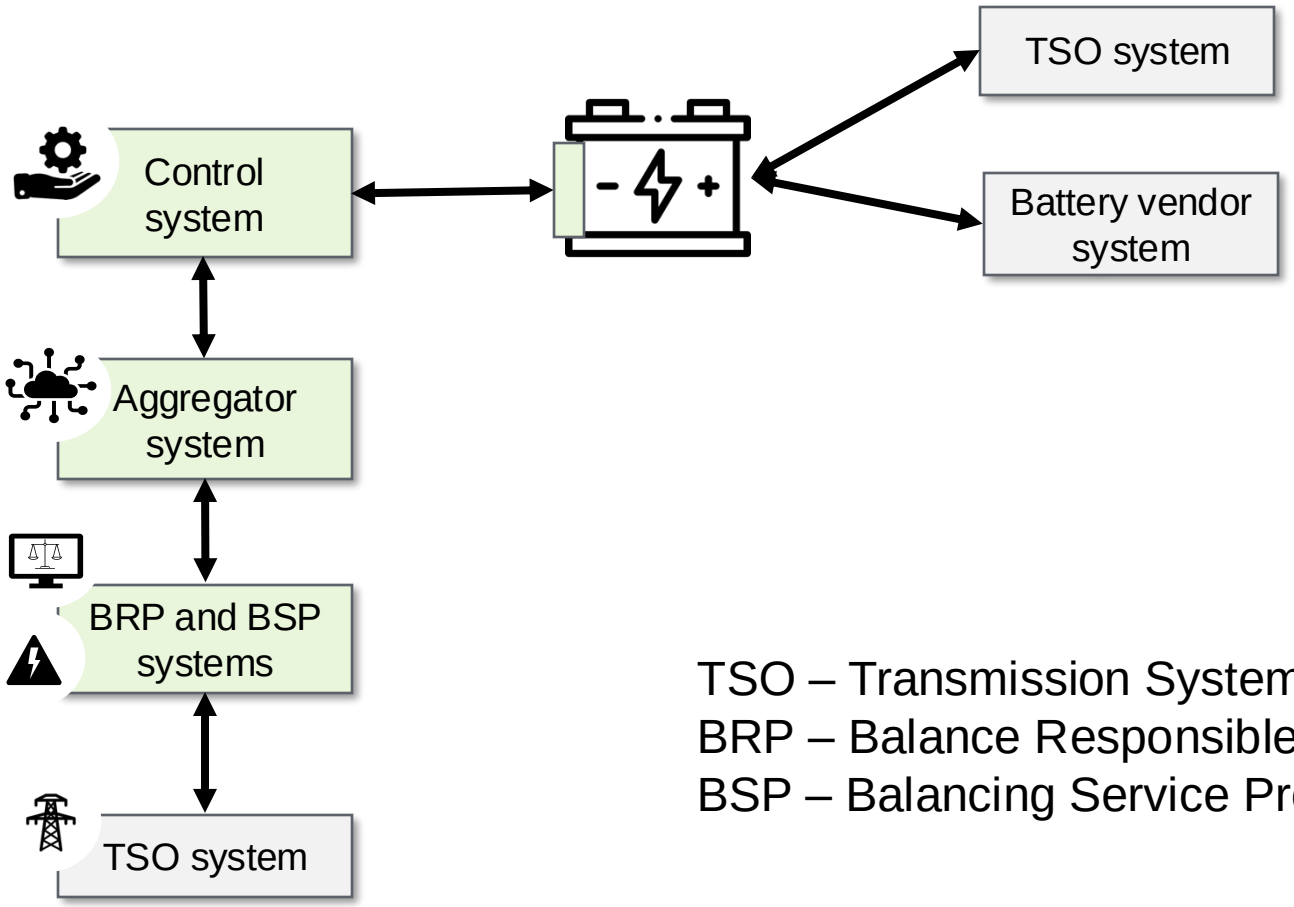
LINKÖPINGS UNIVERSITET RI.SE UKEAB SECTRA EMULATE

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

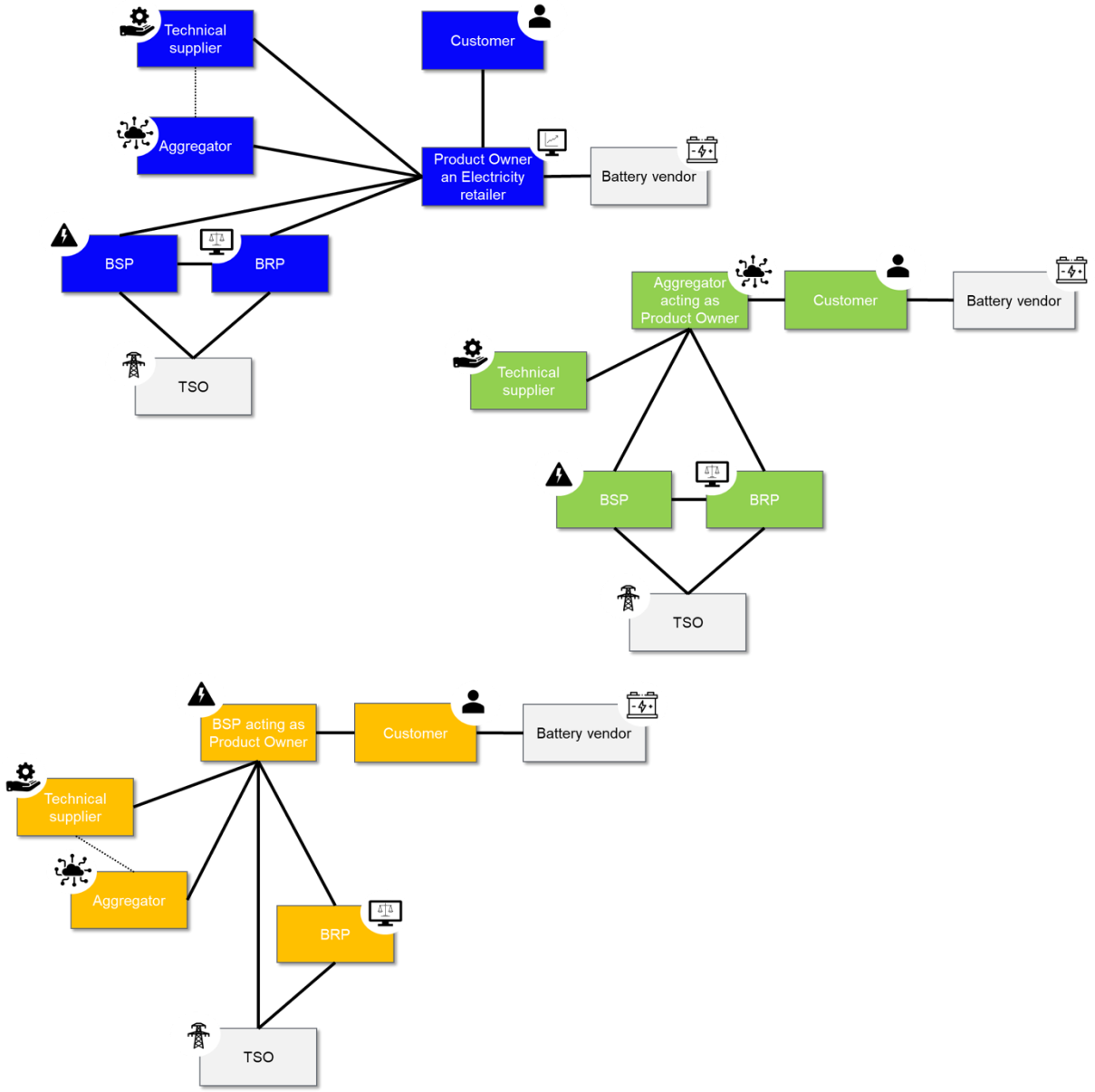
- Vad är möjliggörare och hinder för nya teknologier kopplat till energigemenskaper?
- Hur kan vi modellera effektiva samarbeten kring säkerhet i en miljö med många aktörer?
- Hur kan vi kombinera nya digitala plattformar med kritisk infrastruktur?
- Hur anpassar vi metoder för hot- och riskanalys?
-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


Mingel

Projekt

BizGuardian Connect: Privacy-Preserving Data Aggregation for Government and Business

Alejandro Russo

BizGuardian Connect

Privacy-Preserving Data Aggregations for Government and Business

Alejandro Russo

CEO / Co-founder DPella AB

3.1. Datadelning – en av de största utmaningarna

En viktig erfarenhet är att det ofta är liknande rättsliga frågor som uppstår bland innovationsaktörer, oavsett om verksamheterna är stora eller små, unga eller gamla i branschen. Mycket av diskussionerna har kretsat kring integritets- och dataskyddsfrågor som uppstår när verksamheter på olika sätt delar data med varandra i innovationssyfte. Datadelning är utan konkurrens den fråga som oftast kommit upp i kartläggningen och det som uppfattas medföra flest legala utmaningar för innovationsaktörerna.

Data sharing is, without competition, the issue that most often came up in the survey and the one that is perceived to entail the most legal challenges for the innovation actors.

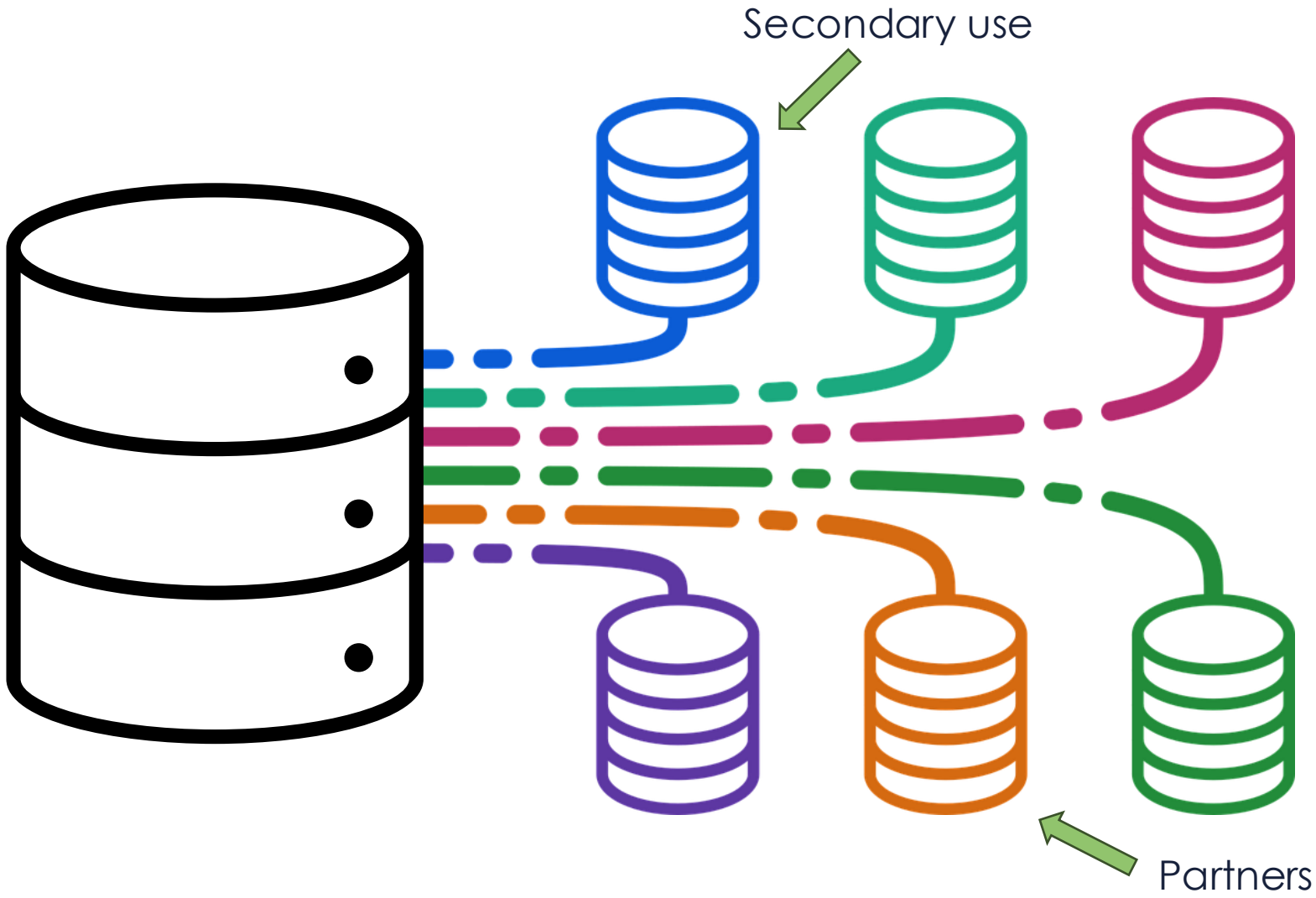

DATA
SHARING

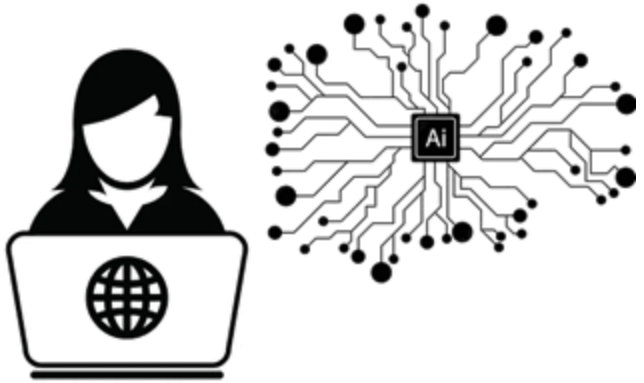
+


Privacy

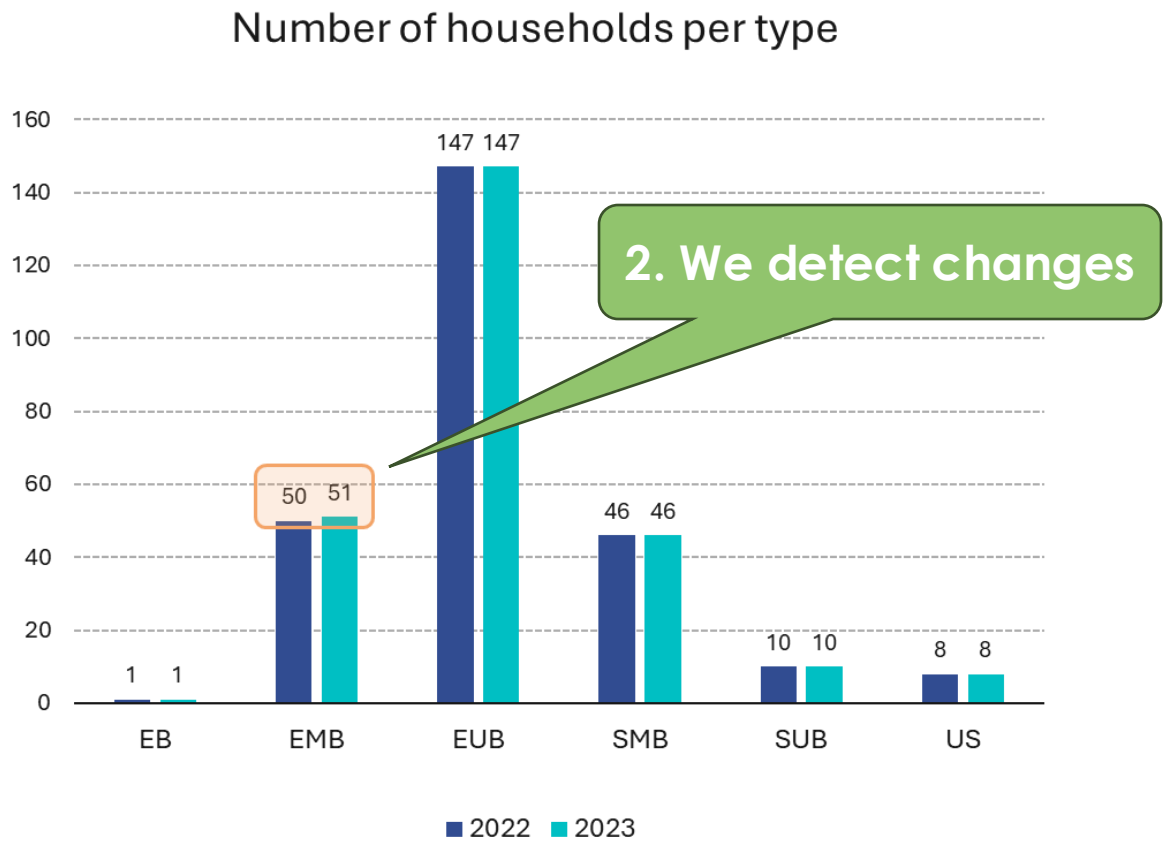
=


OPEN
DATA

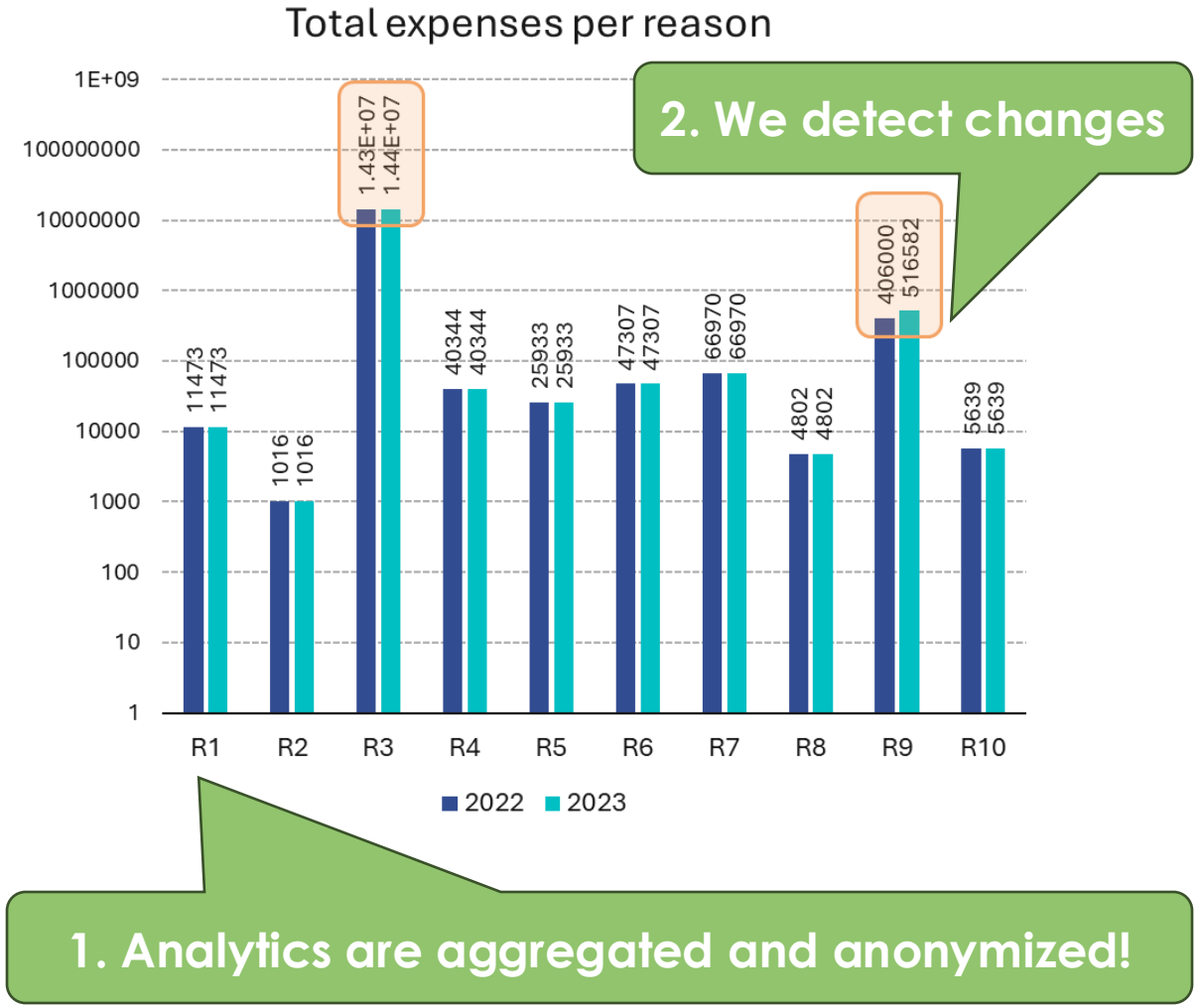

Secondary use
Partners



Lay user + ChatGPT



Classification	Description
EB	Enbart barn
EMB	Ensamstående med barn
EUB	Ensamstående utan barn
SMB	Sammanboende med barn
SUB	Sammanboende utan barn
US	Uppgift saknas



3. Can ChatGPT explain the nature of such a change in R9 using <u>additional data</u>?

Prompt for ChatGPT:

A municipality is interested in releasing yearly statistics about the population, concretely they release:

1. **Histogram of households per household type**
2. **Total expenses per reason of support**

Describe the analytics

Insight #1: From 2022 to 2023 a new household has been included in the dataset. This household corresponds to a single parent with children (EMB, Ensamstående med barn).

Insight #2: From 2022 to 2023, there has been **an increase of 39,313 kr attributed to reason R3 and 110,582 kr attributed to reason R9**. Since only one additional household has been added during this period, these increased expenses can reasonably be attributed to the new household. R3 and R9 are anonymized reasons.

Describe the changes

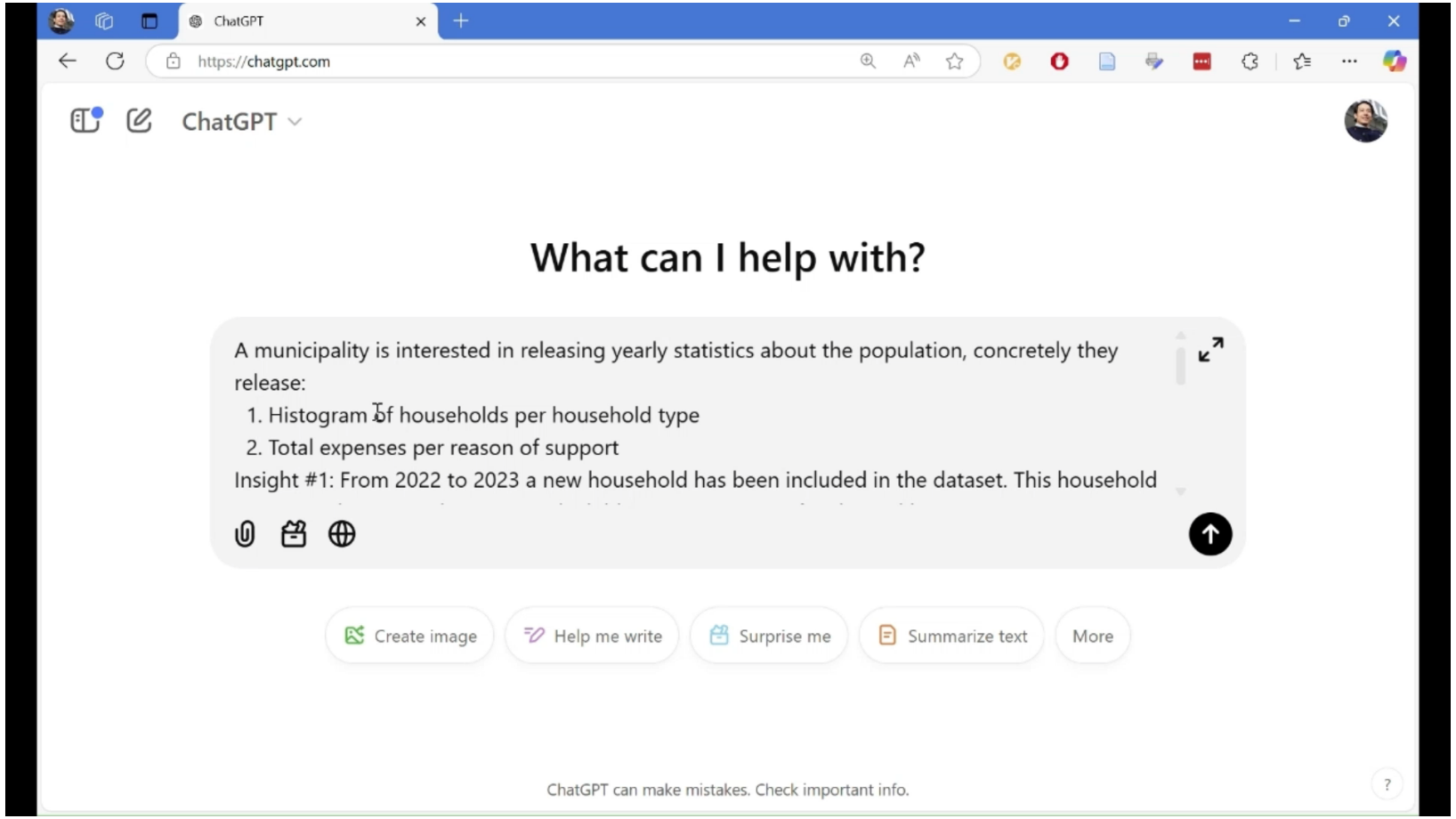
I want to use external data from Sweden to de-identify Reason R9. Sweden is an especially transparent country, so the amounts involved are public and prominently published. In this scenario, the key data is from **Forsäkringskassan** describing the establishment (etableringsersättning) program and the amounts a person in the program can receive: **https://www.forsakringskassan.se/privatperson/arbetssokande/ersattning-for-dig-som-deltar-i-etableringsprogrammet-hos-arbetsformedlingen**

Provide additional information

Based on that online information, what kind of support is the amount of 110,582 kr given in one year and the additional information found in the URL provided above? **Can you figure out what is the reason R9 more likely to correspond?**

Ask to de-anonymize

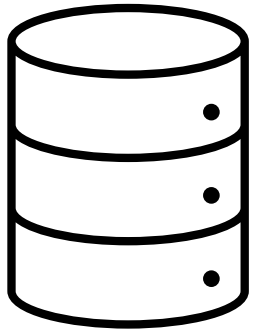
ChatGPT in action!

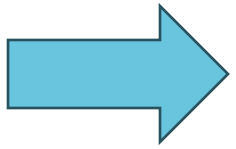


Differential Privacy Technology

- **Quantify privacy protection**
- **Robust against future (i) AI models and (ii) additional information**
- **Science-based (math) guarantees**

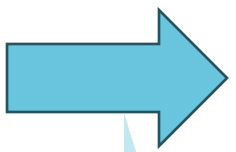
Business-level data



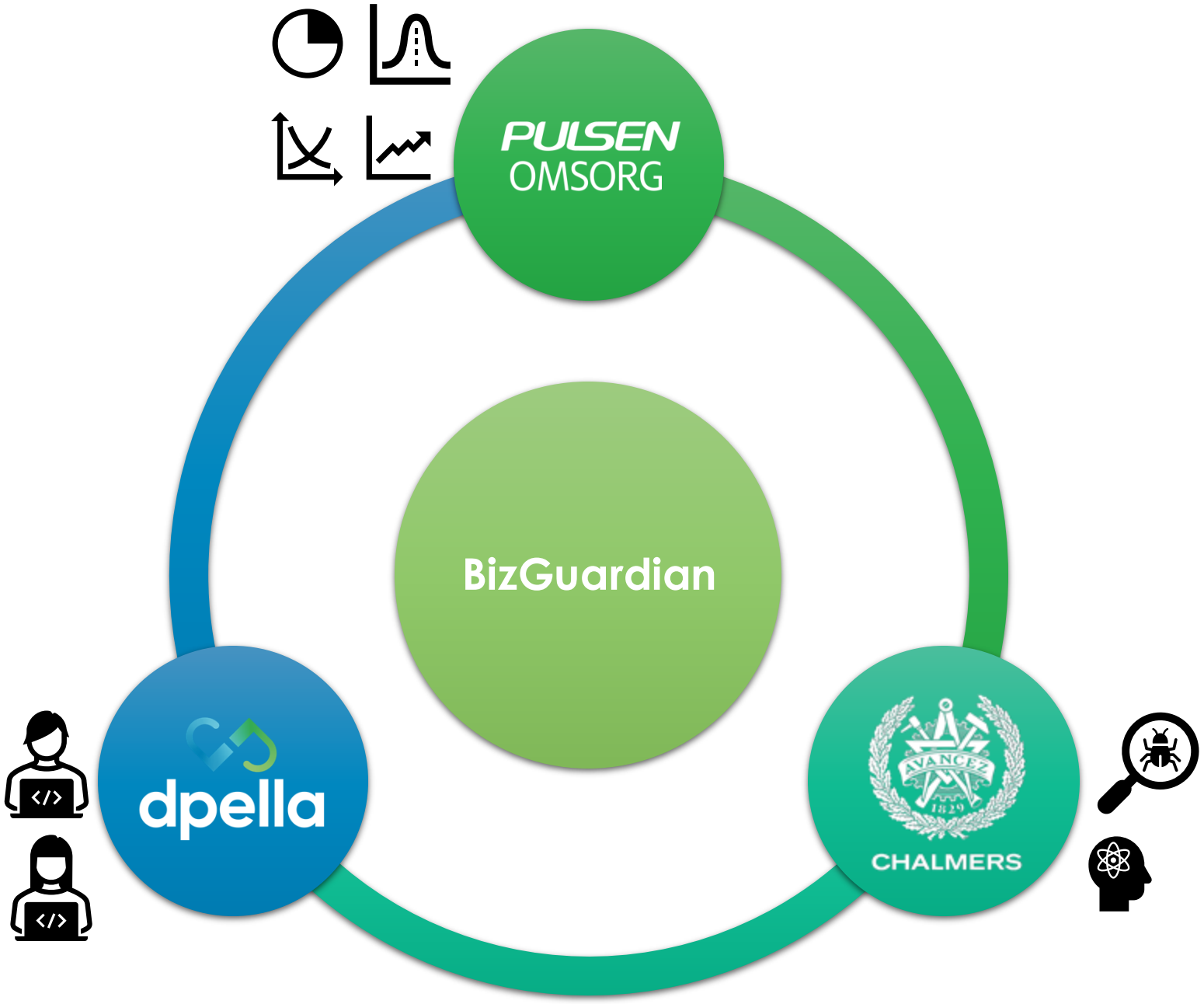


dpella

unleash the power of analytics



Injection of **calibrated** random noise to the result of the analytics


PULSEN
OMSORG
BizGuardian
dpella
CHALMERS

The project WPs

- WP1: Design of a Standardized Differential Privacy Service API
- WP2: Accuracy for Data-Dependent Analytics
- WP3: Strongly Typed SQL-like Language for Queries
- WP4: Integration with Pulsen Omsorg Environment
- WP5: Demonstration of Public Sector Case Studies

- Two bachelor thesis with **Chalmers University**
- Open source releases
  - WebDP
  - FrontDP

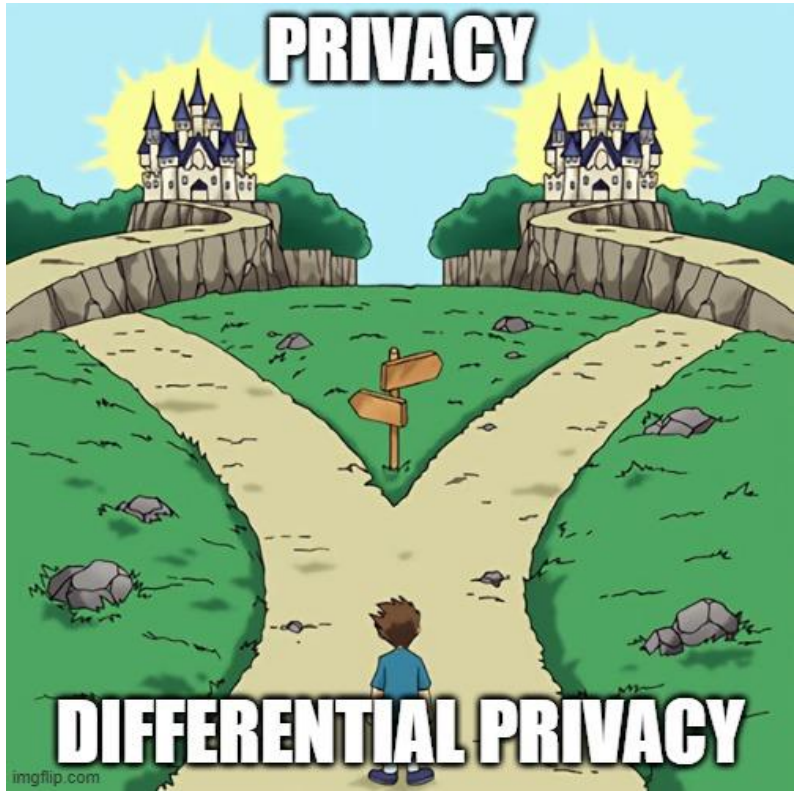
- Patent application PCT/SE2024/050923
- Scientific article under review

- Validation of DP
- Awareness of risks
- AI de-anonymization

85% Completed

Project facts

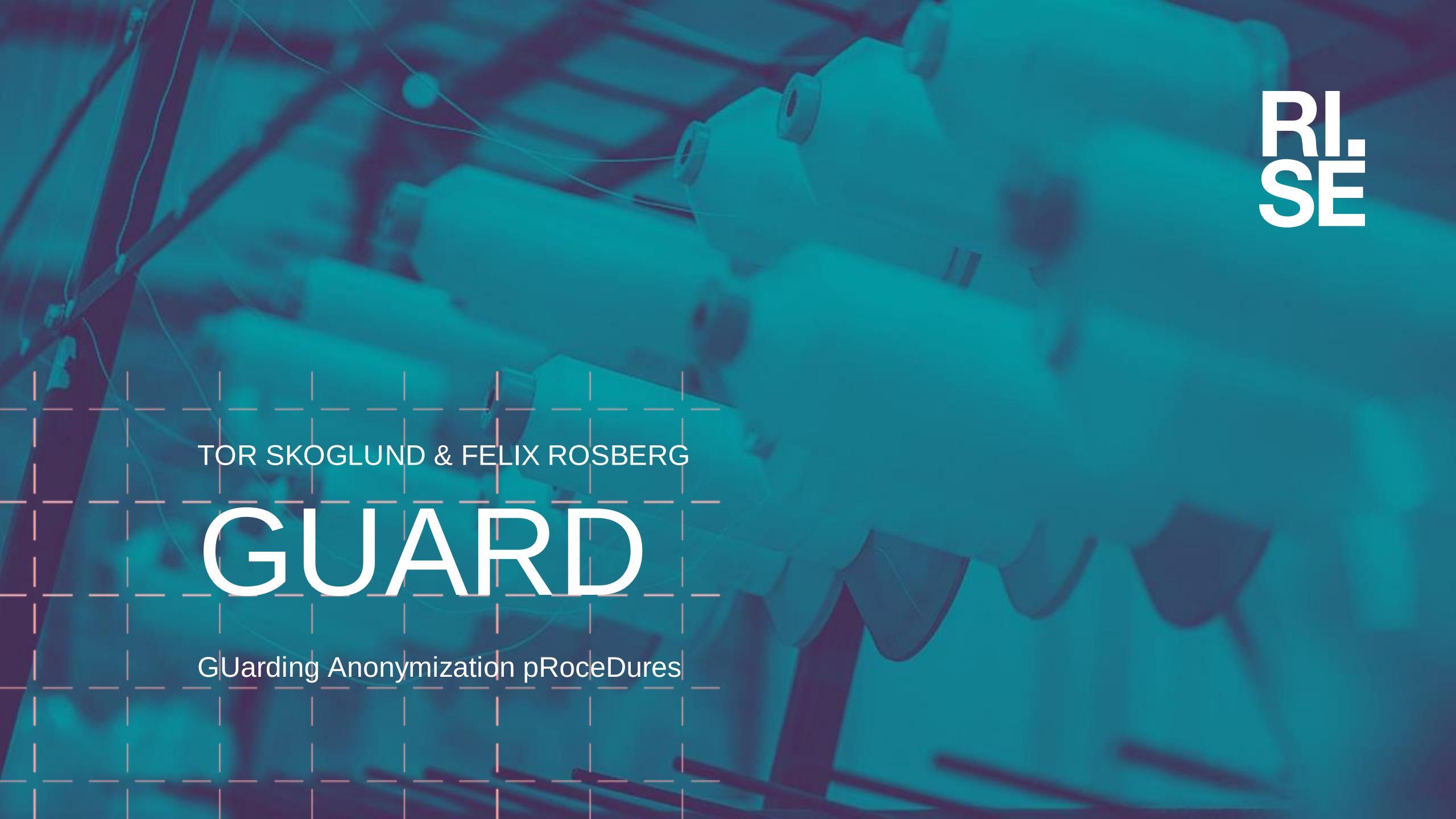
- Project name: BizGuardian Connect: Privacy-Preserving Data Aggregation for Government & Business
- Project Coordinator: DPella AB
- Presenter: Alejandro Russo, CEO of DPella AB (alejandro@dpella.io)
- Project Manager: Carola Compa (DPella AB) (carola@dpella.io)
- Participants: Chalmers University, Pulsen Omsorg AB, DPella AB
- Duration: 2023/11/15 – 2025/03/31



Projekt

Anonymization Defense – GUARD

Tor Skoglund



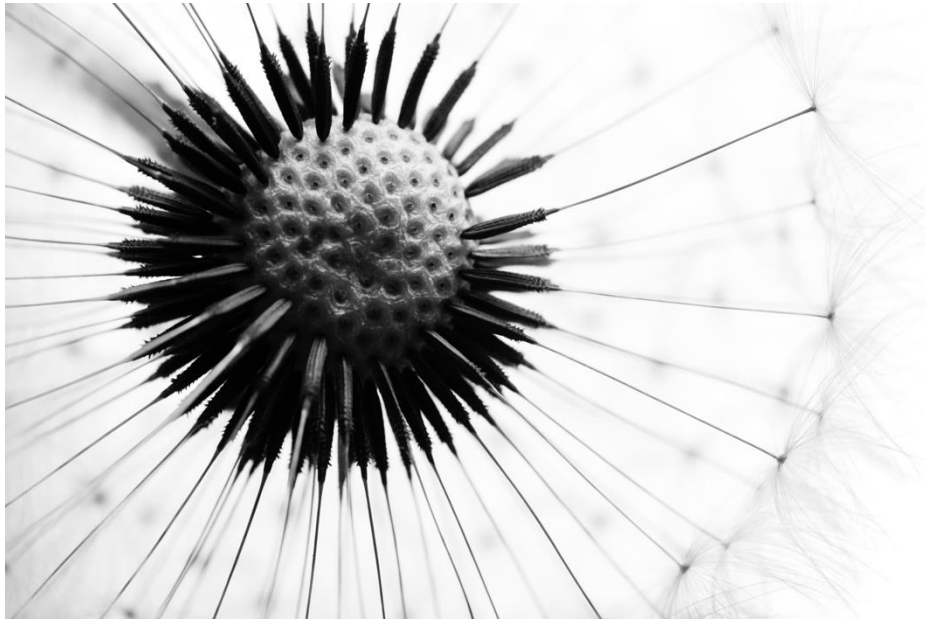
TOR SKOGLUND & FELIX ROSBERG

GUARD

GUarding Anonymization pRoceDures

Basics

- 2 years duration
- Started a year ago
- Budget 7.5 MSEK



Avancerad Digitalisering

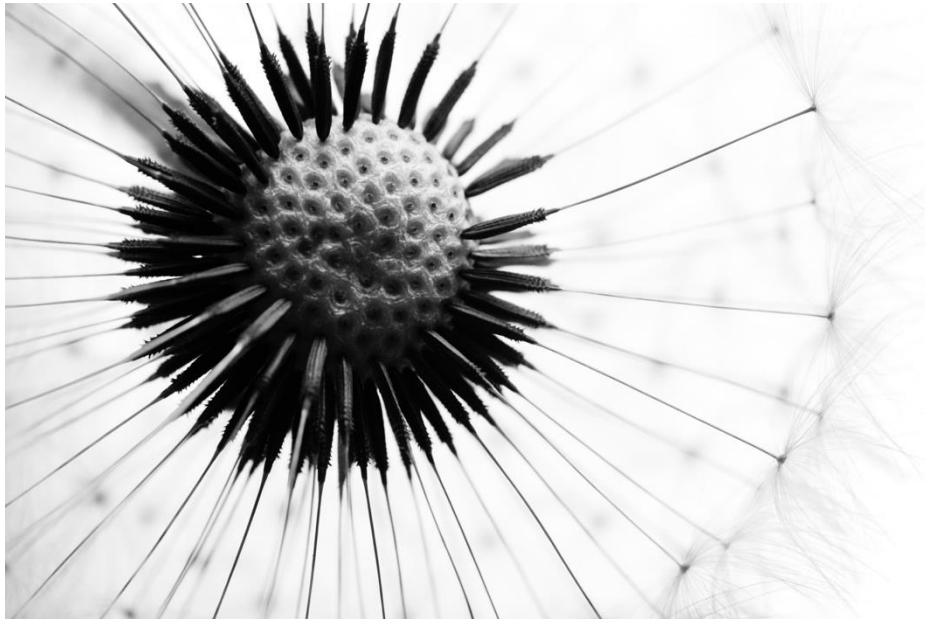
ABB ERICSSON SAAB Teknikföretagen VINNOVA

The work is performed with financing from VINNOVA within the program of Advanced Digitalization

RI. SE

Project partners

- RISE (Coordinator)
- Engage Studios
- Högskolan i Halmstad



Avancerad Digitalisering

ABB ERICSSON SAAB Teknikföretagen VINNOVA

The work is performed with financing from VINNOVA within the program of Advanced Digitalization

RI. SE

Introduction

- Increasing demand for data collection causes friction with regulations such as GDPR

Introduction

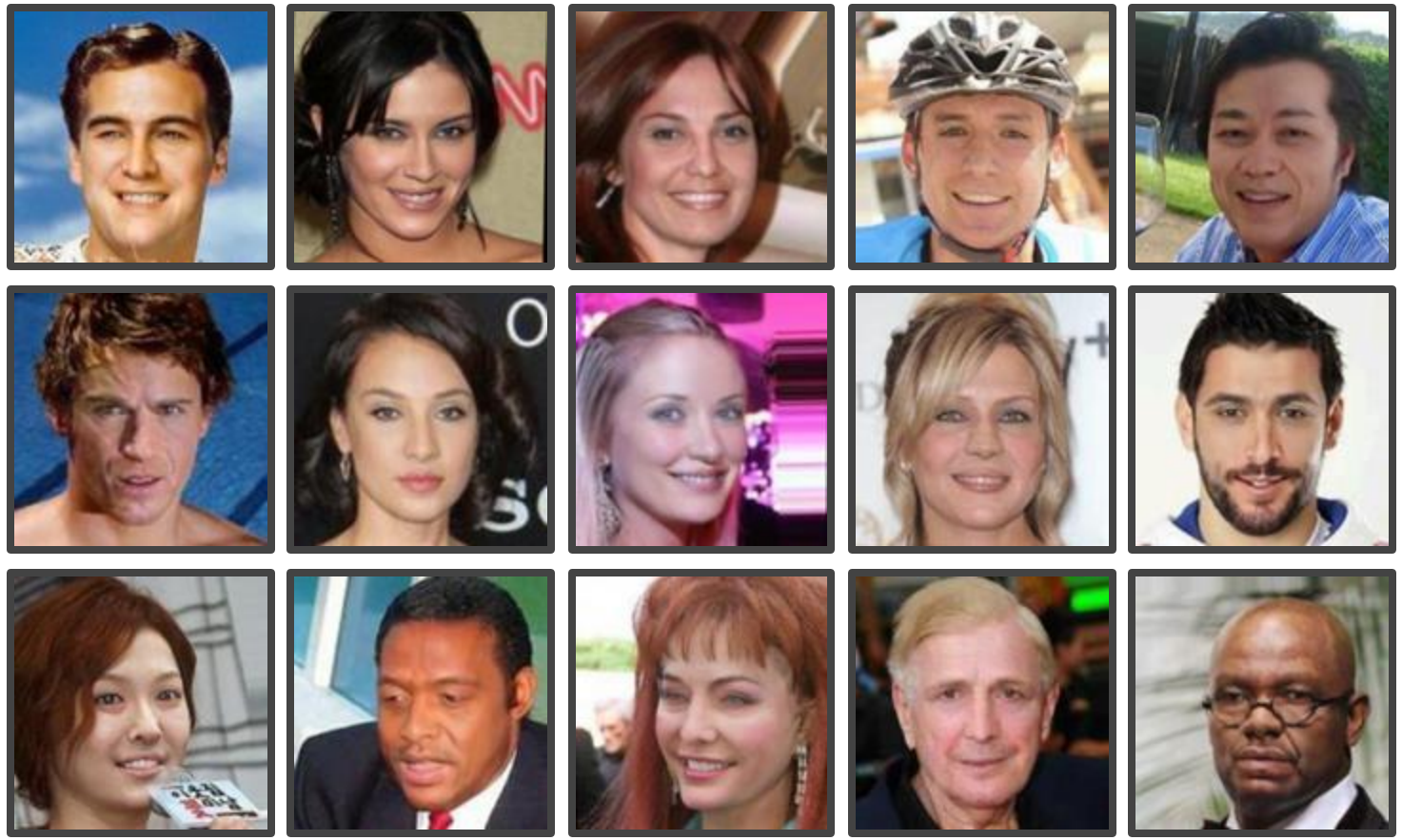
- Increasing demand for data collection causes friction with regulations such as GDPR
- Current anonymization algorithms remove to much valuable information
- There is a need to keep more of the non-identifying information in the data

RI.
SE

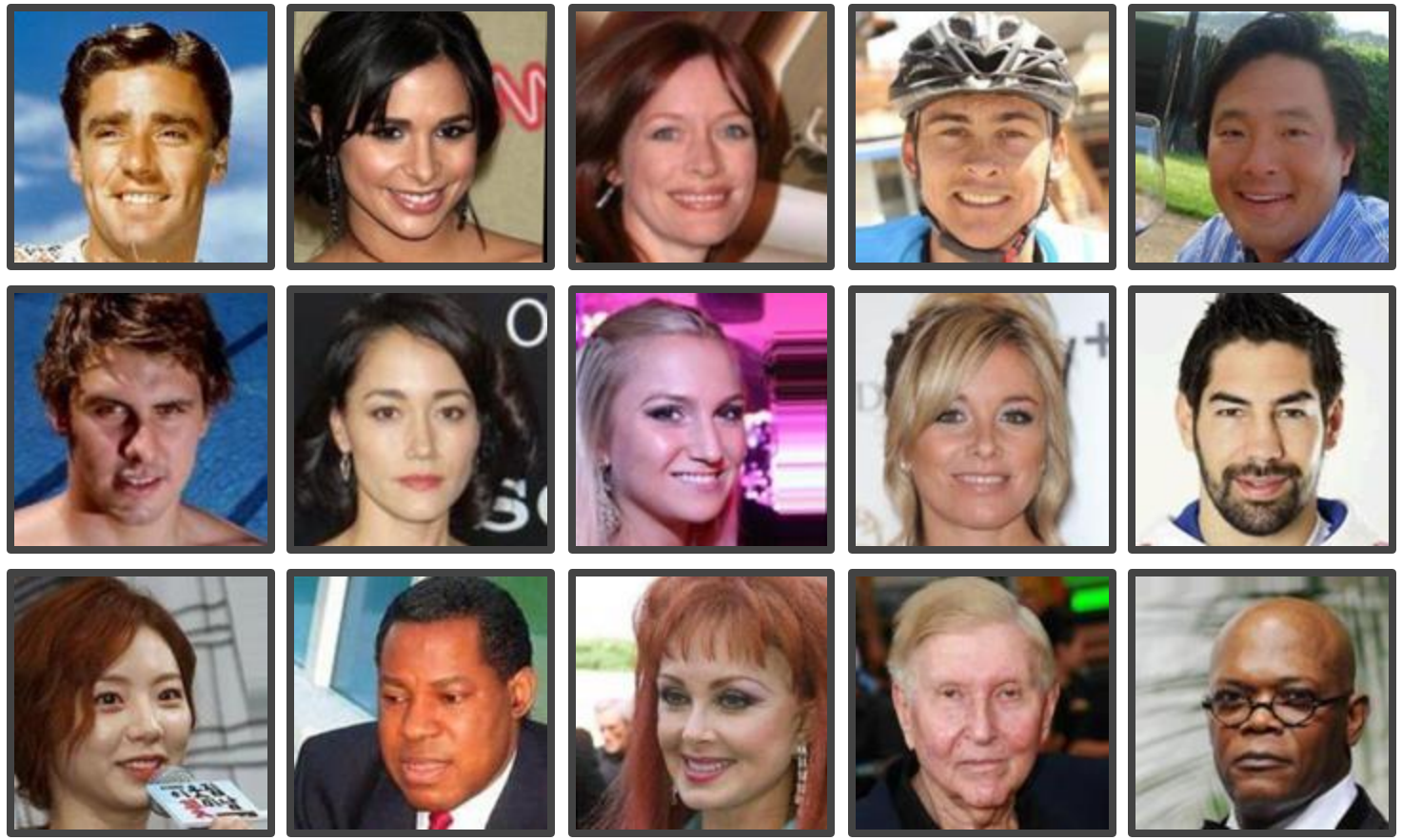
Challenges

- Reconstruction attacks.
- Adversarial attacks.
- Vulnerabilities in the detection stage.
- Unknown unknowns.
- Explainability.

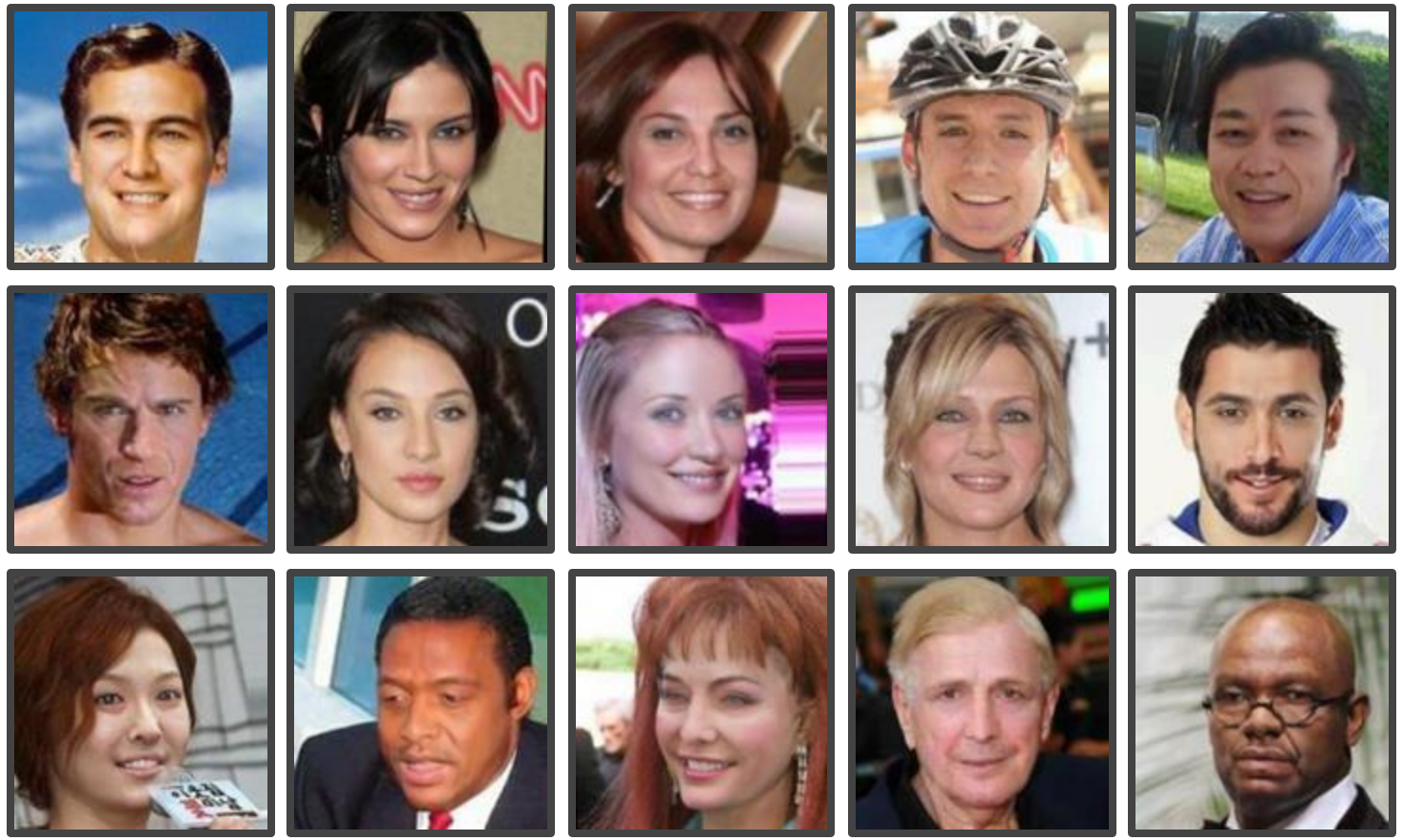
Challenges



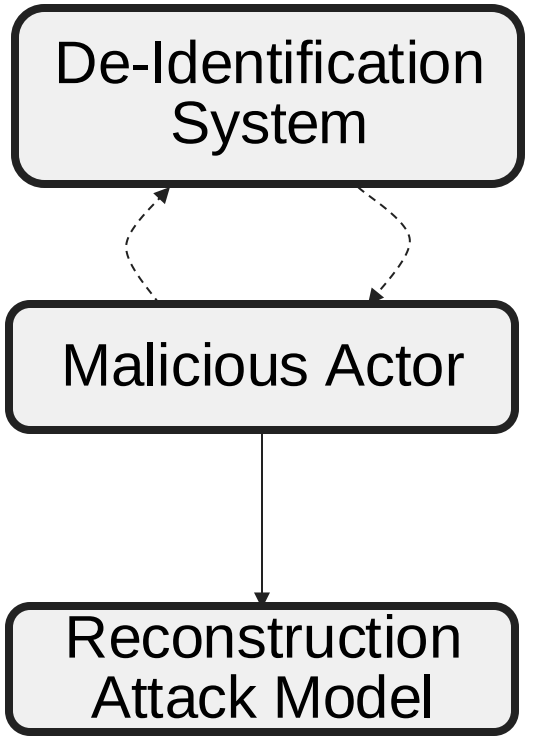
Challenges



Challenges

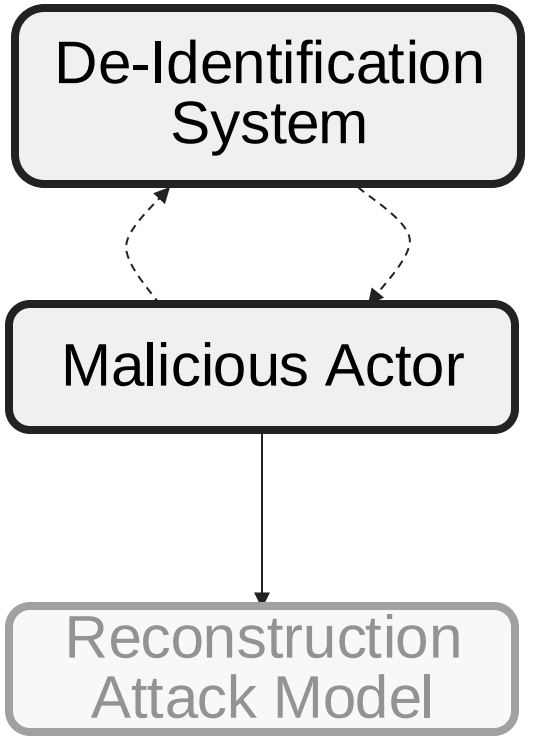


Challenges



RI. SE

The solution



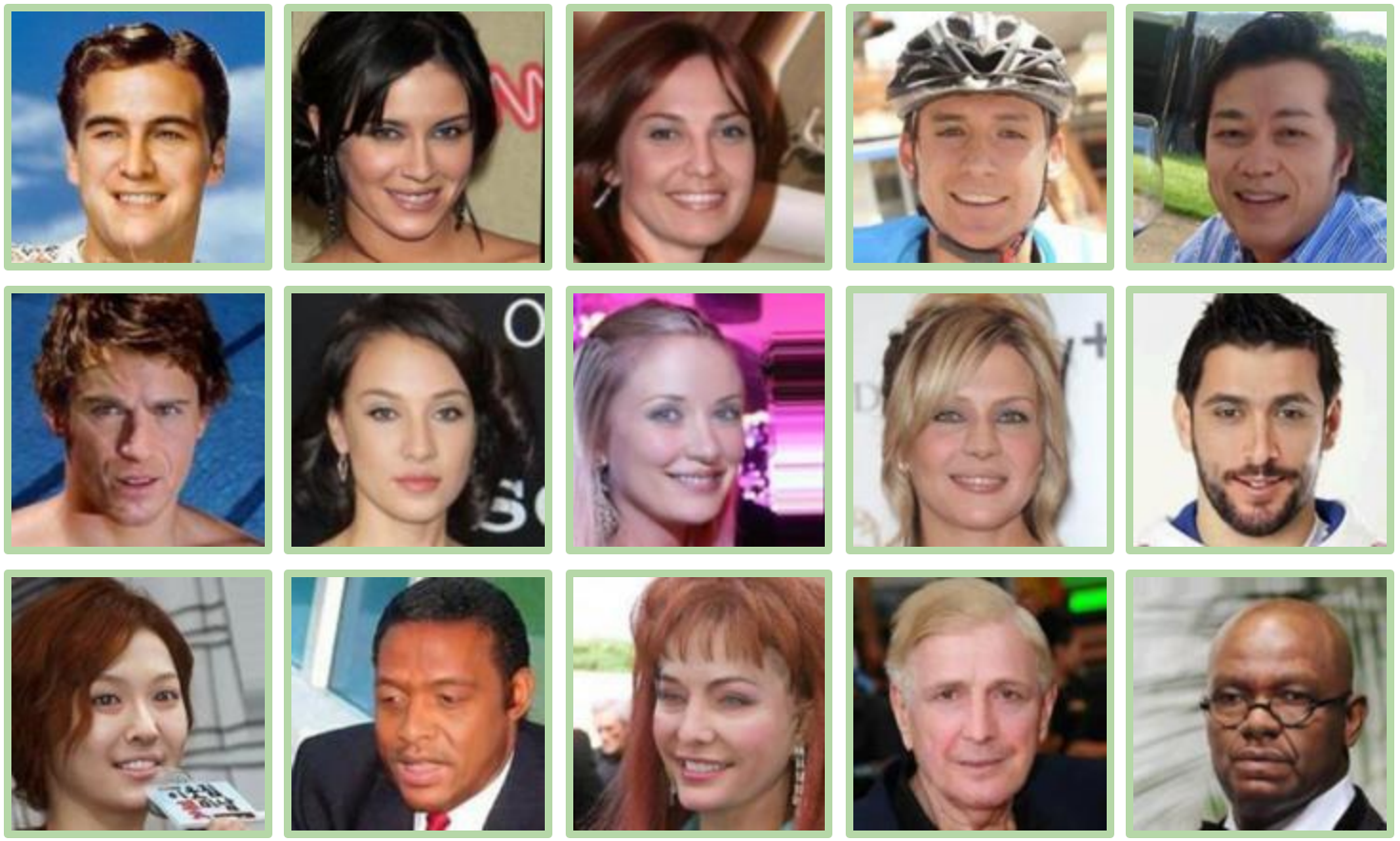
RI. SE

The solution

Corrupts data characteristics!

RI.
SE

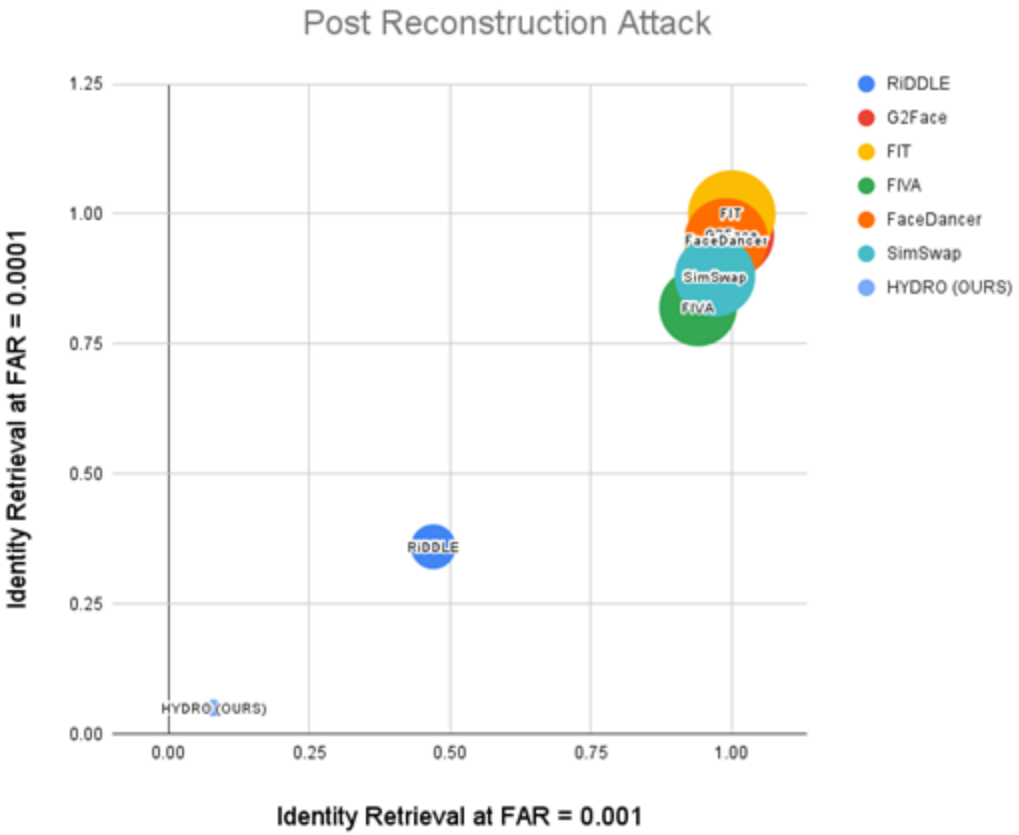
The solution



Diffusion-based recovery of the data distribution.

RI.
SE

The solution



Aggregated results from five facial recognition models / biometric system

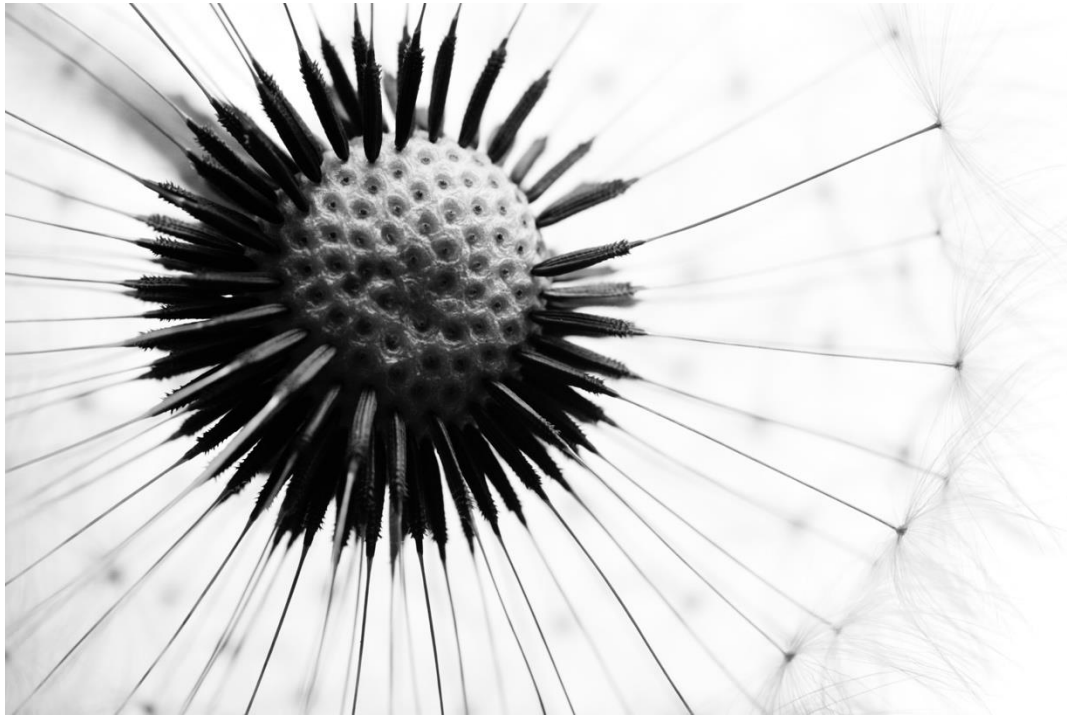
RI.
SE

Improvements to the system

- Diffusion-based generative modeling-defense makes the de-identification non-reversible.
- Diffusion defense also improves attribute retention and visual quality.
- Improved training methods for better gaze retention.
- Adversarial attack prevention has been identified.
- Explainable automatic detection of malicious data.

Conclusion

- GUARD investigates cyber-security issues for face de-identification.
- Reconstruction attacks works on a wide range of state-of-the-art de-identification methods.
- Reconstruction attacks are preventable without drawbacks



Tor Skoglund

RISE

tor.skoglund@ri.se

Felix Rosberg

Engage Studios

felix.rosberg@engagestudios.com

Projekt

AI-baserad cybersäkerhet för CAN och IP kommunikation i befintlig fordonsmiljö

Tobias Bertilsson

AI-based Cybersecurity for CAN and IP Communication in Existing Vehicle Environment

January 23, 2025

AI-based Cybersecurity for CAN and IP Communication in Existing Vehicle Environment

Cybersäkerhet för avancerad industriell digitalisering

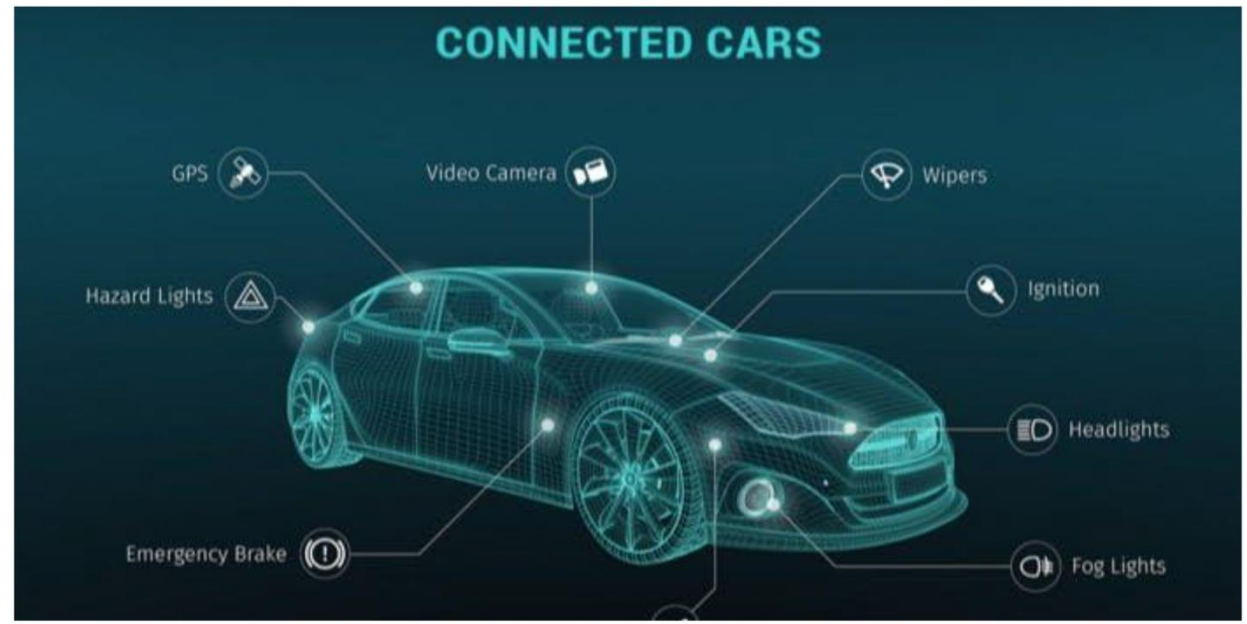
May 2021 – Jan 2023

Omen Technologies

Project Motivation

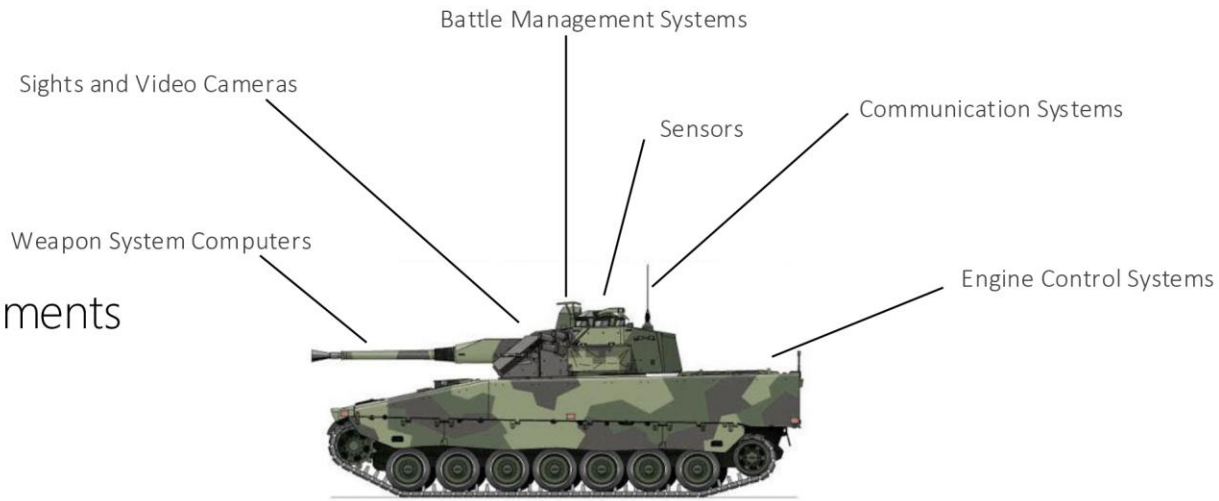
Vehicles are becoming increasingly digital and connected, which also makes them more vulnerable to cyberattacks.

In a future where more and more vehicles become autonomous, cyberattacks could have even greater consequences.



Project Goal

- Test AI monitoring on a specific vehicle type (Technology is applicable to any vehicle type)
- Demonstrate AI capabilities for detecting misbehaving communication in IP and CAN environments
- Efficiently deploy AI-based monitoring in vehicle environments



AI-based Communication Behavior Monitoring

- Define relevant subsystems
- Tap into data streams
- Train AI models
- Verify models using simulated attacks on CAN & IP
  - Digital twin
  - Vehicle environment

Project Results

- Project goals successfully achieved
- AI models were trained & validated for detecting simulated attacks on CAN & IP
- Deployed AI models on local hardware inside the vehicle platform
- Identified roadmap for future developments regarding features & requirements
  - Local model training
  - Improve model configuration
  - Improve runtime environments constraints

How Did Clavister Use the Results?

- **Improvements of the AI algorithm**
  - Improved core routines for model adaptation
  - Optimized for low resources in terms of Memory and CPU utilization
  - On-device training & embedded hardware support
- **AI technology released to the market**
  - Packaged as a C programming library
    - Offered to partners for integration in partner products & solutions
  - Integrated in Clavister NetWall firewall software 15.00.00, powering AI policies for IP network communication behavior monitoring.
- **Continued Research**
  - **MAGIC** (Vinnova) – Application of AI technology for IDS capabilities in vehicle platforms
  - CISSAN (Vinnova) – Application of AI technology for cyber protection and operational monitoring of electrical power grids.
  - COMMANDS (EDF) – Application of AI technology for cyber protection of autonomous and remote-controlled vehicles


clavister
Thank you!
Tobias.bertilsson@clavister.com
SECURITY BY
SWEDEN

Tack!

Nu dags för fika, utställning
och gemensamt pass.