
# EECS Research & Impact Day 2025

# Outlook on Research and Science with Digital Futures

Director General Katarina Bjelke, Swedish Research Council
Monica Billger, Professor and Director of InfraVis
Hanifeh Khayyeri, Vice President of Computer Science
Björn Ottersten, Profesor KTH and Univesity of Luxemburg
Karl Henrik Johansson, Professor and Director of Digital Futures
Mikael Östling, Professor and past Deputy President KTH

# Director General Katarina Bjelke, Swedish Research Council

Vetenskapsrådet
Swedish Research Council

# The Swedish Research council

Perspectives on Digital Futures for Swedish research
@EECS Research Impact Day 2025

**Katarina Bjelke**
Director General

# The role of the Swedish Research Council

- We provide funding for researcher-initiated basic research
- We initiate and support strategic initiatives in research
- We work for an efficient research system
- We work to ensure that researchers gain access to advanced research infrastructure
- We analyse the conditions for research, evaluate research, and give the Government advice on future research policy
- We coordinate and develop communication about the significance, results, and conditions of research
- We promote international collaborative research

# A well-functioning digital future for Swedish research requires:

**Computing resources and AI capabilities**

*E.g. NAISS and AI Factories*

**Data from research and research infrastructures**

*E.g. MAX IV, SciLifeLab, ESS as well as coordinating infrastructures such as RUT, SND and ICOS-Carbon Portal*

**Secure and fast data transfer**

*Sunet provides fast network and trusted identification services*

**High-quality user support**

*E.g. NAISS and ENCCS provide resources to Swedish users of HPC and AI applications*

# Monica Billger, Professor and Director of InfraVis

# InfraVis

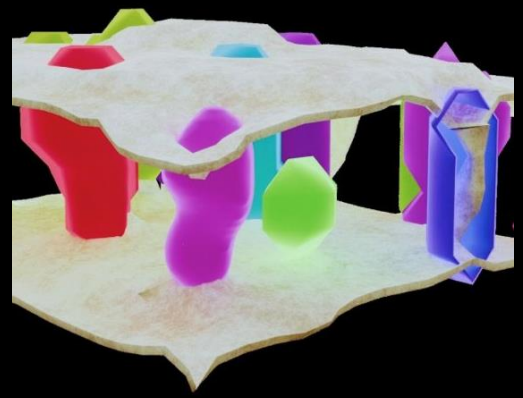
## Scientific Discovery Through Visualization Support

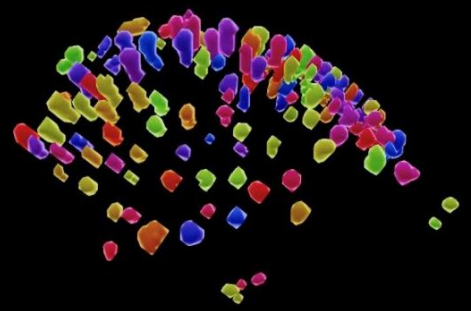
Researchers in Sweden can get help in analyzing and visualizing data – Apply at https://infravis.se

Swedish Research Council

National Research Infrastructure for Data Visualization

CHALMERS UNIVERSITY OF TECHNOLOGY · UNIVERSITY OF GOTHENBURG · KTH VETENSKAP OCH KONST · LINKÖPING UNIVERSITY · LUND UNIVERSITY · Linnaeus University · Mittuniversitetet MID SWEDEN UNIVERSITY · UMEÅ UNIVERSITY · UPPSALA UNIVERSITET



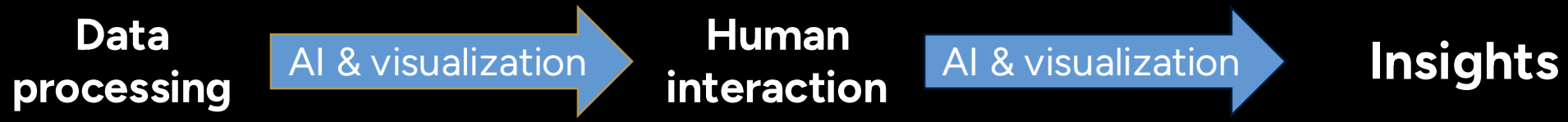


InfraVis

*"Enables scientific discovery through data analysis and visualization support"*

# Addressing Societal Challenges and Sustainability Goals

- Cross-disciplinary research creates data complexity – calls for visualization to enhance exploration and communication
- Bridging between data and  insights enabled by AI and human interplay
- Maximise scientific impact from cross-infrastructure collaborations




InfraVis

*"Transforms complexity into clarity.  Making sense of data – powering discovery"*

# Hanifeh Khayyeri, Vice President of Computer Science, RISE



**We work with groundbreaking technologies.**

**We put Research to Action.**

## Expanding Frontiers


**Advancing** industry, education, healthcare, and everyday life. From ocean depths to orbit—and straight to your fingertips.

# Space Mission Data and Plasma Physics with High Performance Computing

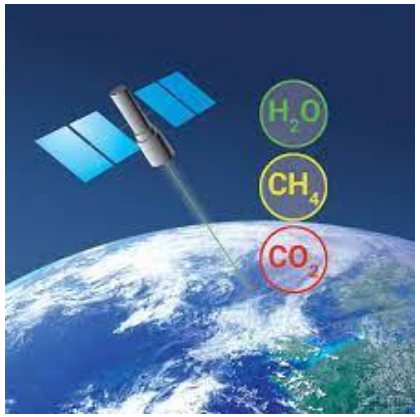
Christer Fuglesang, Professor and Director of KTH Space Center
Tomas Karlsson, Professor Space Plamsma Physics
Svetlana Ratynskaia, Professor in Plasma Physics
Stefano Markidis, Professor of High Performance Computing

# Christer Fuglesang, Professor and Director of KTH Space Center

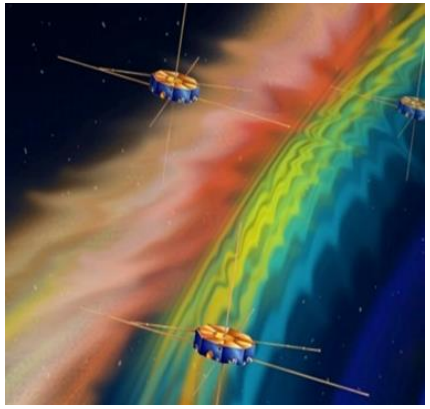
# KTH Space Center – many research activities

Astrophysics

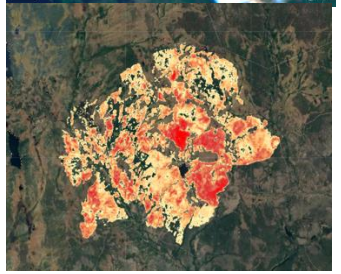
Expandable structure: CubeSat-boom



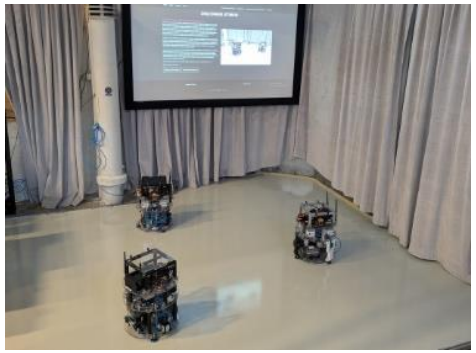

GHG measurements



EM-fields ín the magnetosphere



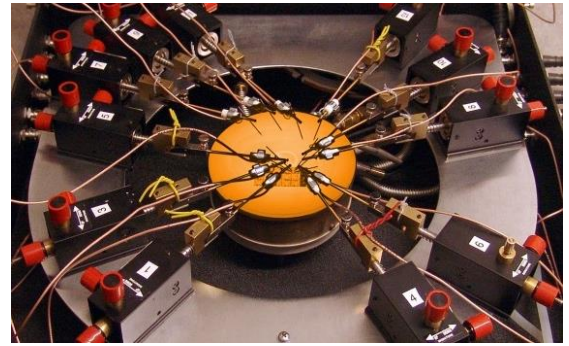
EO Big Data for Wildfire Monitoring



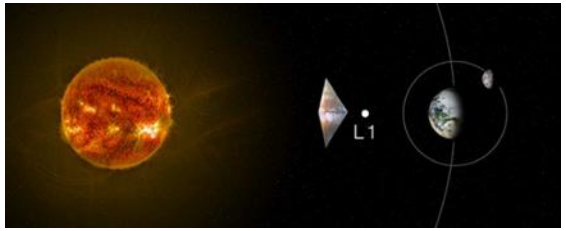
Space robots

Rocket engines


Human behaviour



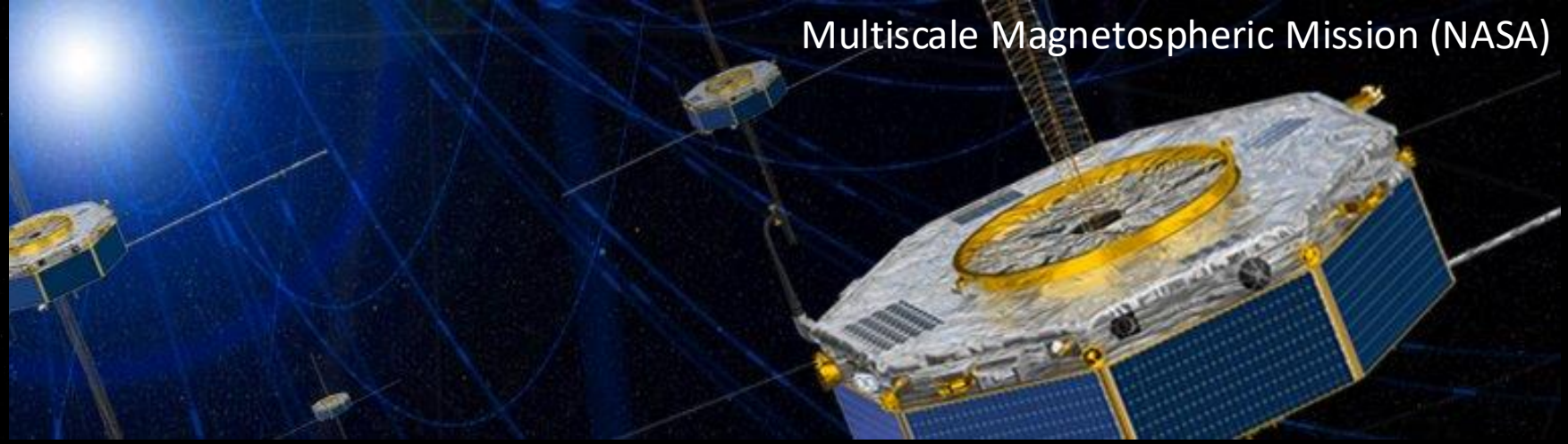
460 °C SiC technology for in-situ on Venus



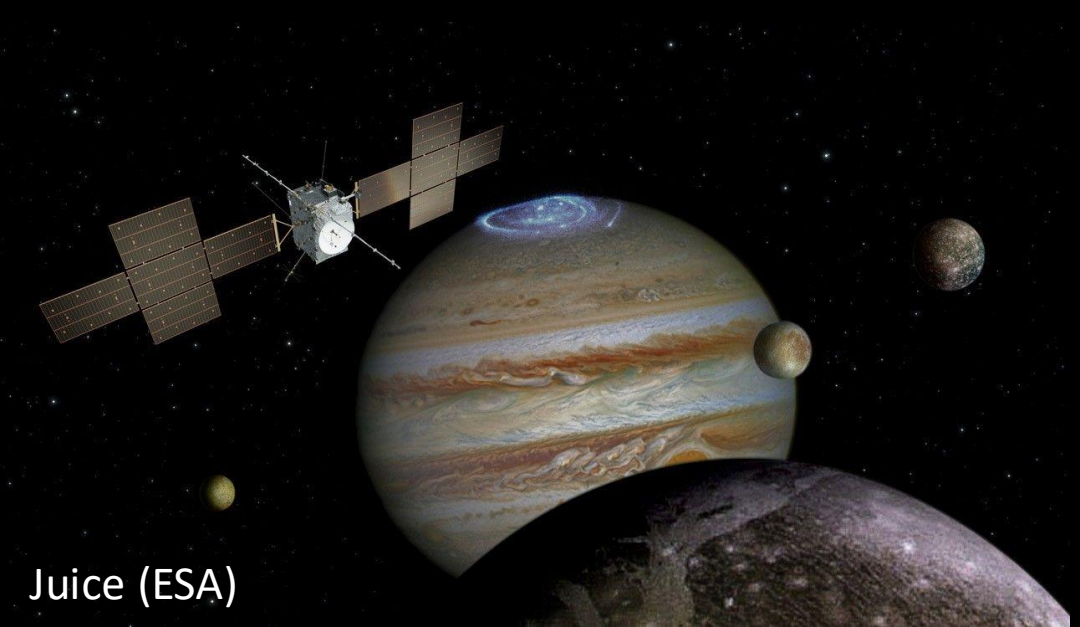

Sunshades in space moderating global temperature rise

# Tomas Karlsson, Professor Space Plasma Physics


BepiColombo (ESA - JAXA)


Multiscale Magnetospheric Mission (NASA)

# Space Missions and Measurements


Juice (ESA)

Big players:

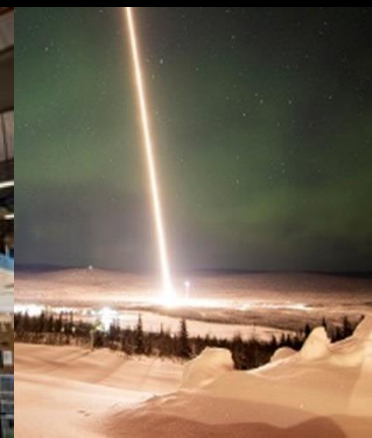
*Europa – ESA*

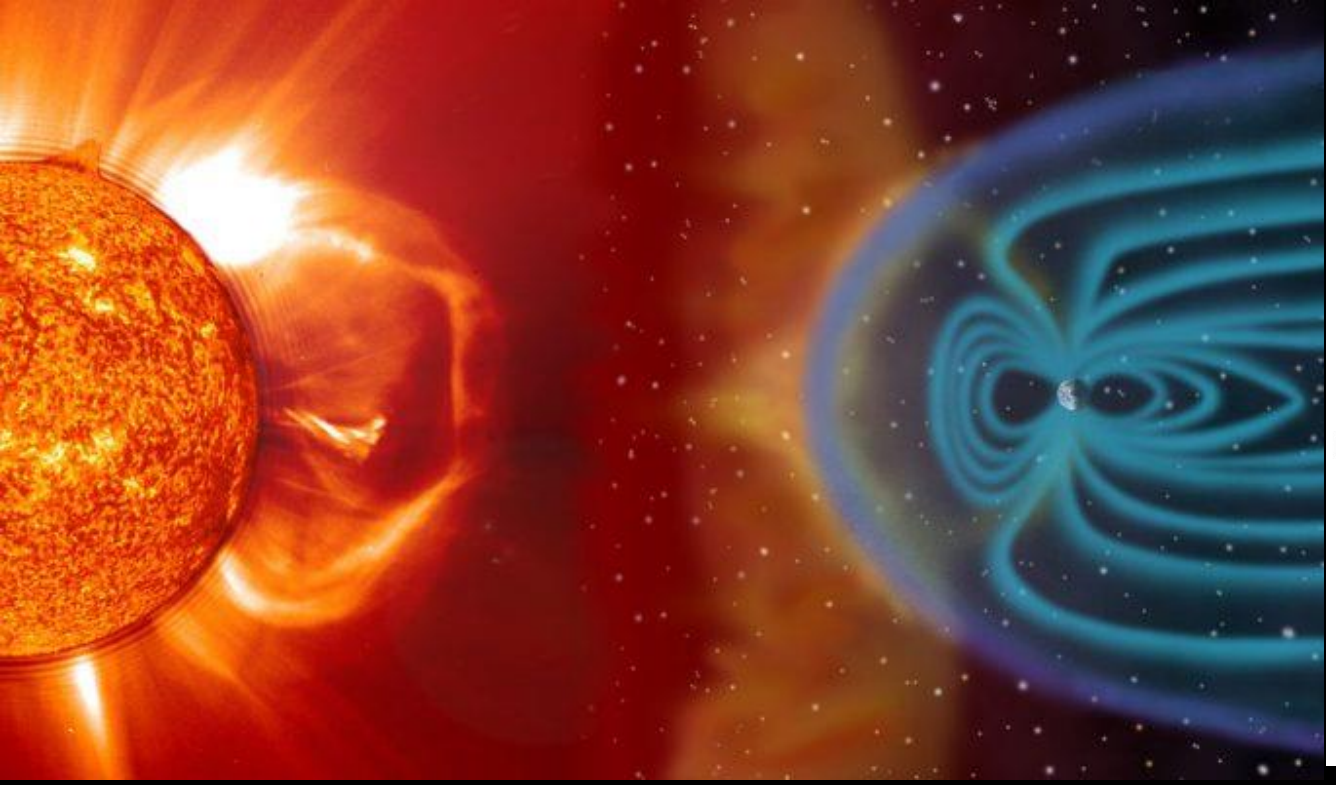
*Japan – JAXA*

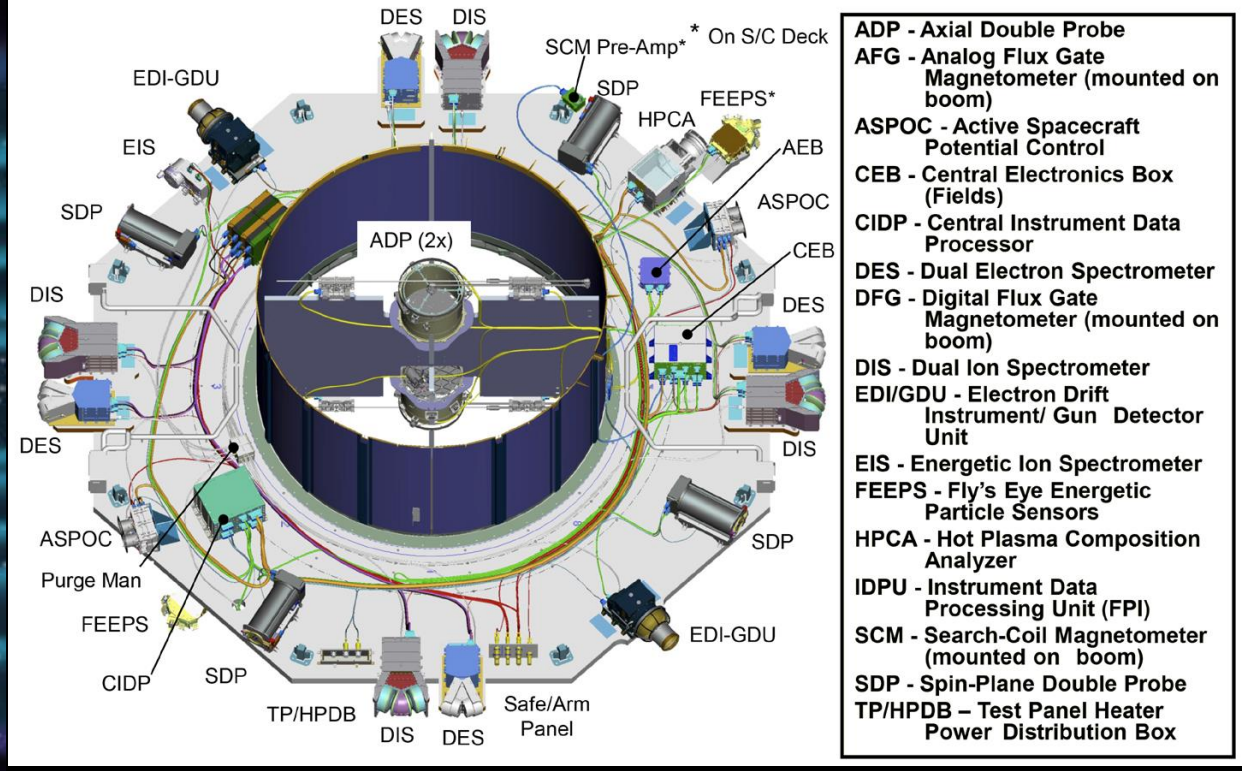
*USA – NASA*

KTH contributes!

But also small national missions: e.g. SPIDER-2








## Goal:

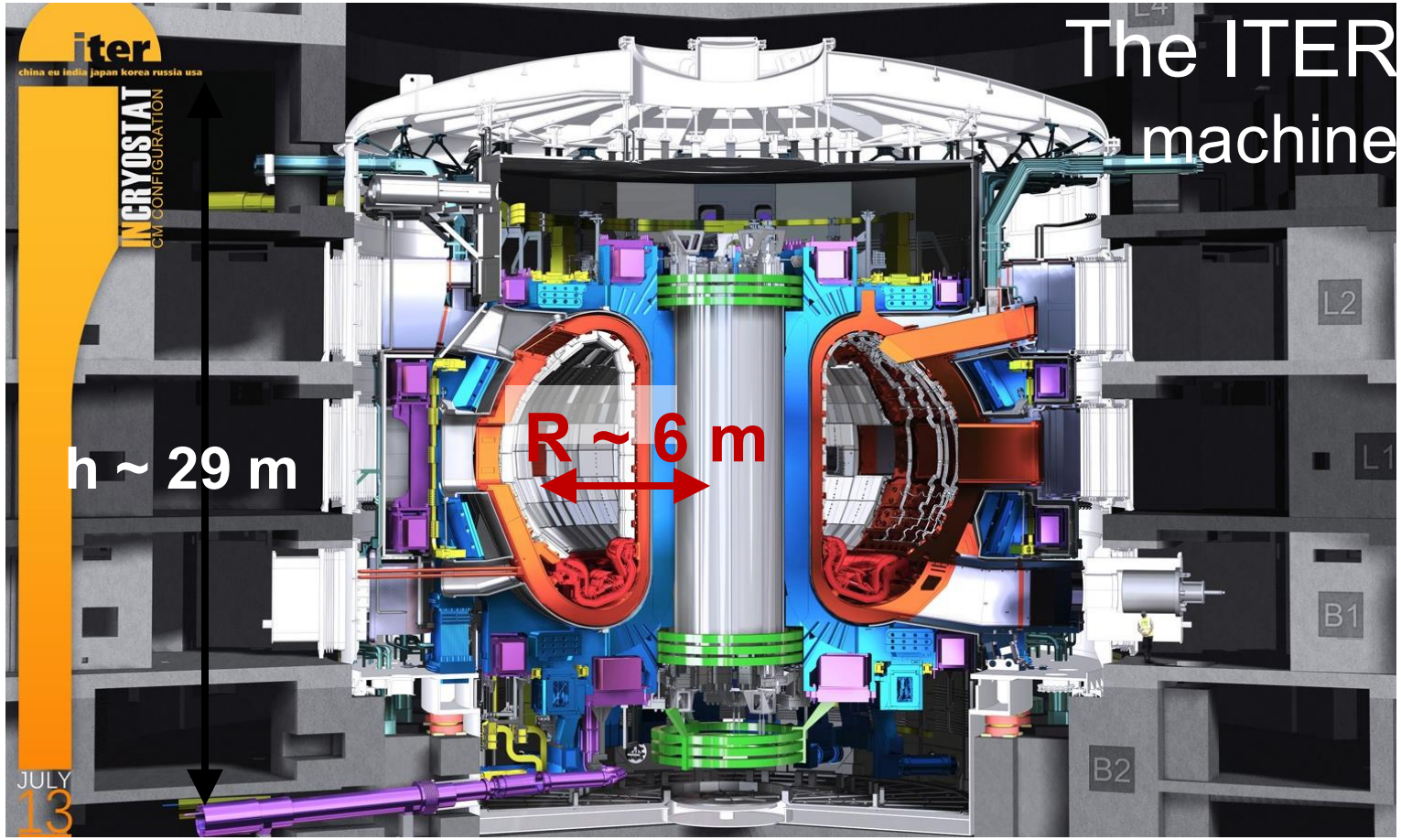
*Understanding how space environment around Earth and other planets form and affect the planets*

## How we do it:

- *Direct measurements by suite of plasma instruments*
- *Comparison to theory and simulations*

# Svetlana Ratynskaia, Professor in Plasma Physics

# Fusion energy: Bringing the Stars to Earth




The ITER machine

- **ITER will maintain burning fusion plasmas for long duration**
- It will test the integrated technologies, materials, and physics regimes necessary for the commercial production of fusion-based electricity

**Validation of the complete system can be performed only when the plant is built**

*while*

EU (FP10) ambitious timeline of 'Fusion on the grid' by 2034

<u>For large leaps forward:</u>

Physics-based models, numerical simulations & digital twins

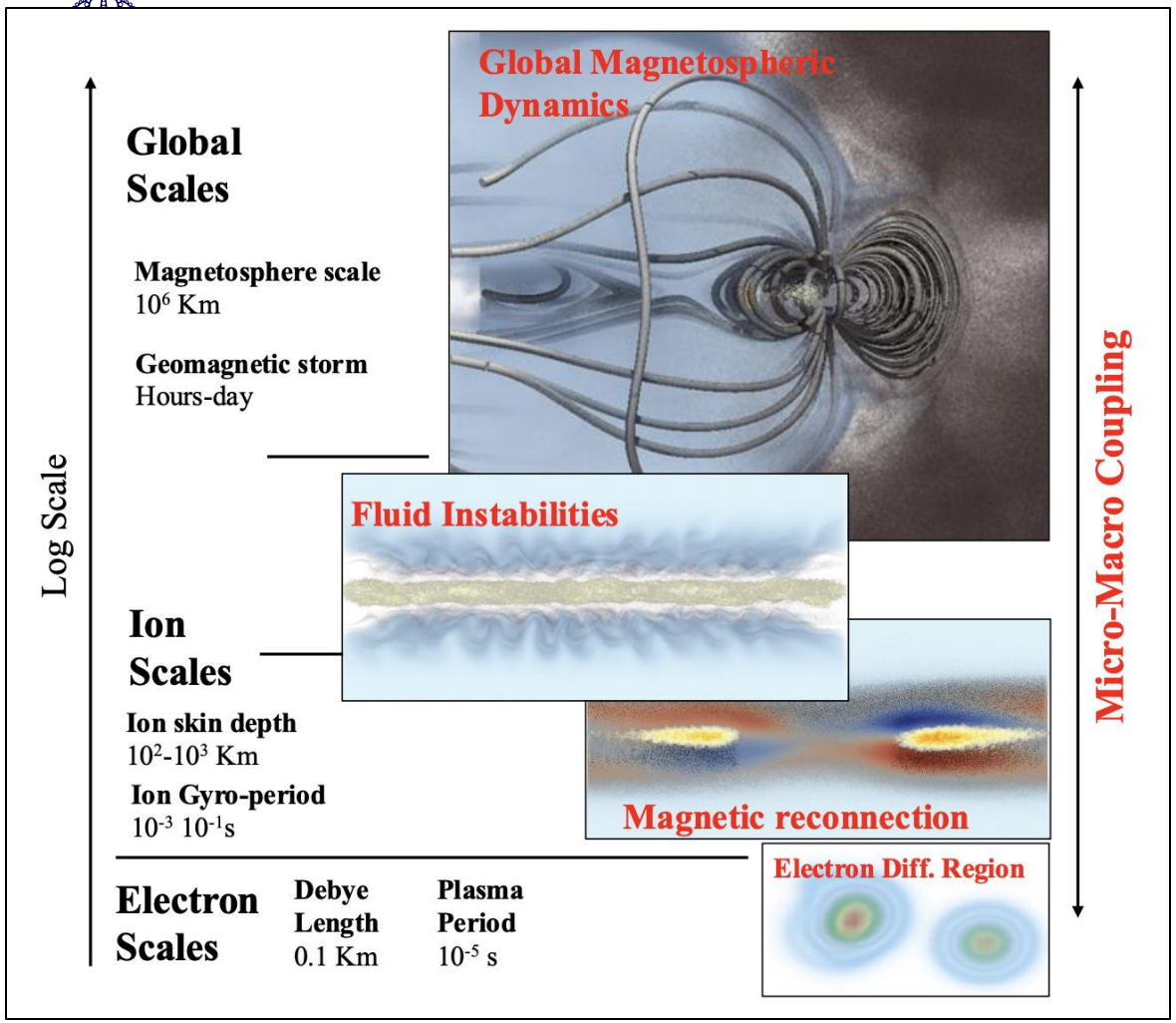
+

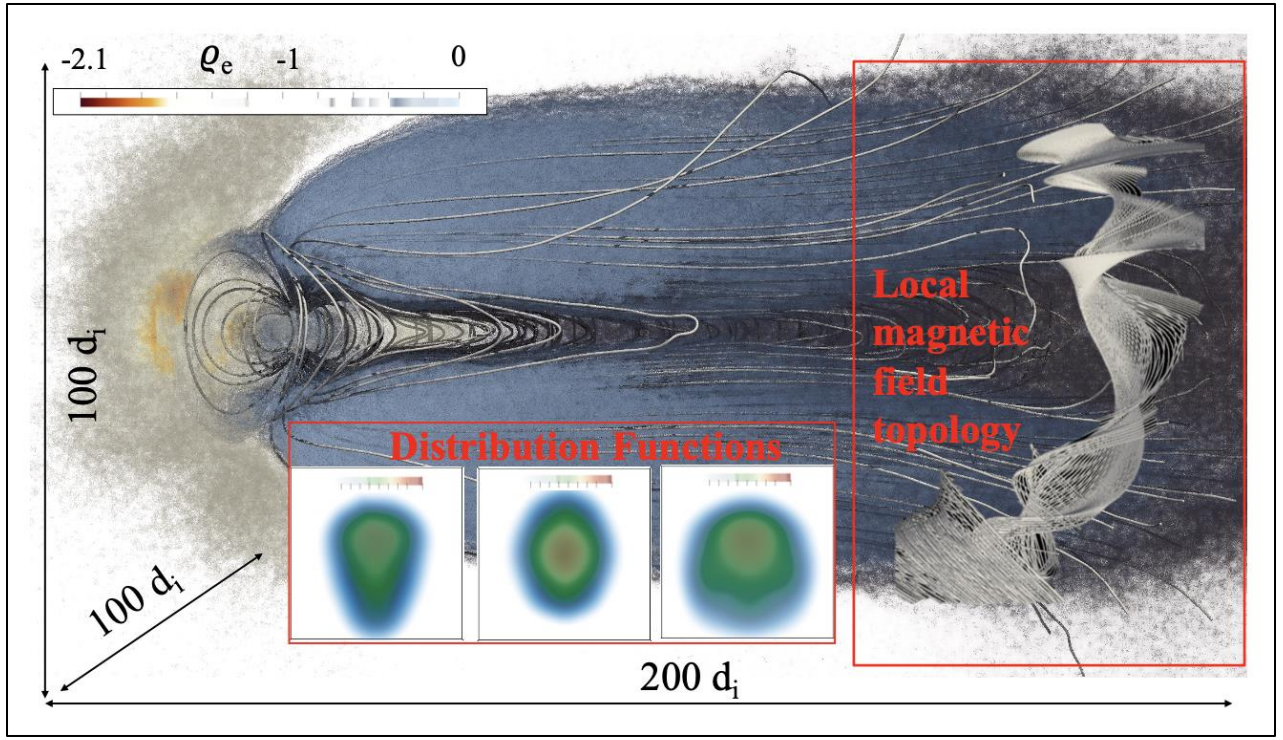
Model validations in today's machines

+

Materials testing & development

# Stefano Markidis, Professor of High Performance Computing



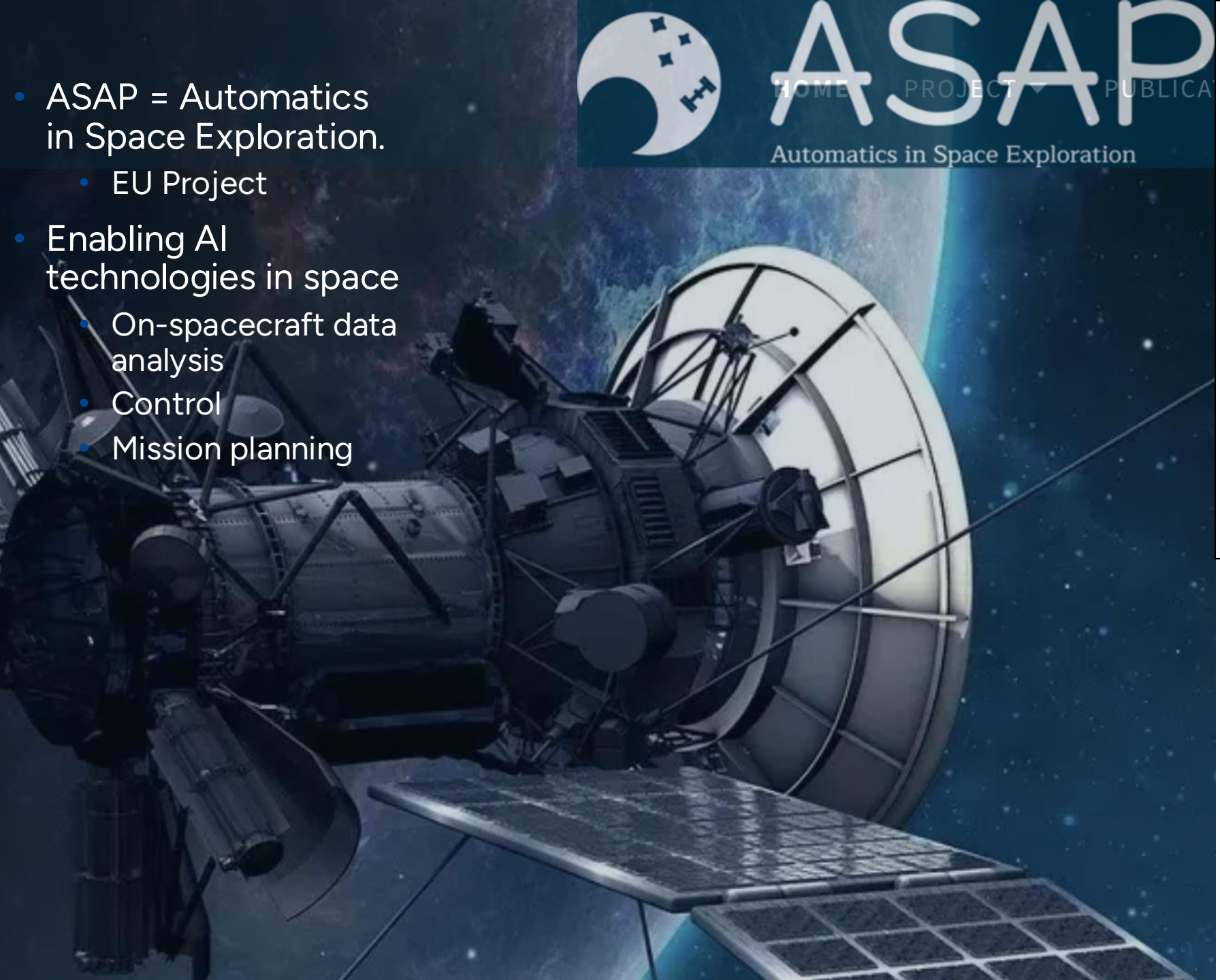



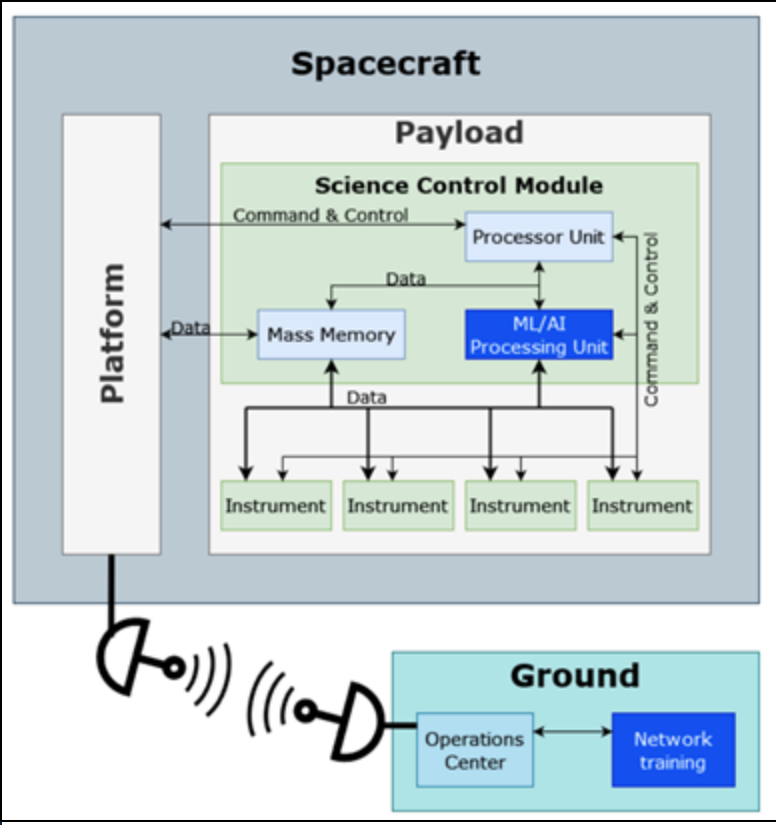


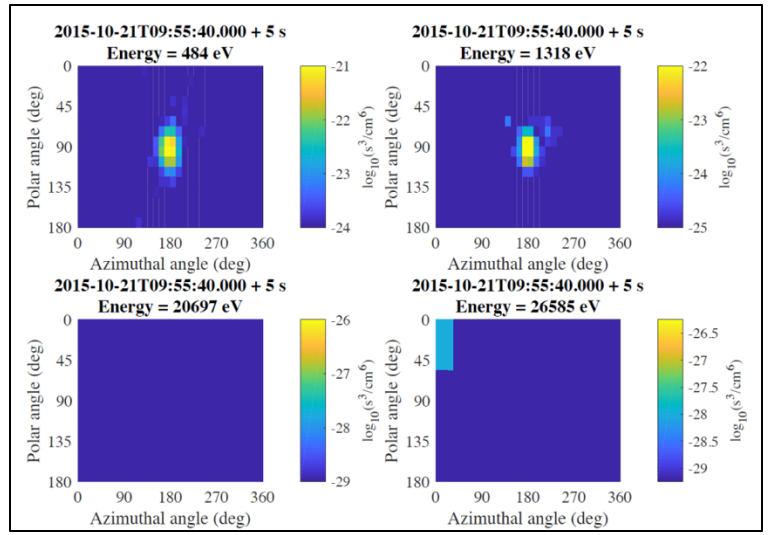
- Plasma-PEPSC, a European Center of Excellence for Plasma Simulations
  - Enabling simulation on Exascale Supercomputers for space weather

PLASMA PEPSC

- ASAP = Automatics in Space Exploration.
  - EU Project
- Enabling AI technologies in space
  - On-spacecraft data analysis
  - Control
  - Mission planning



# AI for Scientific Discovery and Engineering and Society from 6G to Genetic AI

Alexandre Proutiere, Professor and Leader of the KTH Center for AI

Cicek Cavdar, Associate Professor in Wireless Communication

Paris Carbone, Associate Professor in Software and Computer Science

Thomas Winkler, Associate Professor in Micro and Nanosystems

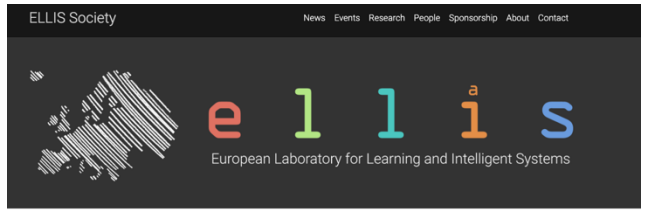
Hedvig Kjellström, Professor in Computer Vision

# Alexandre Proutiere, Professor and Leader of the KTH Center for AI

# KTH Center for AI (A KTH strategic initiative)

Get AI research at KTH more visible, organized, and collaborative to shape the next AI wave: an inter-disciplinary effort


**Foundations of AI**
**AI for scientific discovery**
**AI for engineering and society**



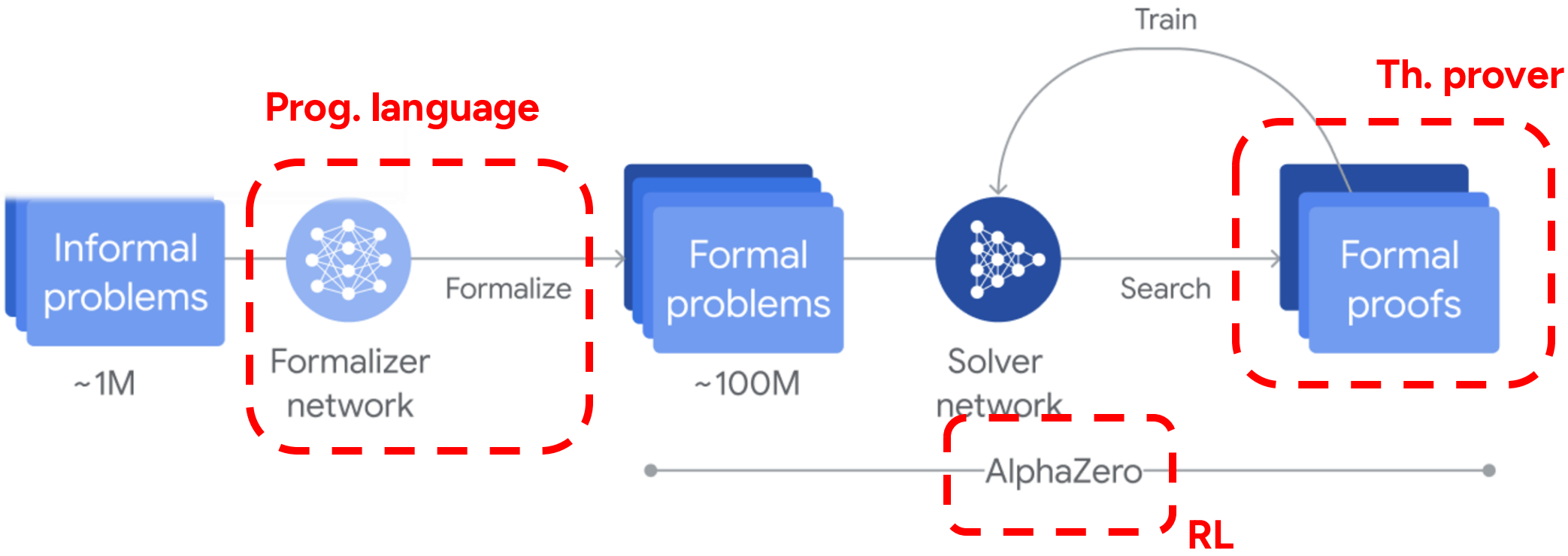

**In 2025:**
ELLIS application
Consolidate partnerships
VR/Vinnova  excellence clusters

# AI Reasoning

Get AI models to match and surpasses top human performance in  rigorous intellectu
tasks

GPT5 (OpenAI) = LLM+CoT

IMO gold medal 2025 (OpenAI, Gemini) = LLM + verification + RL

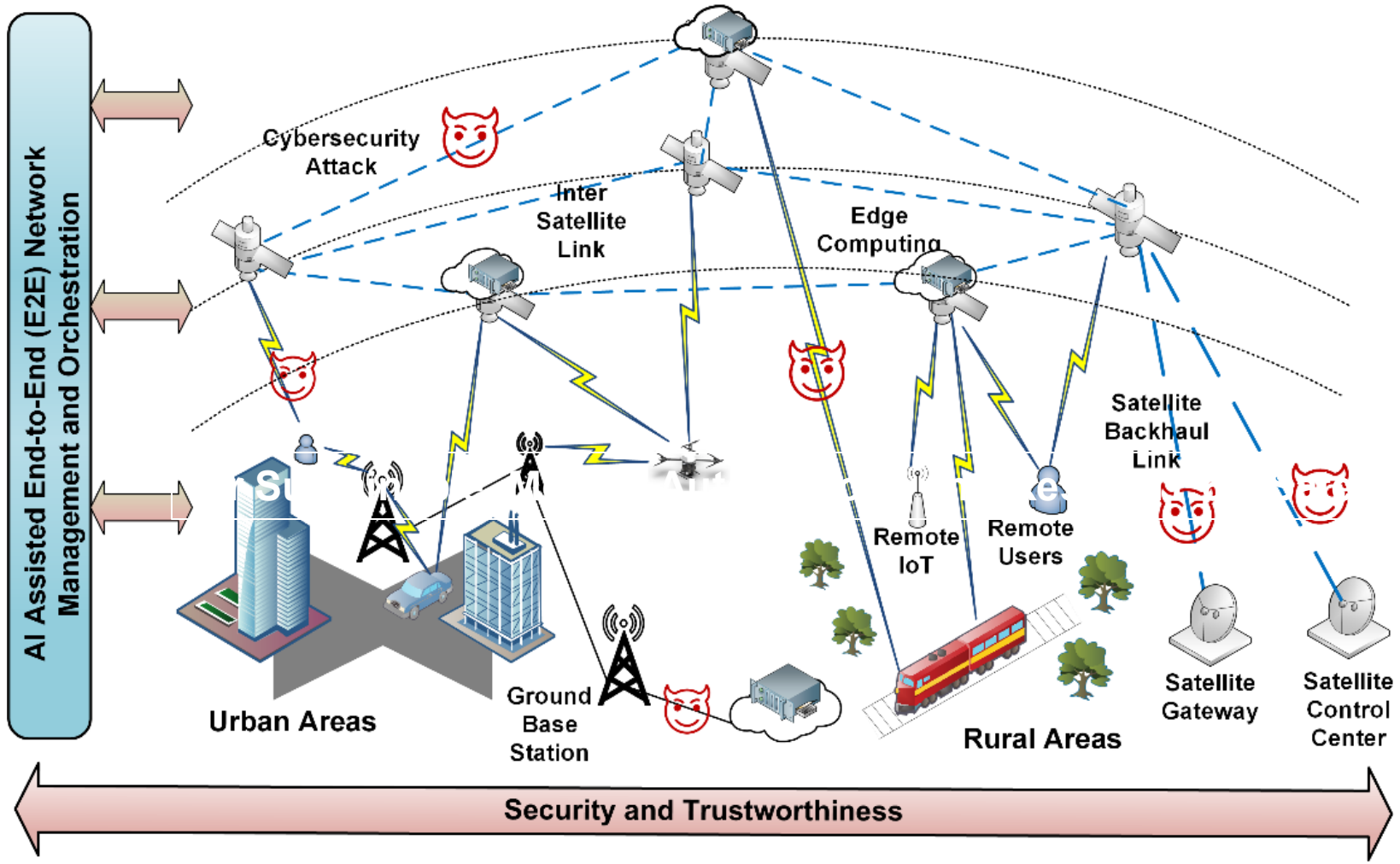


# Cicek Cavdar, Associate Professor in Wireless Communication

# AI Native 6G Communication Systems

## Sustainable, Mobile, Autonomous and ResilienT 6G Satellite Communications (SMART 6GSAT)

S M A R T
6 G S A T




Goal:

Robust and Sustainable Seamless Connectivity via Integrated TN and NTN with Sensing, Localization and Computing

2025-2031, 60MSEK
21 partners from telco and space industry

# AI for Green Mobile Networks

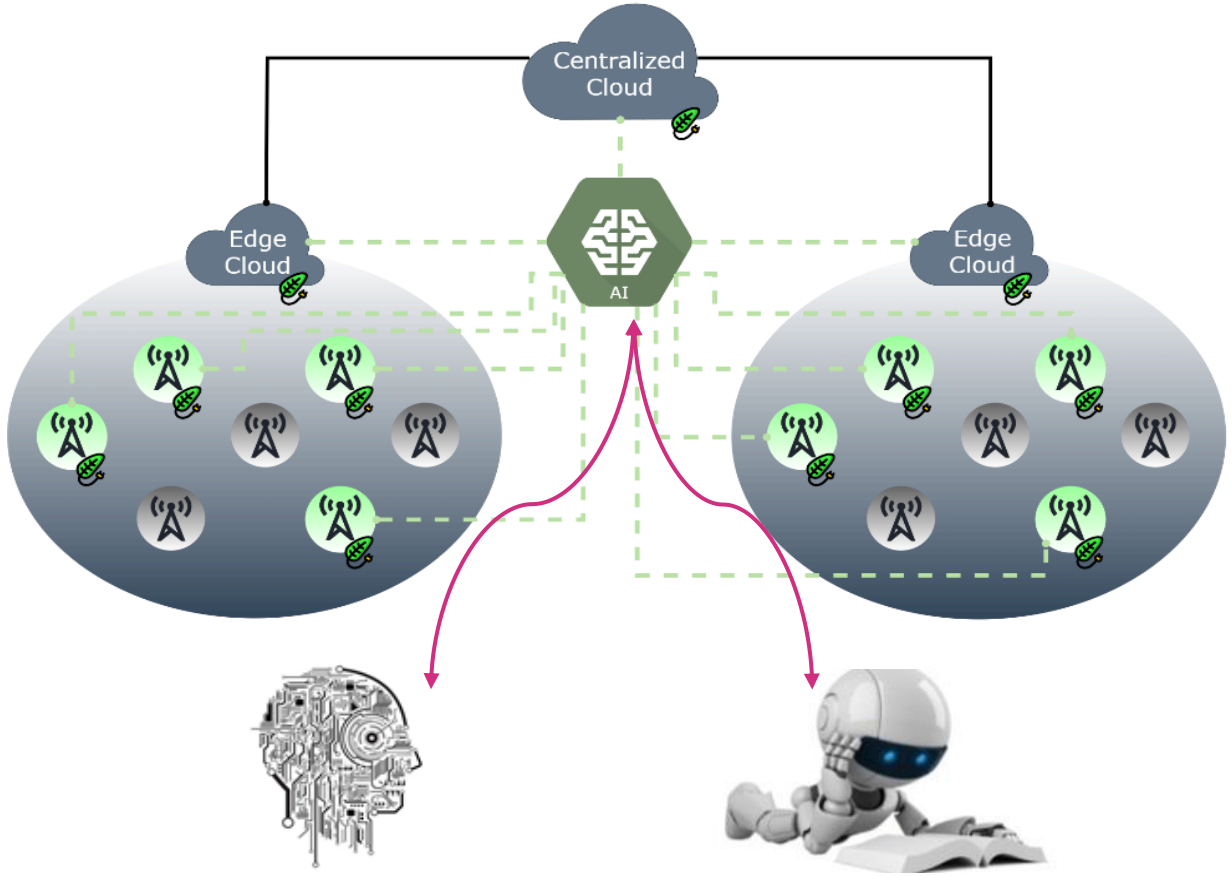
AI4GREEN

- AI4Green enables traffic-adaptive green mobile network solutions

How:

- Analyse the data from different resources
- Predict the future traffic, user behavior and services trends,
- Detect anomalies
- Train ML algorithms with data
- Learn decision impact over time
- Autonomously take decisions on energy saving functions

- Today's cellular networks are not made for adaptive and autonomous management, they are static. Energy saving will be limited if we inject some ML in today's BSs.
- Study advanced technologies and architectures




*Artificial Intelligence & Machine Learning*

# Paris Carbone, Associate Professor in Software and Computer Science

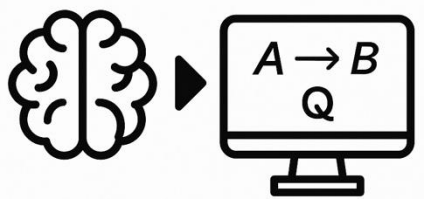
*a systems frontier*

# AI for Scientific Discovery

## key innovations and their applications

**Neurosymbolic LLM-Integration +RL**

**Automated Theorem Provers (ATPs)**




**Agentic/ Compound AI**

**Scientific Assistants & Code Generators**

**Foundational Relational/Graph Models**

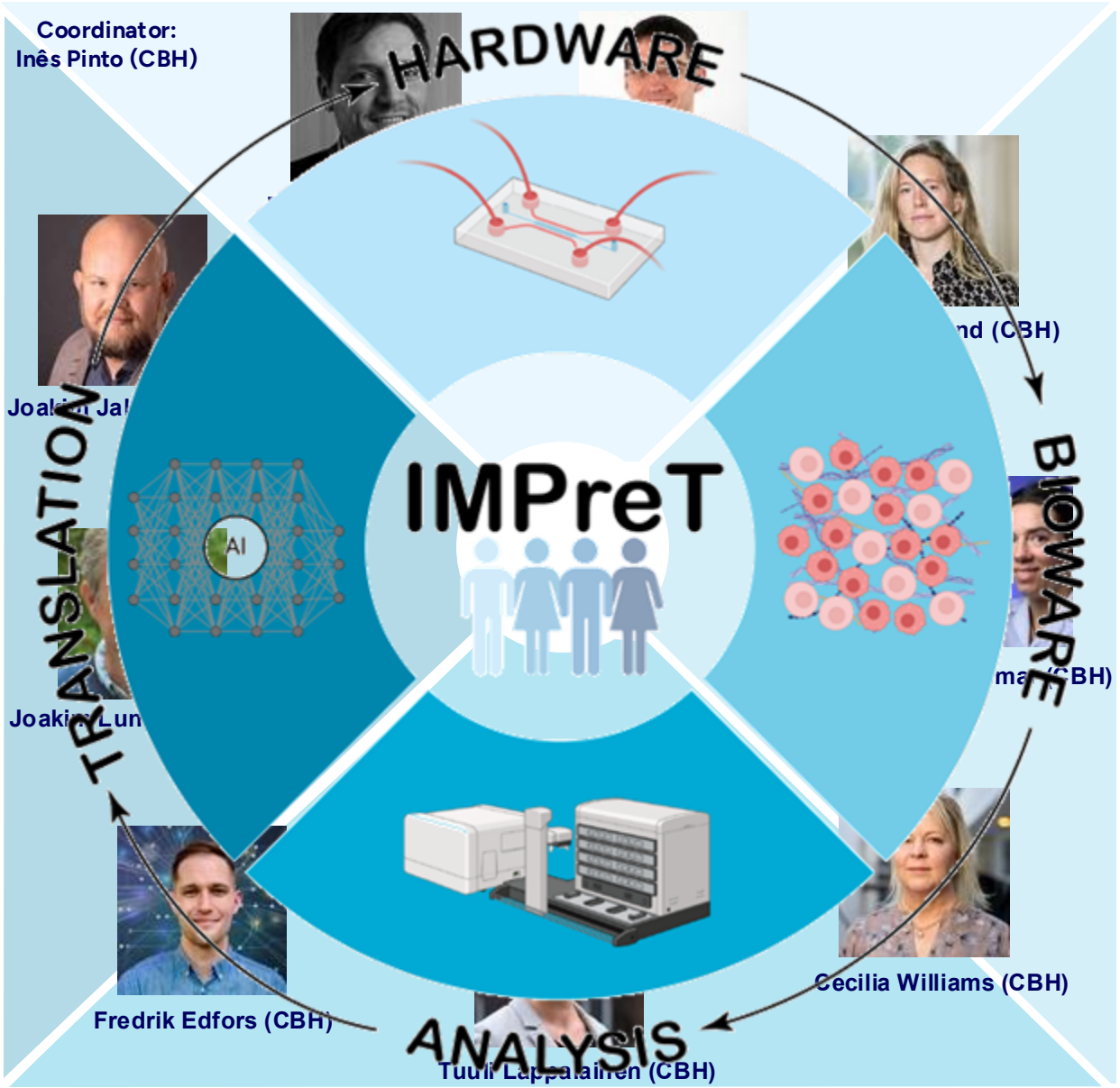
**Predictive Multimodal Reasoning & Integration**

**Advanced Model Quantization**

**Edge AI (6G, avionics, satellites etc.)**

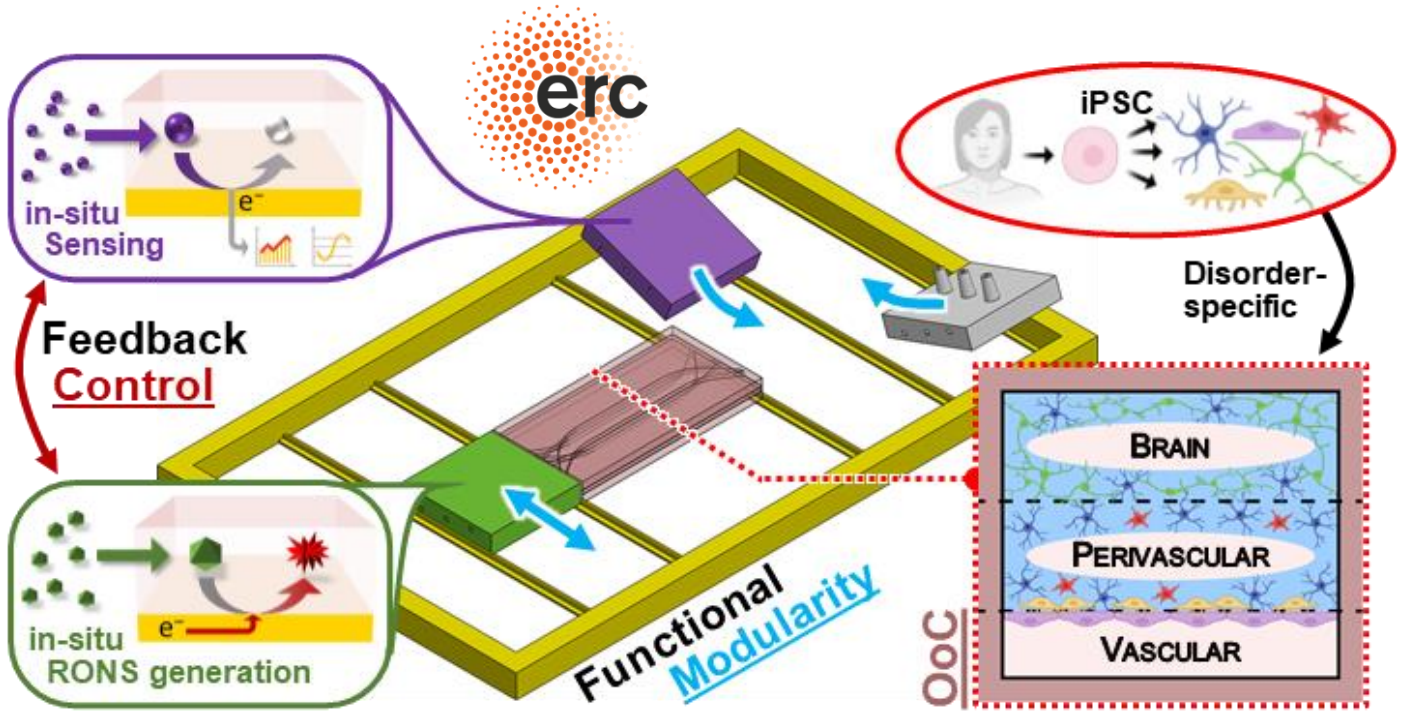
# Thomas Winkler, Associate Professor in Micro and Nanosystems

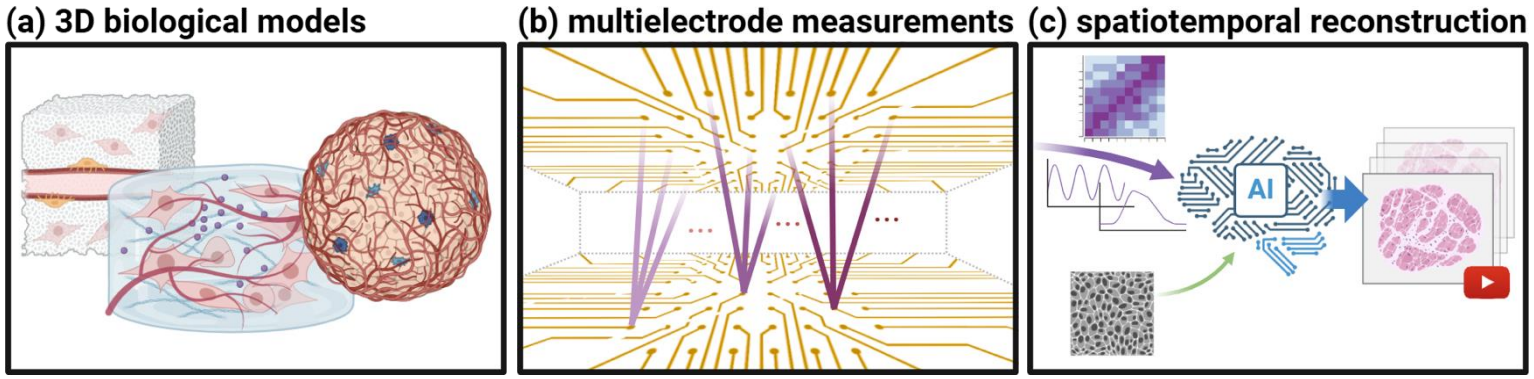
# IMPreT: In vitro Models for Precision Therapies

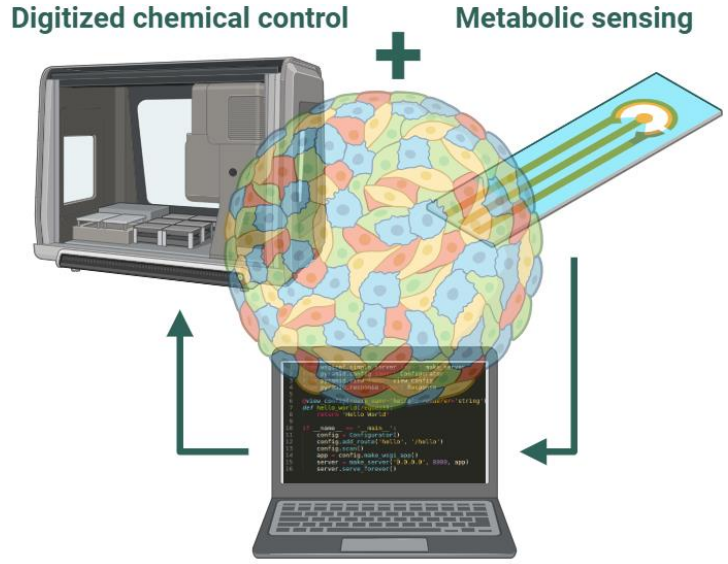


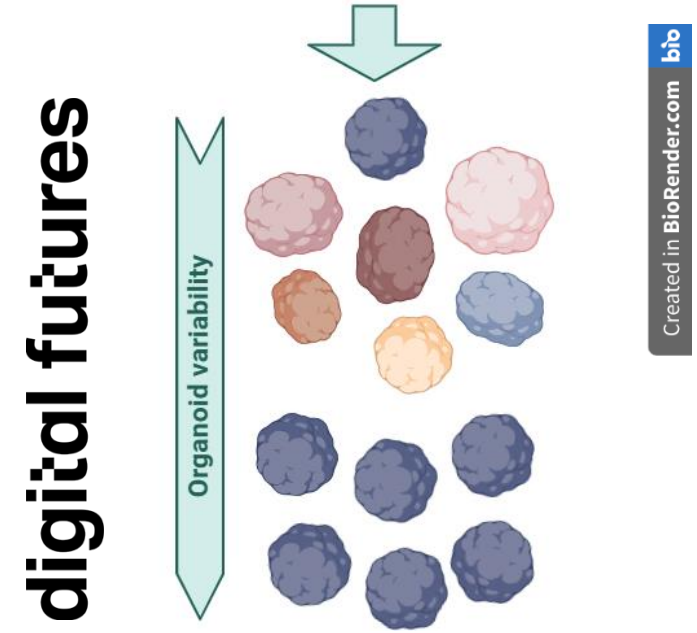

- **Leverage complementary expertise** from KTH EECS, CBH, and SCI along with our national infrastructure MyFab, NMI, NGI, NAISS/PDC, …
- Establish **KTH** as a **national hub** for next-generation precision medicine, integrating **engineering**, **life sciences**, and **AI** into **human-relevant in vitro models**
- Develop a **sustainable**, **scalable** platform for **personalized medicine** in Sweden
- Network expansion through **academic**, **clinical** and **industrial collaborations**

# Intelligent In Vitro Models



# Hedvig Kjellström, Professor
# Computer Vision

# Strategic research initiative at KTH: GAIN – Generative AI for Next-Generation Science

https://www.kth.se/en/forskning/sarskilda-forskningssatsningar/strategiska-initiativ/kth-gain

The GAIN platform aims to build on KTH's strengths in scientific computing to establish broad leadership in applying generative AI methods in high-performance computing environments. Our particular focus is achieving impact in high-profile scientific and societal challenges.

- Modeling scientific processes with generative AI methods
  - Hot topic, e.g., Nobel Prize in Chemistry 2024 in this area
- KTH SCI and EECS schools
- Applications in climate, chemistry, materials, fluid mechanics, medicine, etc
- Leverage and develop high-performance computing resources
  - PDC, NAISS, EuroHPC, Lumi etc
- Leverage and develop national and international collab
  - SciLifeLab, Riken, LiU, WASP AI4Science etc

# Cyber Security and Privacy and Safety Critical Systems

Mathias Ekstedt, Professor in Software Systems Architecture and Security

Cyrille Artho, Associate Professor in Software Engineering

Tobias Oechtering, Professor in Information Science and Engineering

Henrik Sandberg Professor in Decision and Control Systems

# Mathias Ekstedt, Professor in Software Systems Architecture and Security

# Cybersecurity at KTH

- Multidisciplinary subject (according to ACM cybersecurity curriculum)
  - Technical security
    - Data security, Software security, Component security, Connection security, System security
  - Human security (usable security, awareness, deception, …)
  - Organisational security (Risk management, governance, culture, continuity planning, etc..
  - Societal security (policy, law, ethics, ..)
- KTH (mainly) works with parts of Technical security
  - Privacy, crypto, programming language security, software composition security, hardware security, communication network security, enterprise systems security, cyber-physical security, AI/ML security
  - Mainly at EECS, but also ITM
    - COS, NSE, SCS, TCS, DCS, ISE, ESY, MID
- Centers, etc.
  - Center for Cyber Defense and Information Security (CDIS)
    - 15 projects listed
  - Digital Futures
    - Trust group, several projects
  - WASP
    - Several projects
  - Cybersecurity and Privacy (CySeP) Summer School
  - Cybercampus

# Cyber attack simulations for cyber defense

## Digital cyber twin

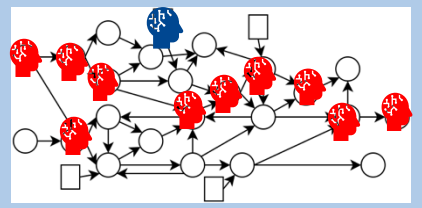
Asset graph

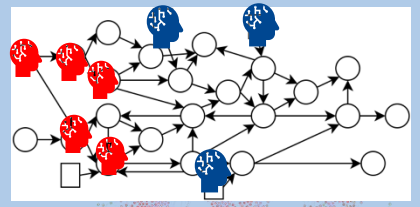
Attack graph

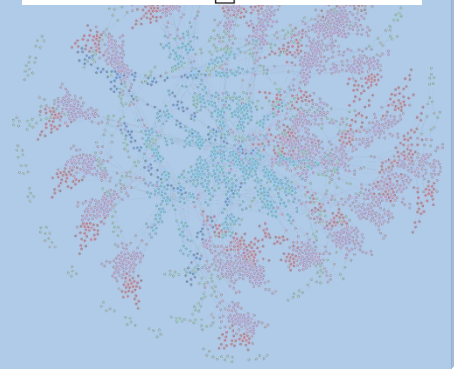
game 1

game 2

game n

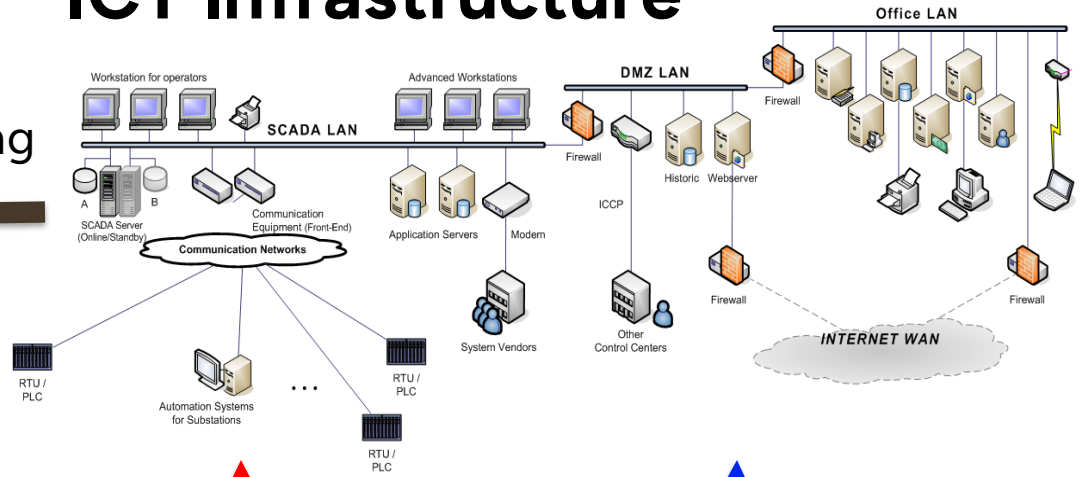






Modeling

## ICT Infrastructure




Malicious actions

Defense actions

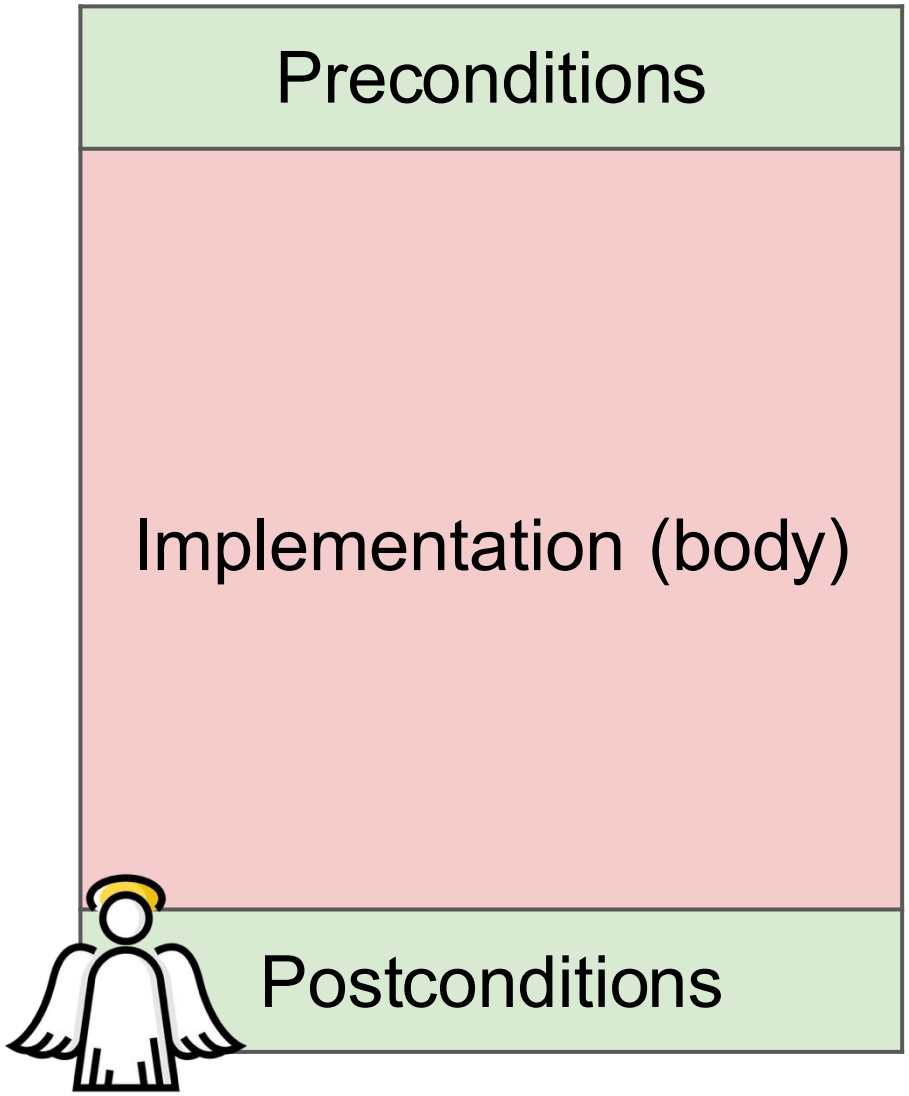
Training

Attacker

Defender

# Cyrille Artho, Professor in Software Engineering

# How to trust untrusted code?

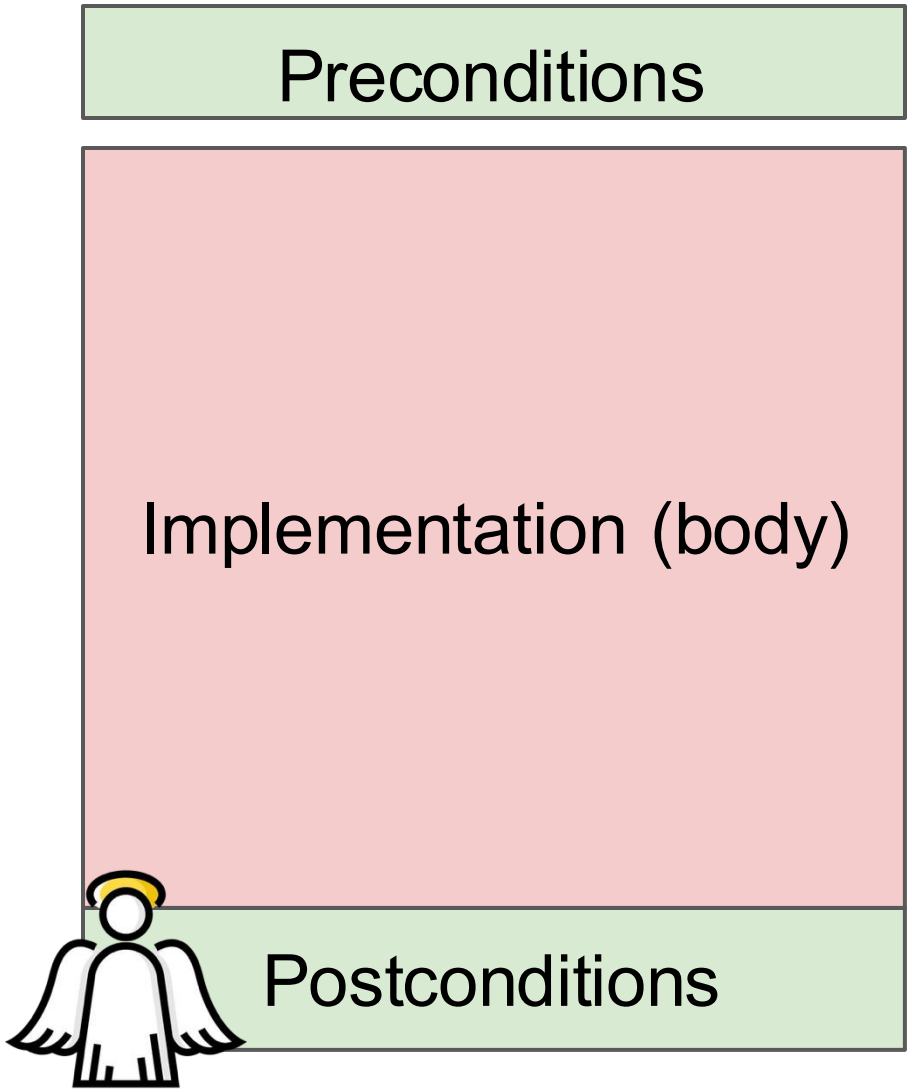



**Ensure** data is valid

Minimal restrictions (sandbox)

**Ensure** output is valid

# How to handle software upgrades with untrusted code




1. Modern **platforms enforce** checks:
   - M. Birgersson, M. Balliu: TEEs
   - M. Eshghie: Smart contracts
2. Modern **tools** offer **graphical** models:
   - M. Esghie: DCR graphs
   - P. Kamboj, R. Guanciale: Petri nets

# Tobias Oechtering, Professor in Information Science and Engineering

# Privacy – A challenge in a data-driven society!

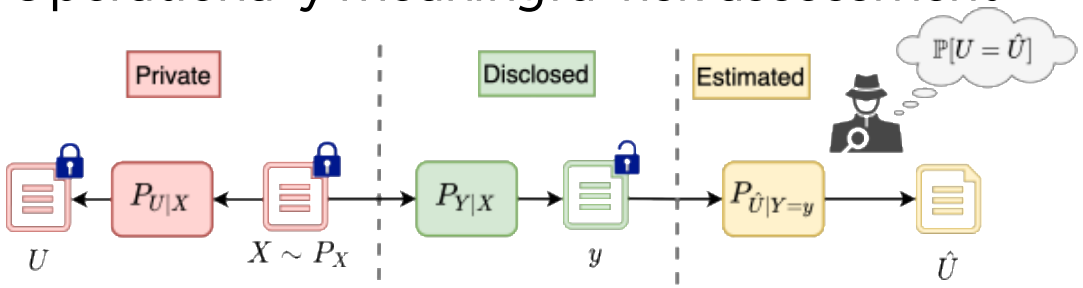
Vetenskapsrådet

## WHY?

- Personal data is freely shared and collected
  - Data brokers create and sell profiles
  - Once compromised, it cannot be restored
- Individuals act irrationally
  - Short term benefit against long-term harm (hyperbolic discounting)
- Advances in ML increase the privacy risk
  - Data can be stored – adversary can wait
- Legal requirement (GDPR)
  - Human right – high fines!
  - Uncertainity what is adequate and conservative approaches slow down technological development
- **Need a "lagom" implementation!**

## HOW?

- Privacy is an abstract concept – guarantees require a mathmatical proof!
- Operationally meaningful risk assessment




- Novel privacy measure **Pointwise Maximal Leakage** fixes problems of differential privacy

$$\ell(X \to y) := \sup_{P_{U|X}} \ell_U(X \to y)$$

$$= \log \sup_{P_{U|X}} \frac{\sup_{P_{\hat{U}|Y=y}} \mathrm{P}\left[U = \hat{U} \mid Y = y\right]}{\max_{u \in \mathcal{U}} P_U(u)}.$$

# Henrik Sandberg Professor in Decision and Control Systems

# DYNACON – DYNamic Attack detection and mitigation for seCure autONomy

**Principal Investigators**

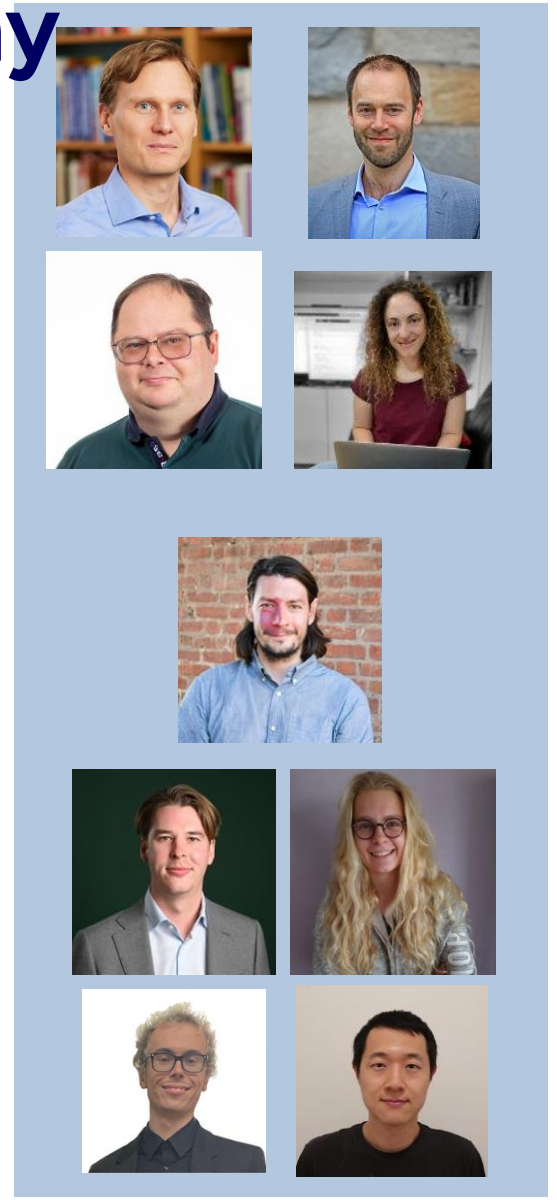
- Henrik Sandberg (KTH Decision and Control Systems)
- György Dán (KTH Network and Systems Engineering)
- Andrei Gurtov (LiTH Computer and Information Science)
- Martina Maggio (LTH Automatic Control)

**Postdoc**

- Rijad Alisic (KTH Decision and Control Systems)

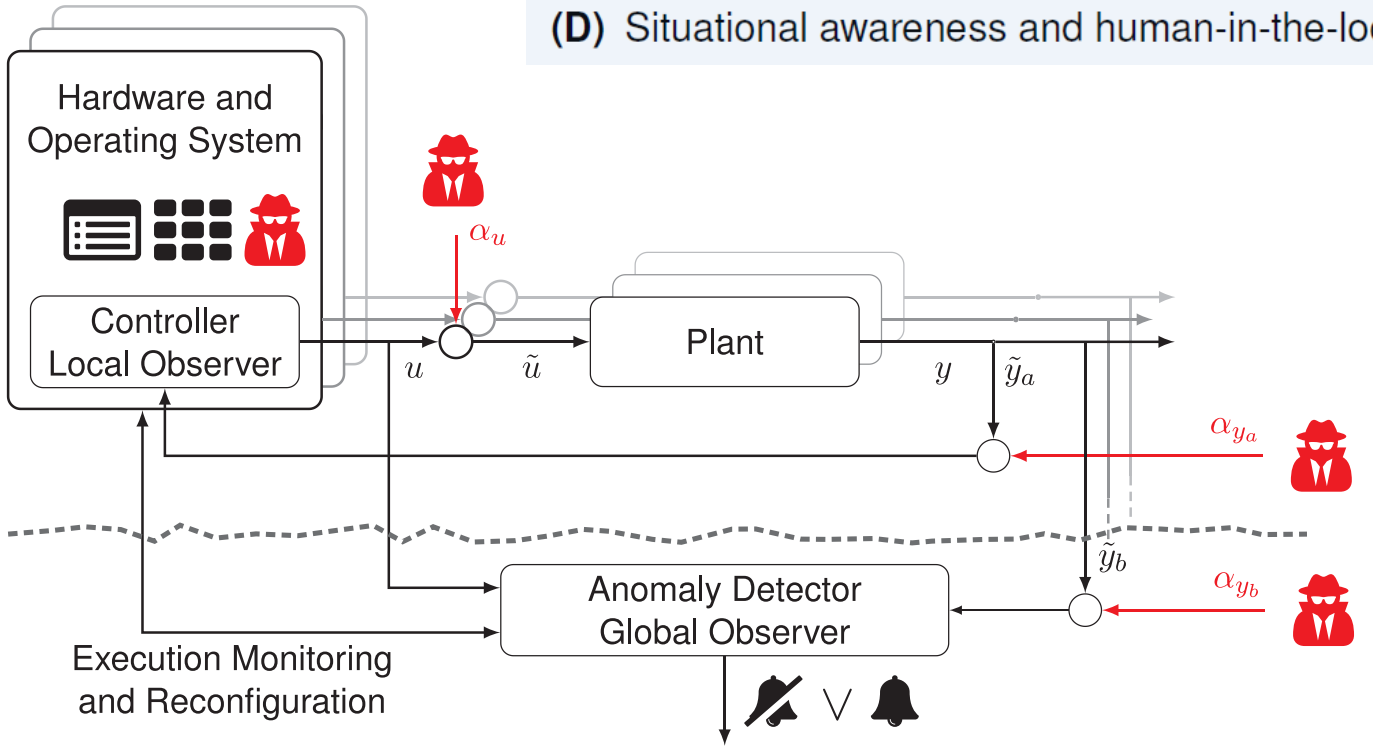
**PhD students**

- Axel Andersson (KTH Network and Systems Engineering)
- Talitha Nauta (LTH Automatic Control) [until Jan. 2025]
- Jacopo Porzio (KTH Decision and Control Systems)
- Zelong Wang (LiTH Computer and Information Science)



# Secure Autonomy Challenges

(A) False-data injection attacks and authenticated resilient state observers
(B) Timing attacks and switched trusted execution environments
(C) Identity spoofing and robust remote agent identification
(D) Situational awareness and human-in-the-loop AI for intrusion detection



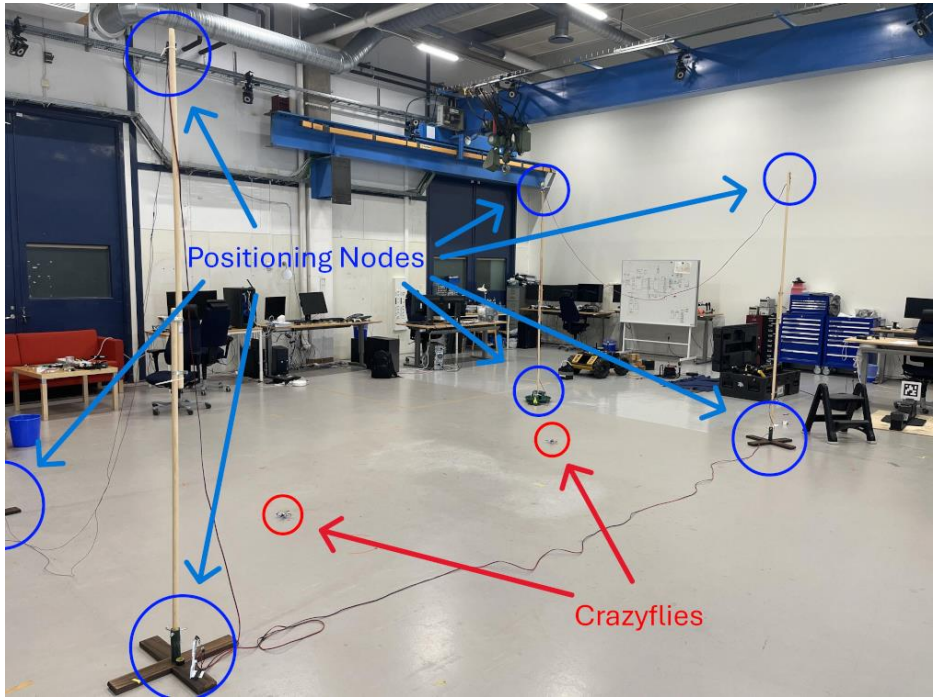

"...**cyber-physical security** (control systems, real-time systems, communication, and network security)"

"...injection of **false data** and **manipulation of timestamps** in **time-critical control loops**."

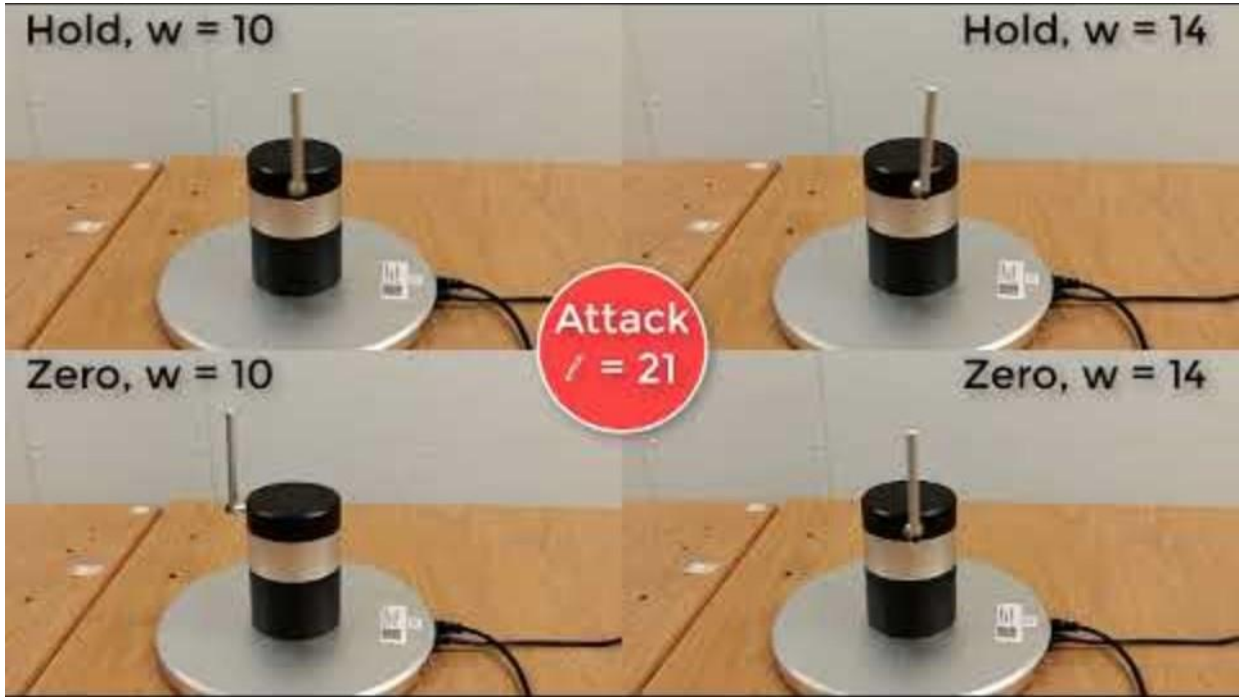
"...adaptively enabling the use of **trusted embedded devices** and **(limited) cryptographic authentication** when necessary. Furthermore, **distributed anomaly detection** and state **observer schemes**..."

"As a use case, we consider **swarms of unmanned aerial vehicles (drones)**. A particularly relevant scenario is that of "identity theft", where **malicious identity signals** are exploited by attackers to deceive the control system operators."

# Testbeds




[Larsson-Kapp, Kniivilä, Wang, Wzorek, Lemetti, and Gurtov, "Trust-Based Collision Avoidance for Unmanned Aircraft Systems," INCAS'24, [https://doi.org/10.1109/INCAS63820.2024.10798560]]




[Nauta, Sandberg, and Maggio, "Stealthy Computational Delay Attacks on Control Systems," ICCPS'25, https://dl.acm.org/doi/10.1145/3716550.3722013]