Security is not a single dimension

Simin Nadjm-Tehrani

Dept of Computer and Information Science

LINKÖPING UNIVERSITY

Back to the 50’s

Interesting times

- Our systems have never been as digitally connected as today
- The frequency and severity of data breaches and outages is monotonically increasing
- Geopolitical tension is intertwined with technical development

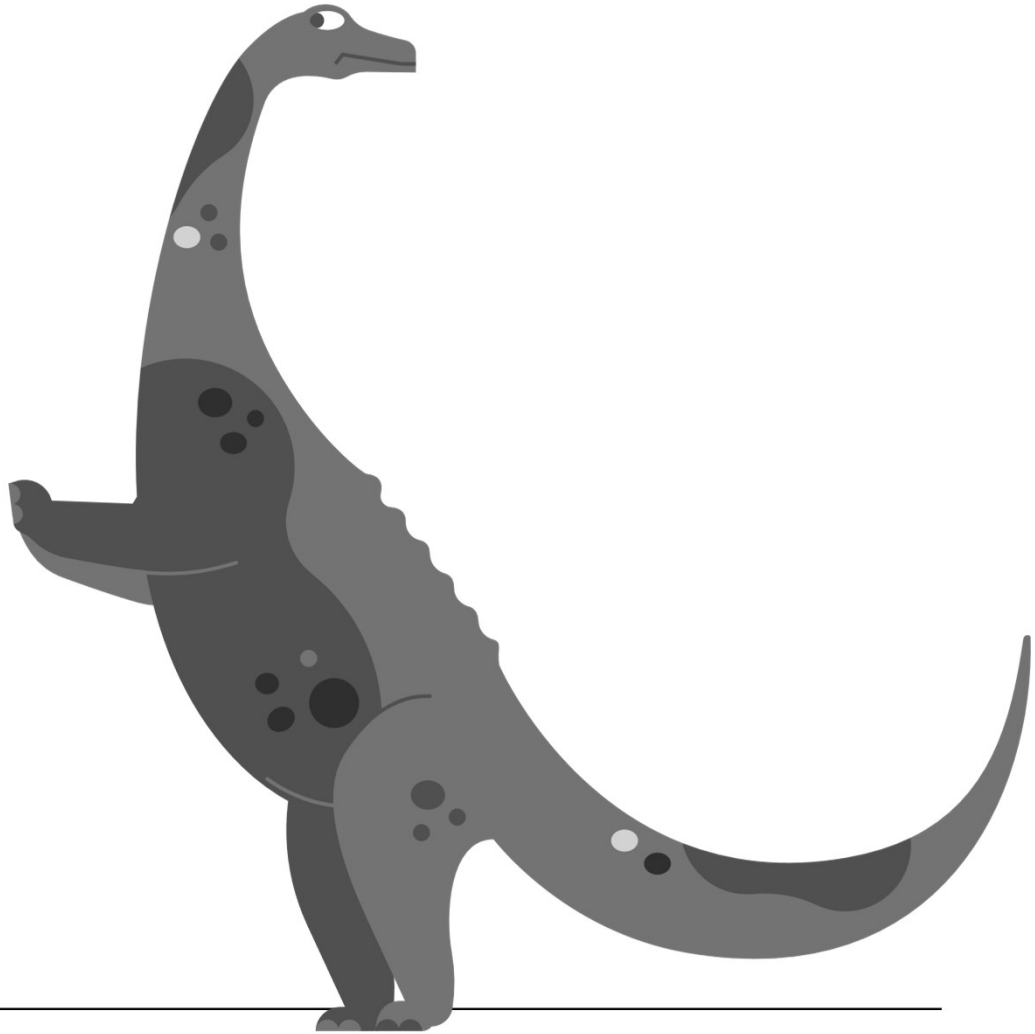
Rush to use AI but not many are sure why!

If we were to look into future…

"Crystal Ball" by deanfotos66 is licensed under CC BY 2.0.

AI can be used for different purposes

- Exploration
- Data fusion
- Optimisation
- Prediction
- Detection
- Decision
- Action
- Autonomous mission



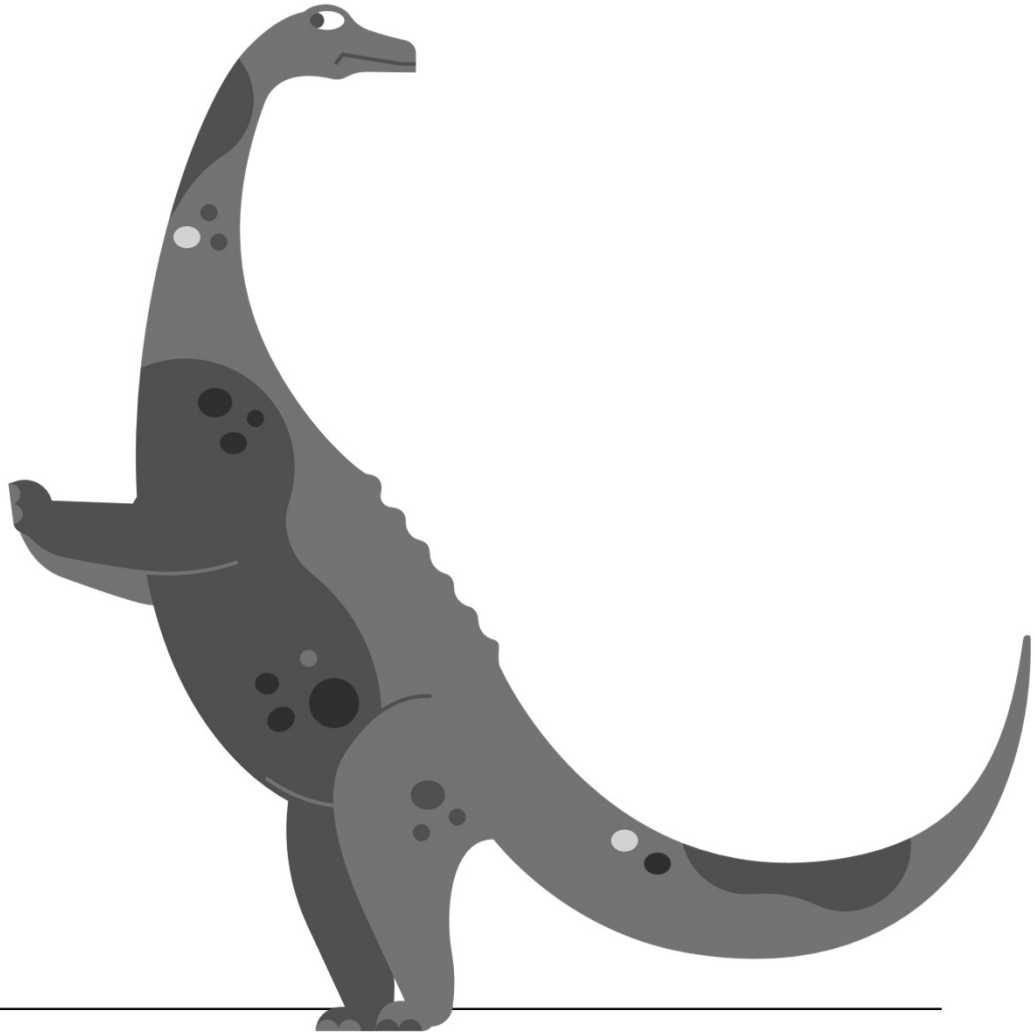
This summer…

LLMs being used for

- Hacking into systems

AI can be used for different purposes

- **Exploration**
- Data fusion
- Optimisation
- Prediction
- **Detection**
- **Decision**
- **Action**
- Autonomous mission

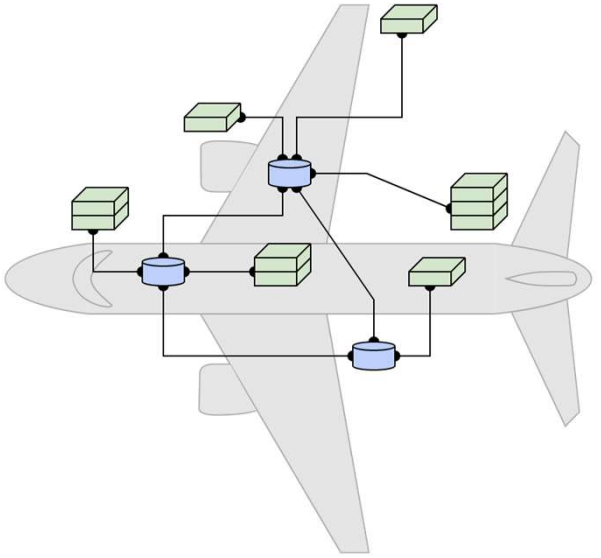


AI & Exploration

Integrated Modular Avionics (IMA)

Avionics concept design

- Resource adequacy
  - find a schedule for a *given* platform configuration
  - proof that a such a schedule exists (does not exist) for a *given* platform configuration
- Our work: Reasoning about *different* platform configurations
  - comparing their merits w.r.t. fault tolerance, security, resource efficiency, cost

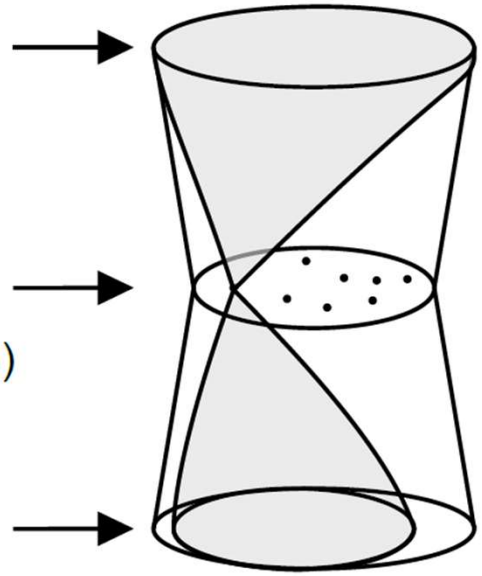


How to find a good enough architecture and mapping?

IMA Platform Modules and Connection Patterns
(HW/SW)

Alternative Platform Configurations
(Sets of Modules and Connections)

Concept Avionic Application Model
(SW Requirements)

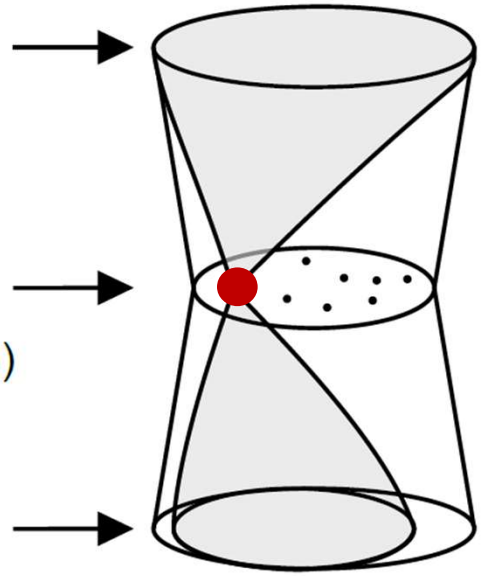


How to find a good enough architecture and mapping?

IMA Platform Modules and Connection Patterns
(HW/SW)

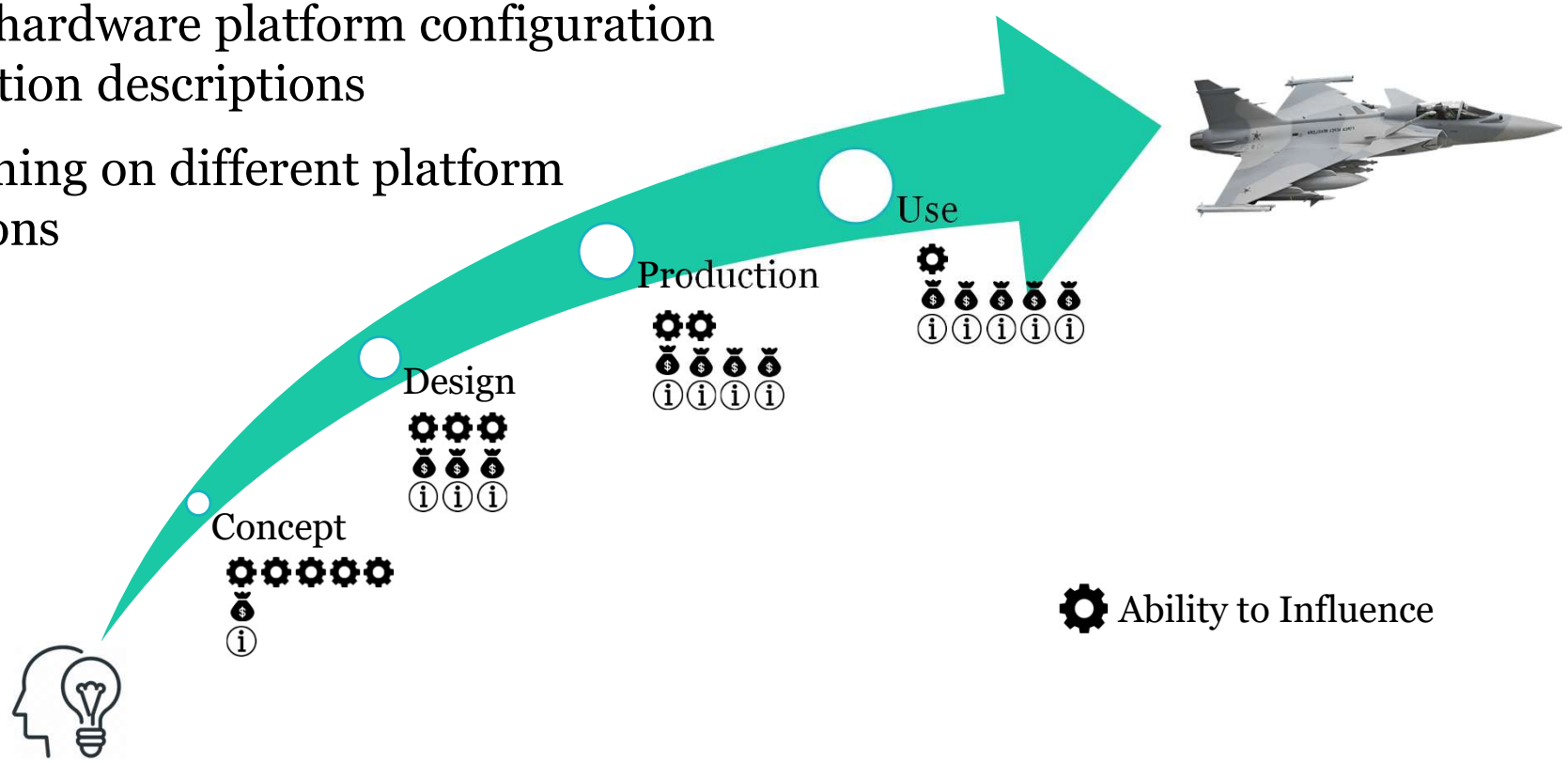
Alternative Platform Configurations
(Sets of Modules and Connections)

Concept Avionic Application Model
(SW Requirements)



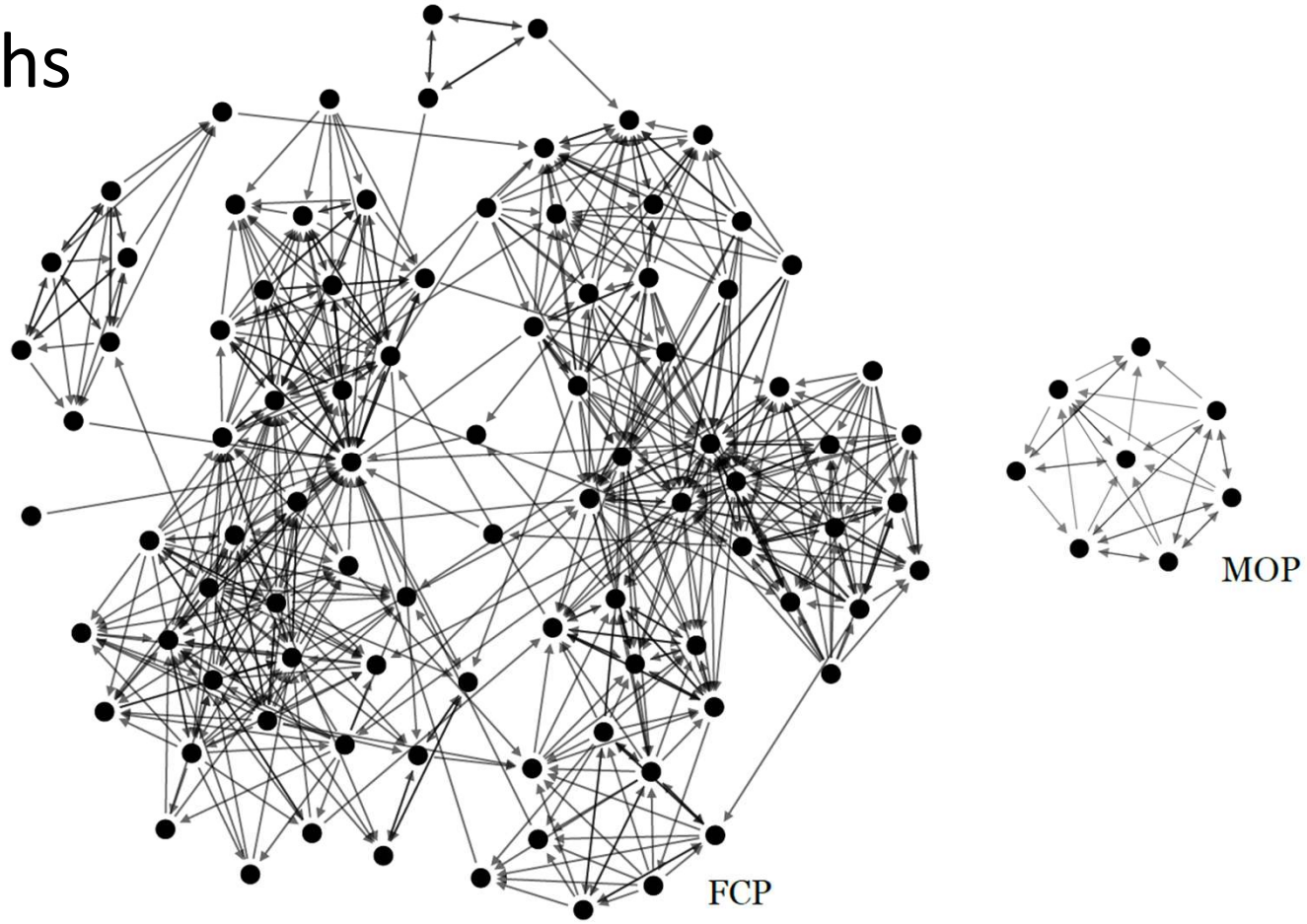
Goals

- Separating hardware platform configuration and application descriptions
- Early reasoning on different platform configurations

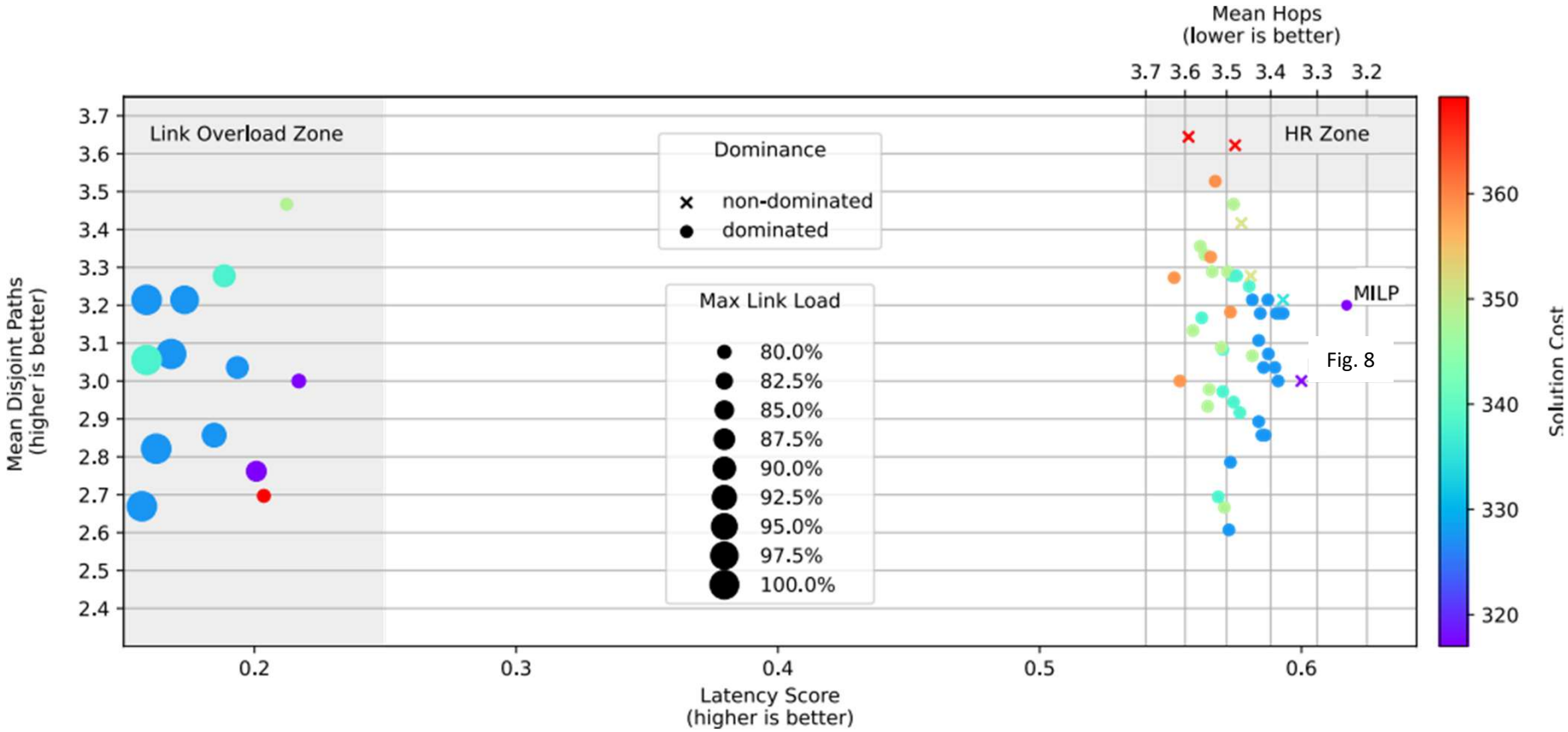


Saab Use Case

- Message paths



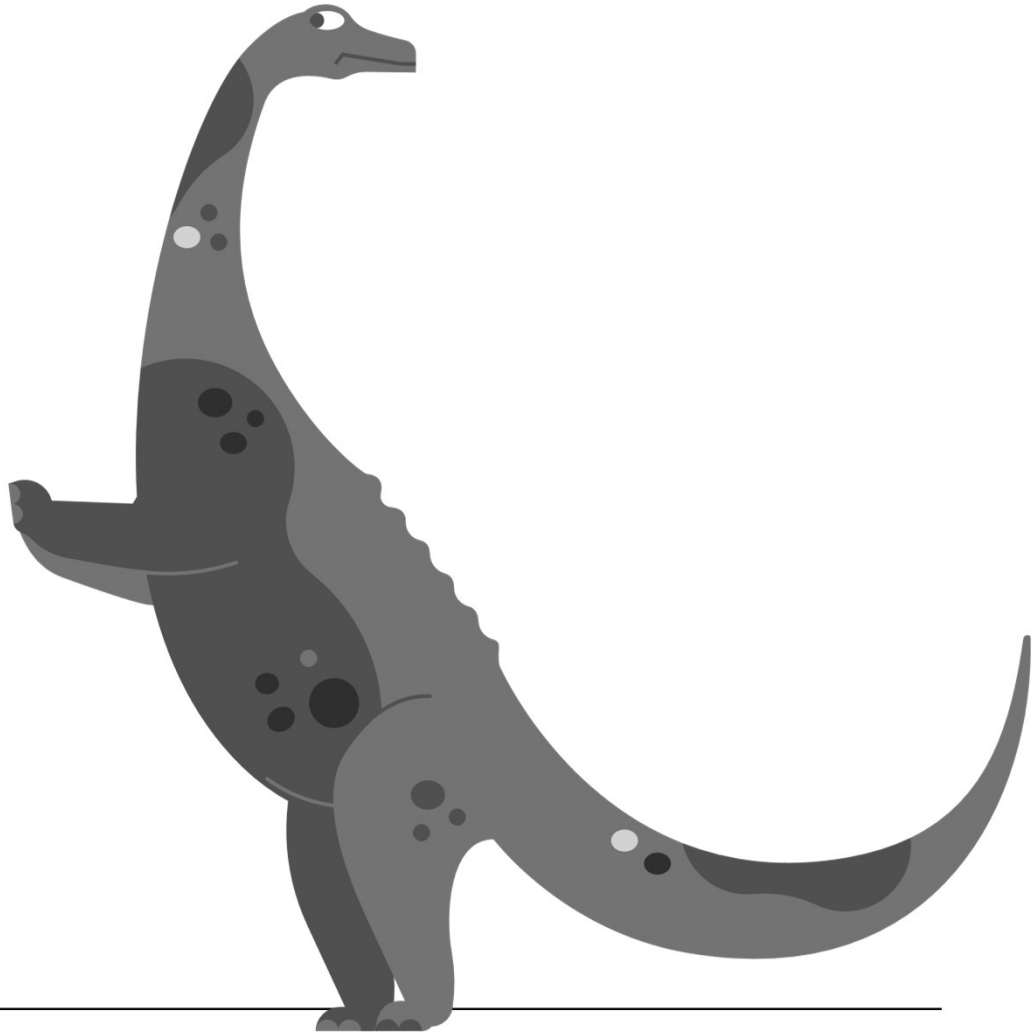
Our Approach: NetGAP



R. Moraes, S. Nadjm-Tehrani, *Engineering Applications of Artificial Intelligence,* 2024
doi:10.1016/j.engappai.2024.108089

AI can be used for different purposes

- **Exploration**
- Data fusion
- Optimisation
- Prediction
- **Detection**
- **Decision**
- **Action**
- Autonomous mission



AI & Decisions

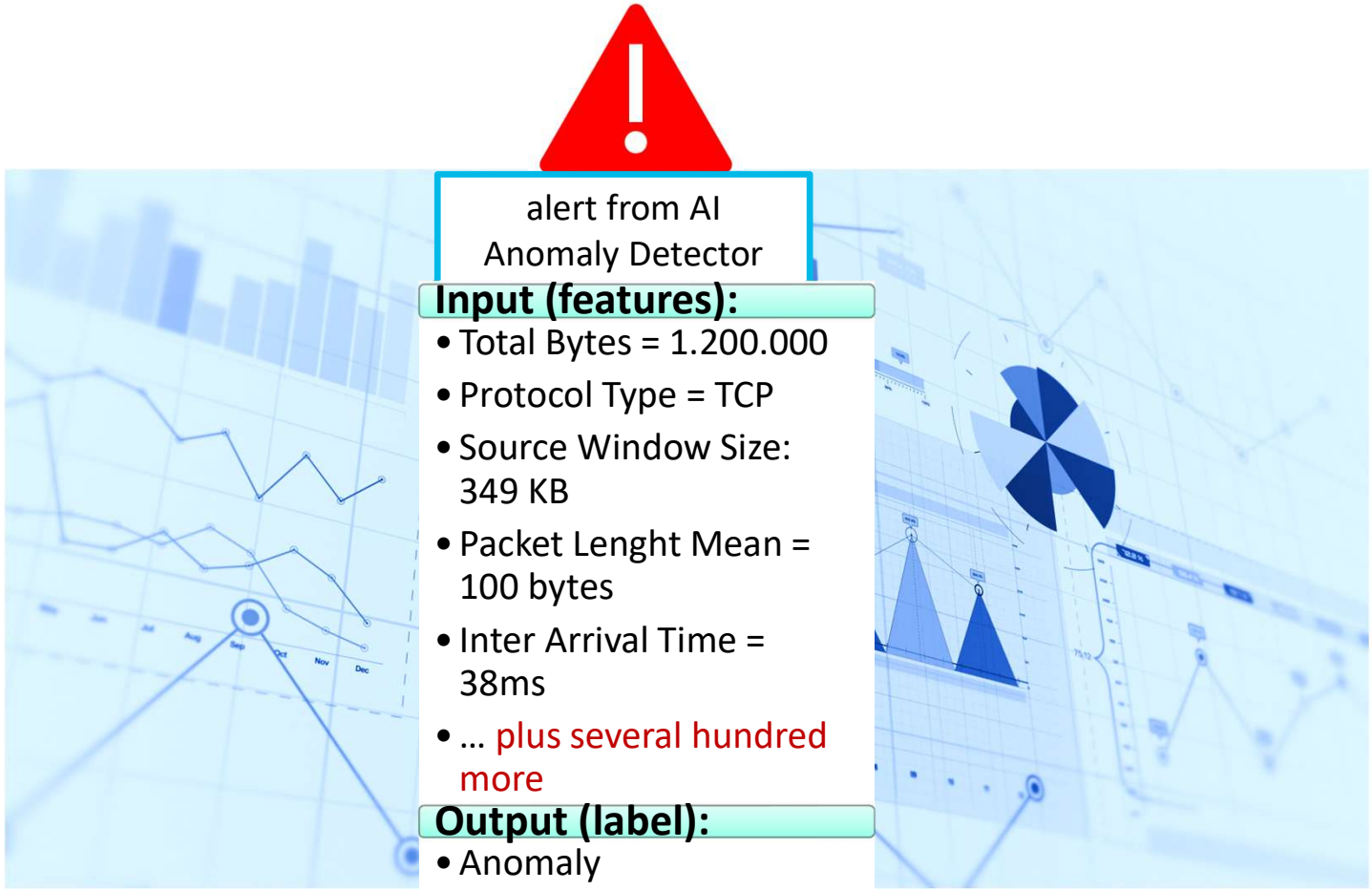
Protecting Critical Communication Infrastructures

LINKÖPING UNIVERSITY

AI & decisions

- EU AI Act constrains use of AI in decision making
- Some decisions are important
- Some have severe consequences
- **Our research:** Correctness of AI outputs needs to be verified

Intrusion detection in critical infrastructure



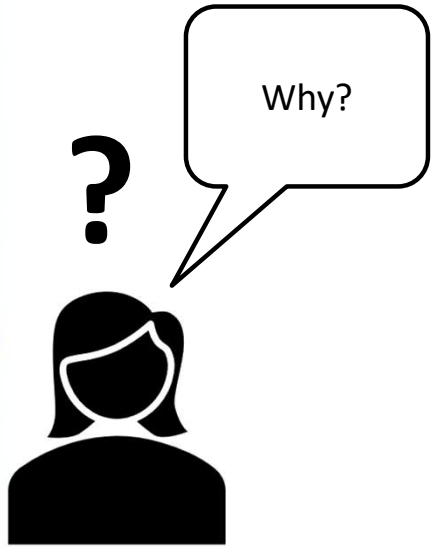
alert from AI Anomaly Detector

Input (features):

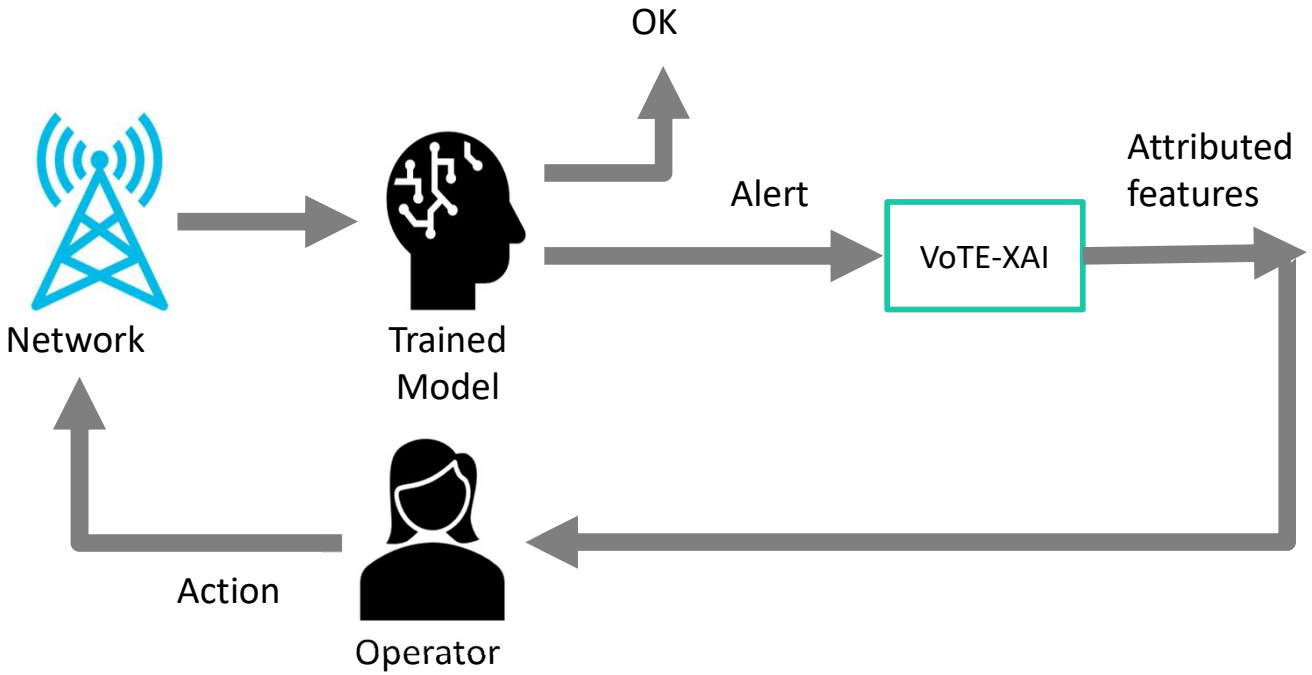
- Total Bytes = 1.200.000
- Protocol Type = TCP
- Source Window Size: 349 KB
- Packet Lenght Mean = 100 bytes
- Inter Arrival Time = 38ms
- … plus several hundred more

Output (label):

- Anomaly

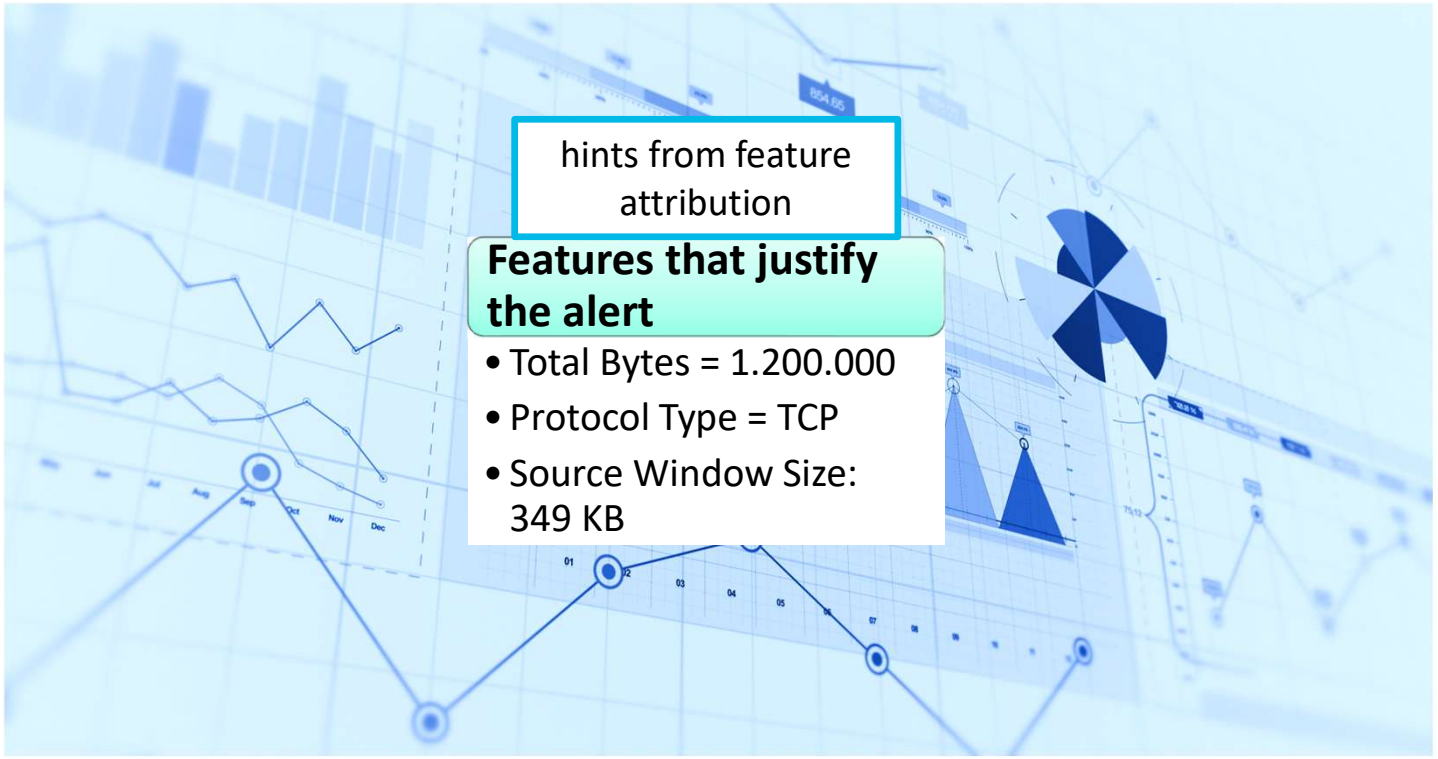


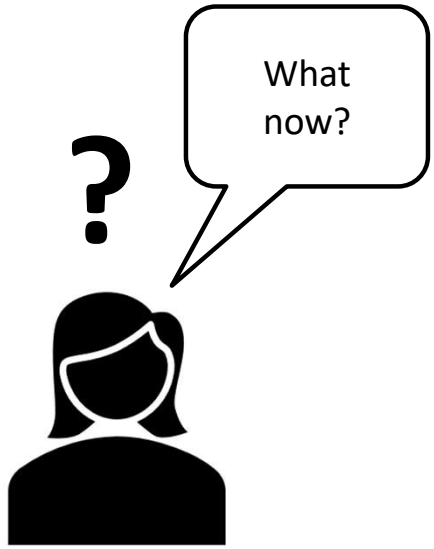
Which set of features explain the alert?



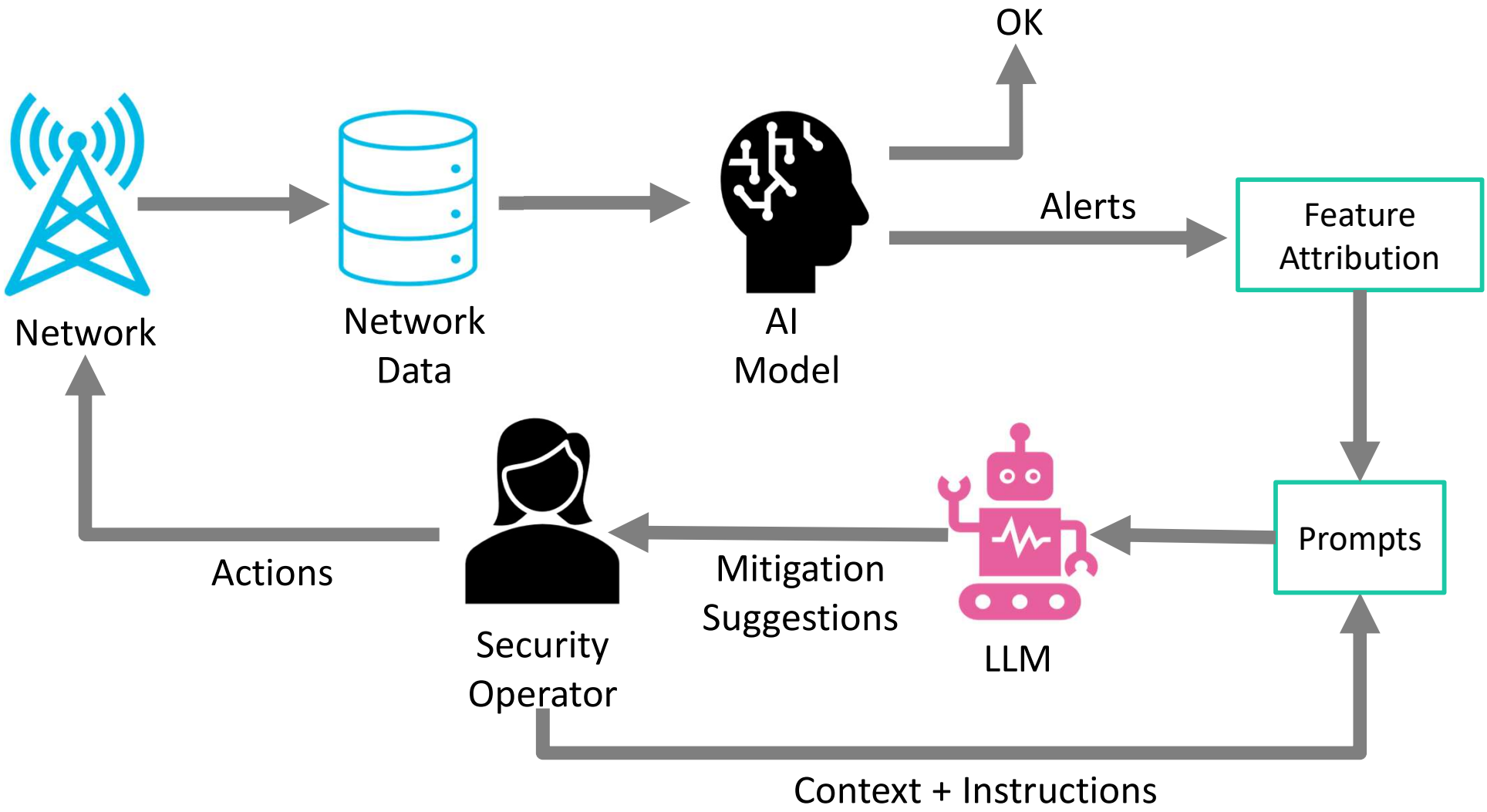
J. Törnblom, E. Karlsson, S. Nadjm-Tehrani, Finding Minimum-Cost Explanations for Predictions Made by Tree Ensembles, March 2026, https://doi.org/10.1002/spe.70061

Explanations help the human



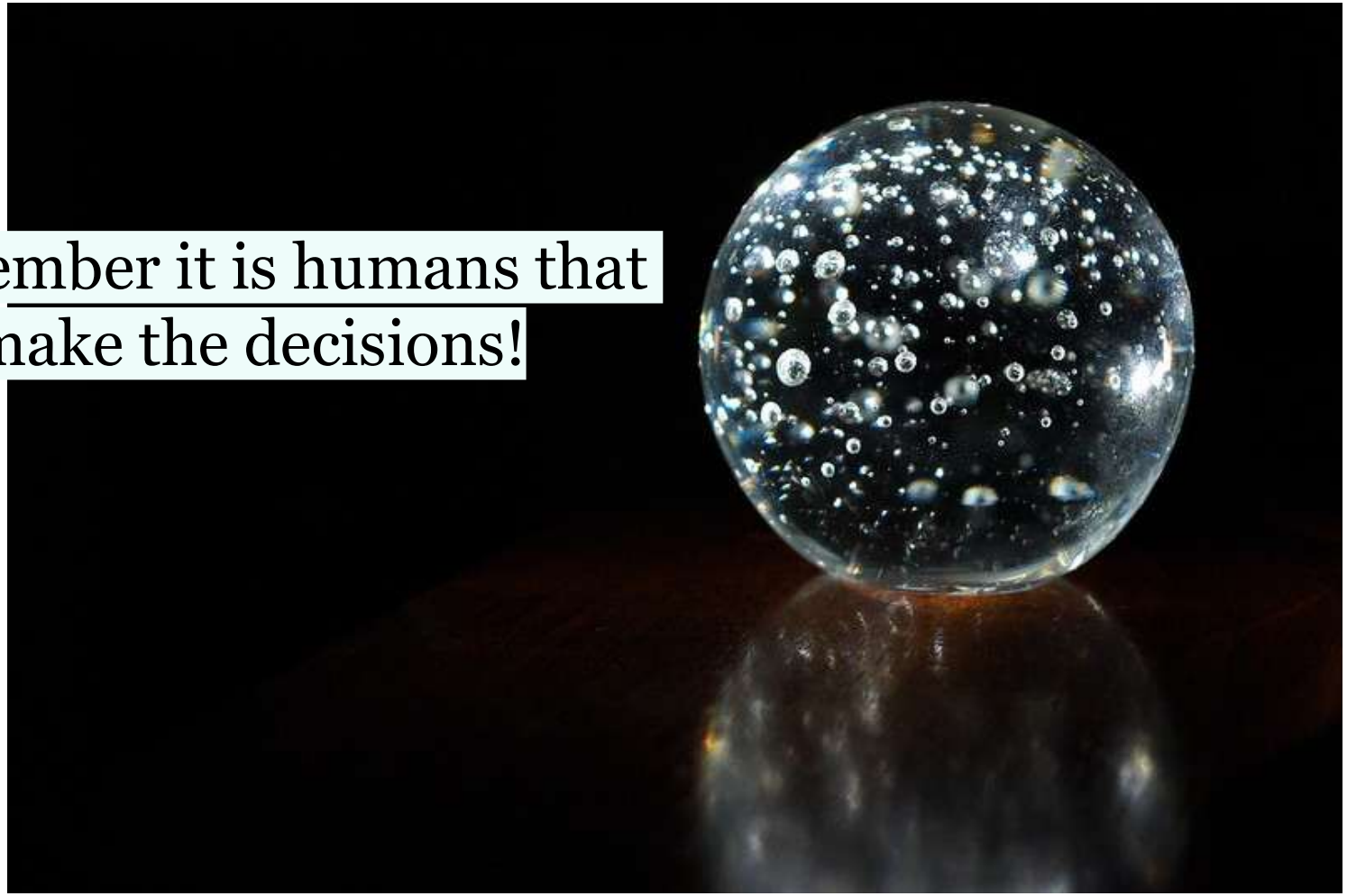


Joint work with Purdue University



Federica Uccello, et al. Mission Explainable: From Feature Attribution to Mitigation in 5G Anomaly Detection, ICNC 2026, DOI: 10.1109/ICNC68183.2026.11416967

AI or no AI?



simin.nadjm-tehrani@liu.se

New Centre: https://liu.se/en/research/resist