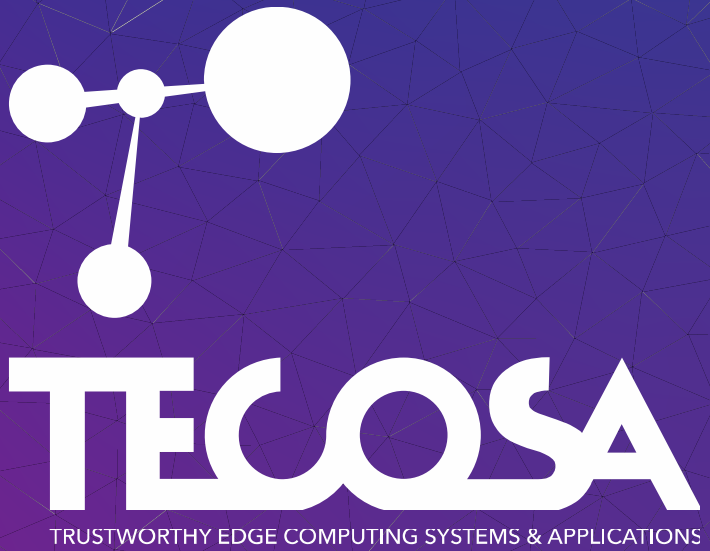
TECoSA – Trustworthy Edge Computing Systems and Applications

https://www.tecosa.center.kth.se



BY MARTIN TÖRNGREN

TECoSA - Trustworthy Edge Computing Systems and Applications - in a nut-shell

www.tecosa.center.kth.se

- A Swedish based multidisciplinary research center
  - Inaugurated March 2020, long term Swedish national funding
  - Needs driven excellent research in collaboration
  - Consortium with a growing set of industrial partners (currently 5 large and 9 SMEs) and KTH Royal Institute of Technology
  - Strong national and international networks
- Domains and focus:
  - **Critical industrial applications**
  - **Trustworthiness: Predictability, Security and Safety**
- Open for collaborations!

What's all the fuss about the edge?

(enterprise - near - far - nano - *edge*, multi-access *edge*, *cloudlets*, *fog* computing, distributed cloud, ...)

POLL

1. Its a buzz word to get new funding
2. It is really a new term for smart embedded systems – the ”device edge”
3. It is about leveraging existing and new communications infrastructure (e.g. 5G) to provide localized computation for the data and AI age
4. It is about getting close to the ”action”, leveraging advances in cloud and software engineering

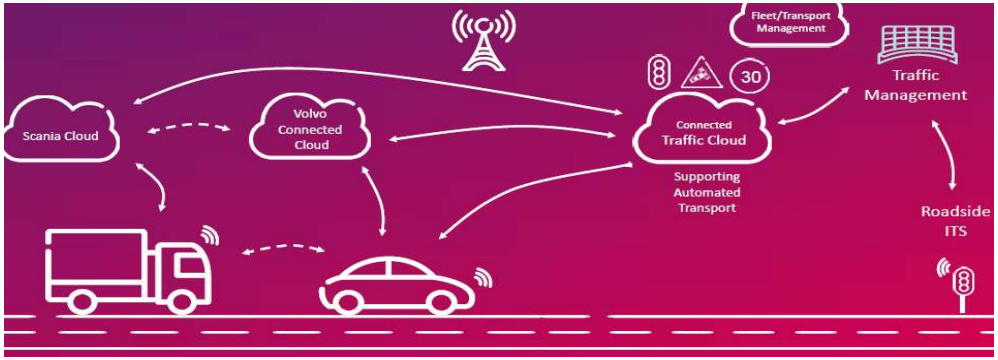
Some confusion; locality vs. technology/domains; Different perspectives

Motivation: Digital infrastructure and connectivity

- Telecommunication: …3G, 4G, 5G, …
- Smart phones/pads
- Wireless and wired communication
- Internet and cloud
- Satelite communication and navigation
- Industrial computing
- Smart devices and embedded systems

The world as a connected and SW defined distributed system

But really as a CPSoS!
with a computing continuum
(Cyber-Physical Systems of Systems)
www.hipeac.net/vision/#/latest



Courtesy of Ericsson

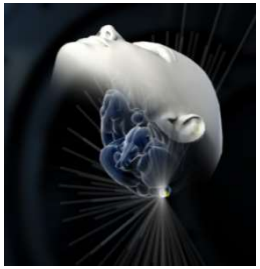
Motivation and domains: Edge computing in Industrial applications

Human-in-the-Loop

Real-time Analytics

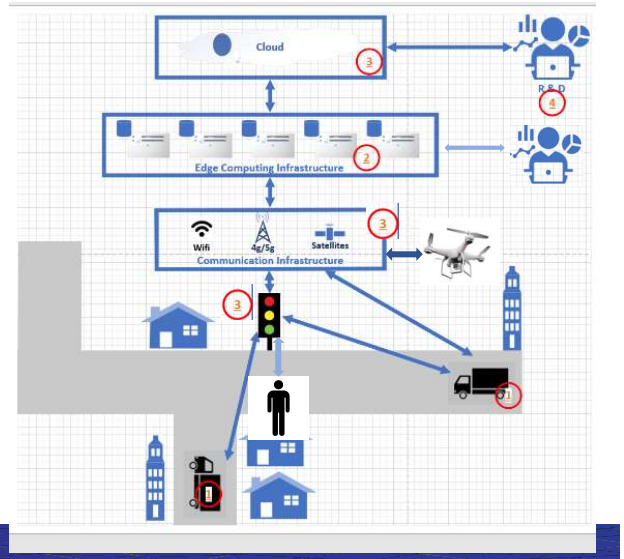
Atlas Copco

Real-time control



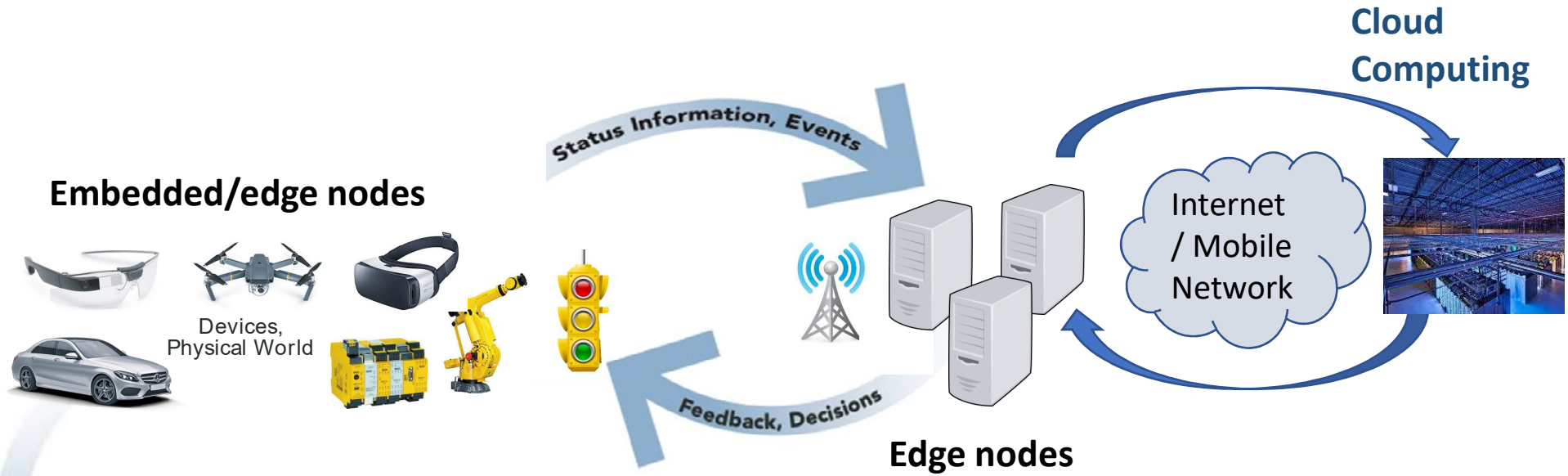
Elekta

Collaborative CPS



Leading to new demands for computing!

Focus: *Trustworthy Edge Computing Systems and Applications*



Predictability!
- Low latency
- E2e coms & computing
- Stateful management

Security!
- Secure computing
- Lightweight crypto
- Adversarial ML
- ML and confidentiality

Safety!
- Safe ML
- Prob. Programming
- Architectures
- Human-machine

Vision for TECoSA

Partners and researchers

SME's

AVASSA

Einride

Kvaser

Inkonova

RTE

Safety Integrity

Synective

Syntell

Thhink

Large companies

Atlas Copco Industrial Technique

Elekta

Ericsson

SAAB

ÅF

David Broman
Programming models, security SW Eng., machine learning

György Dan
Edge computing, resource managemen

Elena Dubrova
Security and reliab computer systems

Lei Feng
Mechatronics, supervisory ctrl, optimization, model-checking,

Elena Fersman
Machine intelligence, 5G+ architectures

James Gross
Wireless, predictab edge computing
Co-director

Iolanda Leite
Human-machine interaction, Machine learning

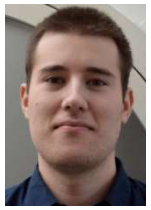
Jana Tumova
Formal methods, Artificial Intelligence

Martin Törngren
Systems engineerin safety & security, CI embedded systems
Director

TECoSA projects and people!


Oscar Eriksson


Lars Hummelgren


Daniel Lundén


Raksha (postdoc)


Lifei (Atlas)


Rusyadi


Jose

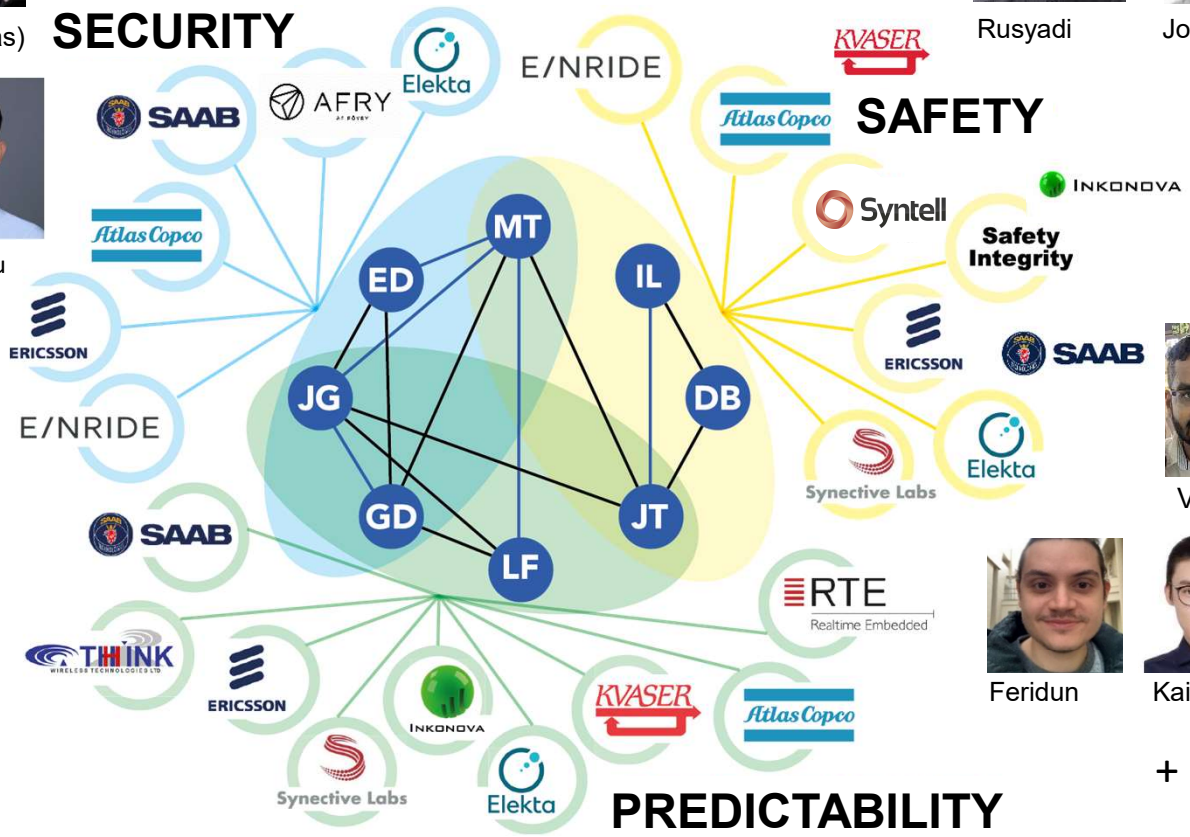

Wei


Huanyu


Daniel Marta


Michail Moraitis

More people on their way in!!




Vishnu


Nils


Samie

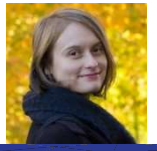
Feridun


Kaige


Andrii

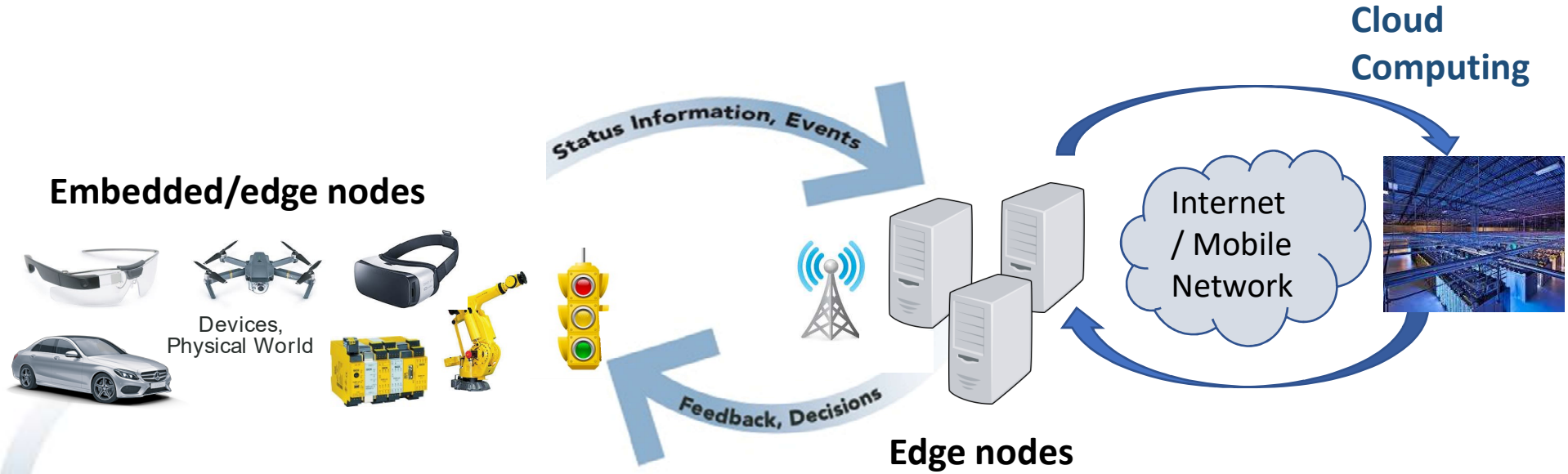

Manuel

+ Sladana



TECoSA: Industrial Digitalization

Trustworthy Edge Computing Systems and Applications



Predictability!
- Low latency
- E2e coms & computing
- Stateful management

Security!
- Secure computing
- Lightweight crypto
- Adversarial ML
- ML and confidentiality

Safety!
- Safe ML
- Prob. Programming
- Architectures
- Human-machine

Research topics (students and postdoc)

- **Safe machine learning systems**
  - Safety and Perceived Safety in Deep RL
  - Multi-Agent Task Allocation with Deep RL
- **Architecting and risk management**
  - Reference architectures for collab. CPS
  - Occlusion motion planning & risk management, for automated vehicles with edge-based enhancements

  + Risk analysis for edge based CPSoS
- **Languages and Compilers for Probabilistic Programming (PP)**
  - Correct, Efficient, and Composable Monte Carlo Inference for PP Languages
  - Semantics, Composition, and Compilation of PP and Equation-Based Languages
  - Efficient het. compilation of functional programs for mixed CPU/GPU systems
- **Optimized edge computing resource management**
  - Optimized properties for edge-based ITS (energy, performance, …)
  - Decentralized resource management for edge orchestration
- **Closed loop systems on the edge**
  - Human-in-the-Loop QualitY-of-Experience under Delays
  - Energy-Efficient Sampling of Random Processes at the Edge
  - ML-based End-to-end Latency Prediction for Edge Systems
- **Planning and communication for cyber-physical systems**
  - Reasoning and communication for autonomous CPS
  - Formal methods and AI for risk assessment and planning for multi-agent systems
- **Fault and side channel attacks**
  - Deep-learning based side-channel attacks
  - FPGA bitstream modification and reverse engineering
- **Privacy and security for machine learning**

Testbed

- Essential for “breaking new ground” – exploring solutions, technologies and their consequences
  - + A “vehicle” for collaboration
  - Multiple interests, aspects and initiatives, and engineering efforts
- Two major different aspects of edge computing testbed identified
  - Application and Infrastructure-oriented Testbed Aspect
- Plans:
  - Ramp-up 1st versions of both testbed aspects in the fall 2021
  - Seeking strategic alignment with other initiatives
  - Leverage partner equipment/ resources

TECoSA near term calendar

- November
  - LincSic interaction!
- December
  - 1st – Innovation eco-systems!
  - 2nd: Research Forum – student pitches!
  - 9th: Quarterly meeting (6th!)
  - 16th: Board meeting
- 2022!
  - 24th March! – Quarterly!
  - 2nd June – Quarterly (provisionally)

Monthly seminars:

- Dec. 2: Amy Loutfi (title to come)
- March 3rd: Hermann Kopetz
- Spring seminars being formed!

Scandinavian Conf. on System and SW Safety - Nov. **23-24,** 2021
http://safety.addalot.se/2021

6th ACM/IEEE Symposium on Edge Computing, Workshop!
Dec. 14-17; 2021
http://acm-ieee-sec.org/2021

Activities and partner involvement

www.tecosa.center.kth.se

- Open seminar series and newsletter
- Actively joining the network (”continued educ.”)
  - Tutorial and state of the art course (KTH and industrial partners)
  - Quarterly meetings and Research forum
  - Innovation eco-systems effort
  - Researcher affiliation
- Research agenda work
  - Reinitiated Dec. 2021 with an update spring 2022
  - Gathering new ideas, directions, themes (from small to large)
- Research and testbed
  - Research projects/ sub-projects
  - Industrial PhD students, adjuncts, affiliated faculty

TECoSA – Contact points

https://www.tecosa.center.kth.se

Contact: martint@kth.se

TECOSA

TRUSTWORTHY EDGE COMPUTING SYSTEMS & APPLICATIONS