WASP | WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM

WASP
Autonomous Systems and Software
2021 Kick-Off
Karl-Erik Årzén

CHALMERS UNIVERSITY OF TECHNOLOGY

KTH VETENSKAP OCH KONST

LINKÖPINGS UNIVERSITET

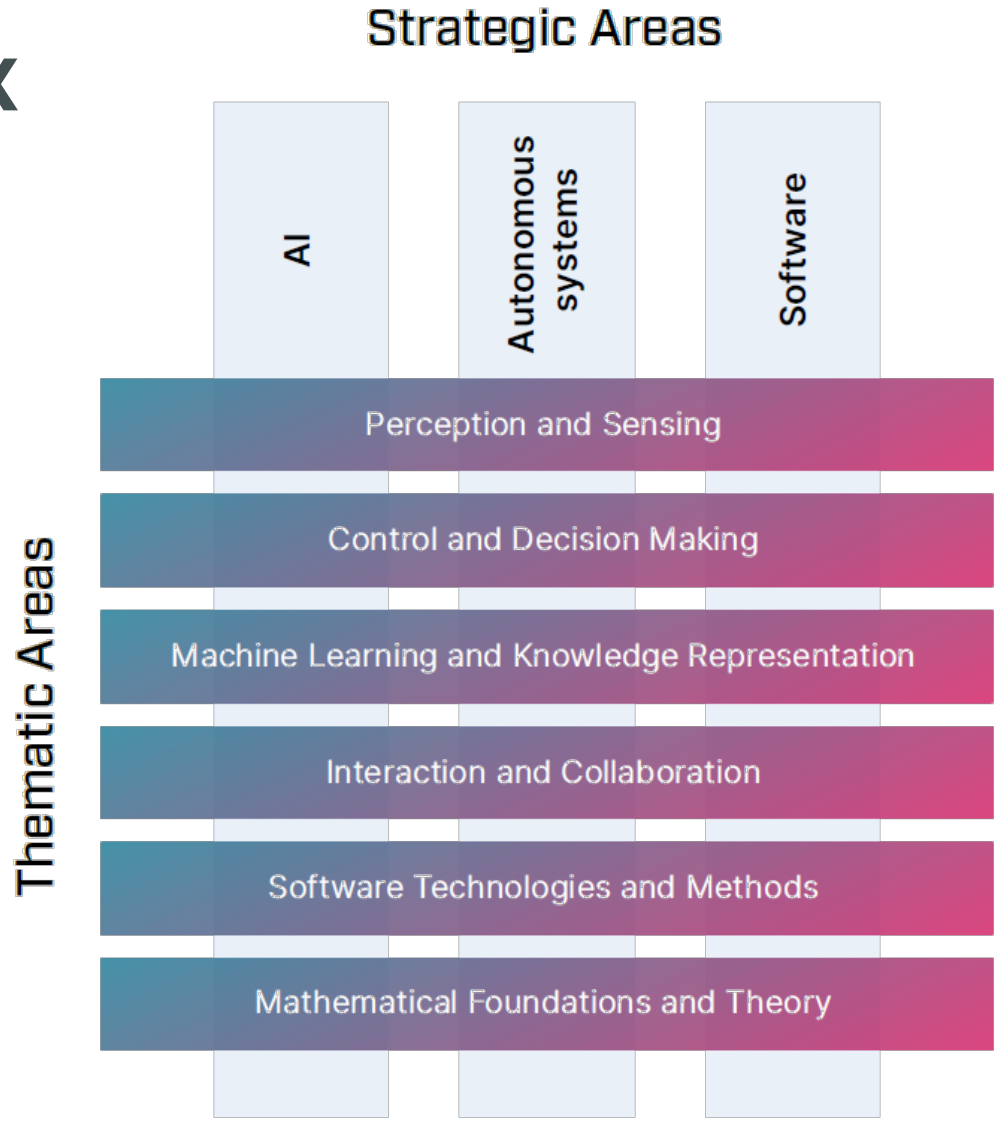
LUNDS UNIVERSITET

UMEÅ UNIVERSITET

WASP Structure

- WASP
  - Autonomous Systems and Software
    - The original part of WASP
    - AI and Machine Learning included but mainly as tools or methods in Autonomous Systems and Software
  - AI
    - Added to WASP in 2017 with substantial budget increase
    - Increased emphasis on AI and Machine Learning in WASP
    - WASP-AI/MLX
      - Focused on Machine Learning
      - Danica Kragic
    - WASP-AI/MATH
      - Mathematical Foundations of AI/ML
      - Johan Håstad

Research Matrix



WASP Autonomous Systems

- Research on autonomy, including enabling technologies for autonomous systems:
  - Transport systems, self-driving vehicles, perception, interaction, visualization, human-machine collaboration, multi-agent systems, robotics, autonomous clouds and networks, security, localization, optimization, localization, computer vision, ...

WASP Software

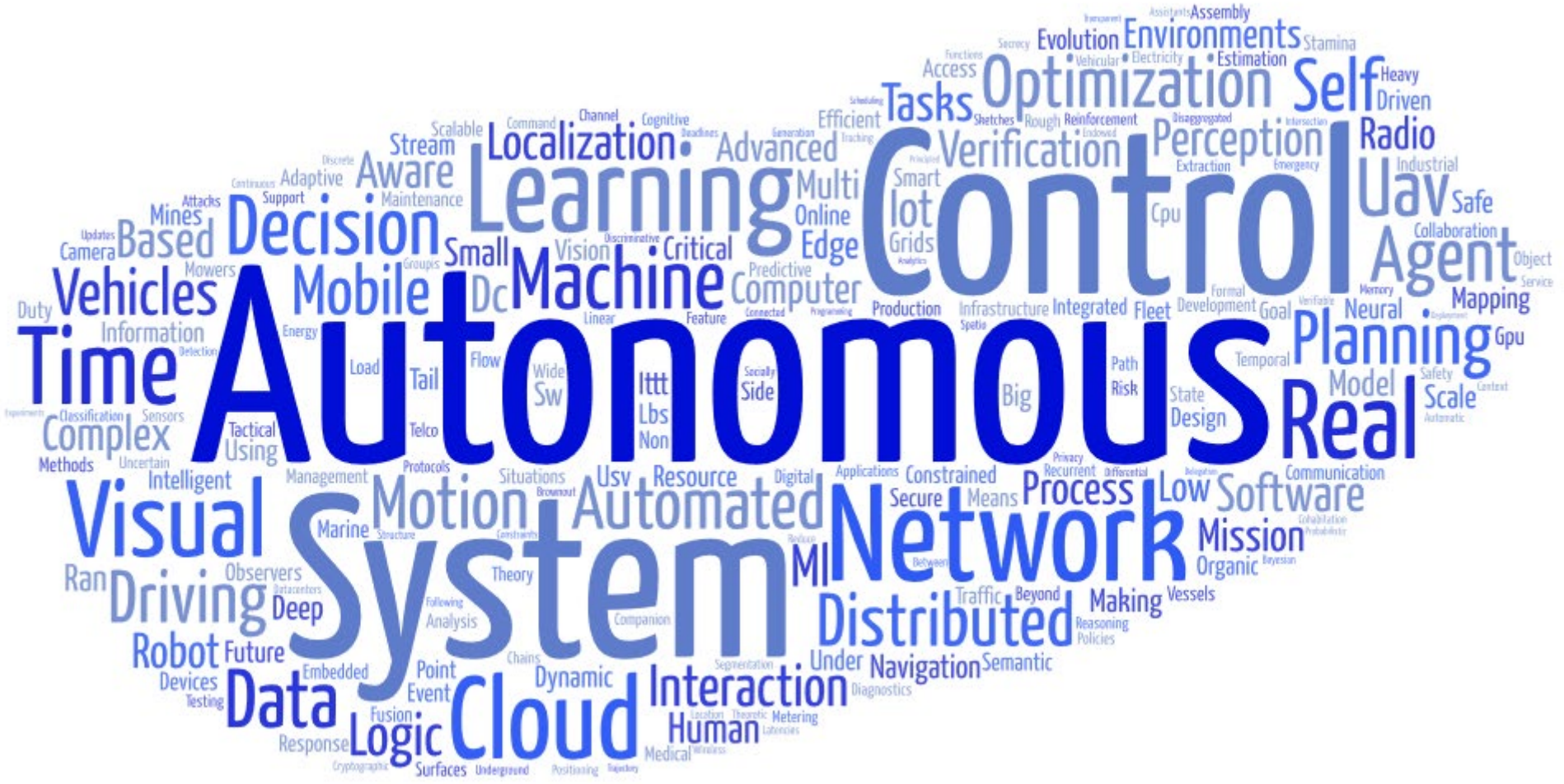
The software research in WASP falls primarily within two areas:

1. Software methodology and technology for the modeling, analysis, development, training, verification, and deployment of autonomous or AI and ML-based systems.
2. Software methodology or technology that contains or utilizes autonomy, automation, AI, learning, or feedback. This includes, for example, experiment-driven development practices, self-reflection, self-adaptive software systems, self-repairing software, and automatic programming.

In addition to this software research in the context of WARA-SW

- Will support software research on continuous system testing, static program analysis, software debloating, and automatic program repair.

What the students actually do



What the AI students actually do

Main activities so far

- Three calls for university PhD students, industrial PhD students and affiliated PhD students
- In total around 185 PhD students
  - Including 10 that have graduated
- Seven Expedition Projects
  - 17 PostDocs
- Six NTU-WASP Collaboration Projects
  - Six PostDocs
- Recruitments:
  - 7 Professors
  - 3 Associate Professors
  - a few on their way

Some Examples of Autonomous Systems and Software Research in WASP

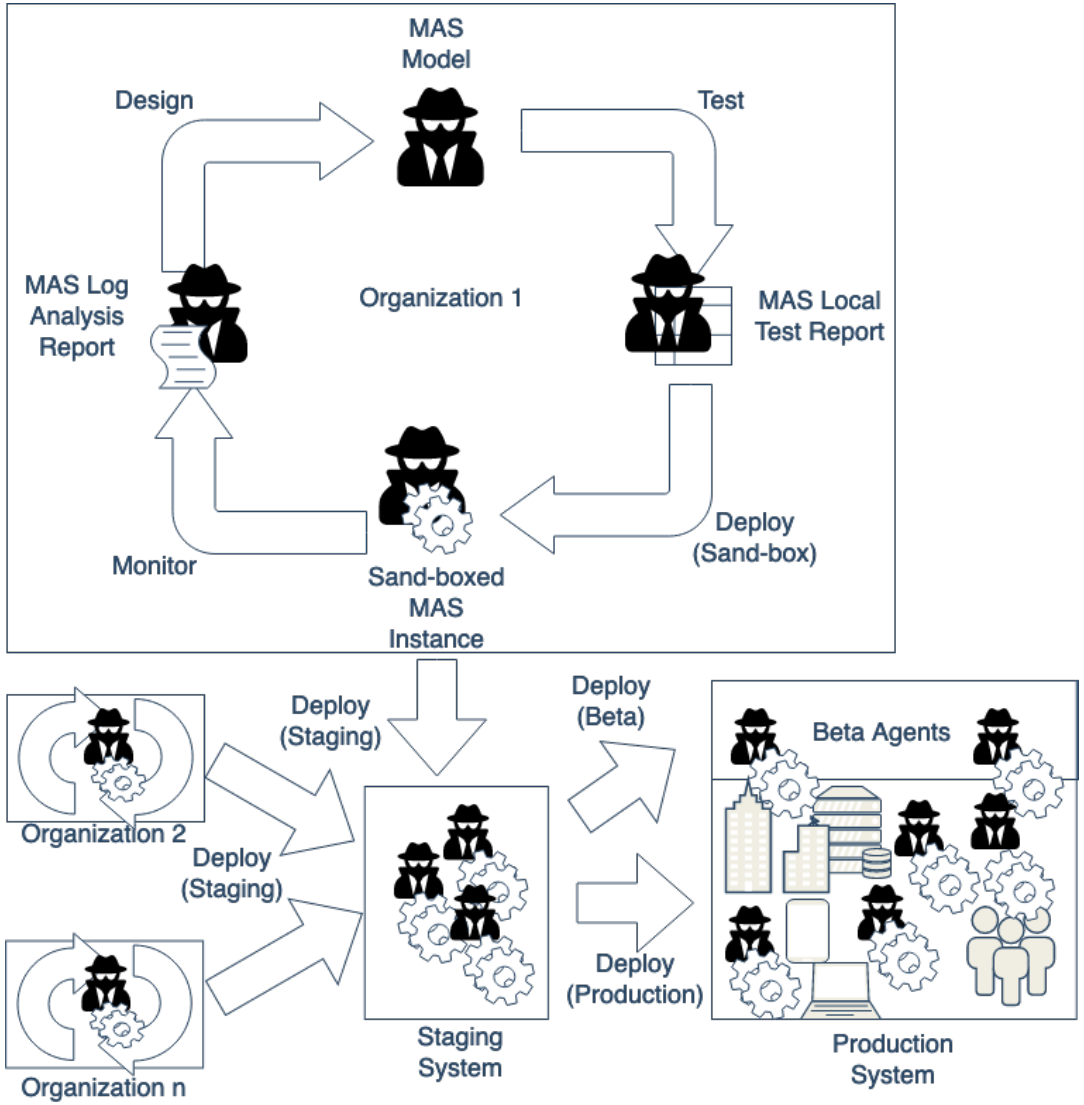
Socially Intelligent Systems for Human-Agent Collaboration

- **PIs:** Helena Lindgren, Juan Carlos Nieves (UmU)
- **Researcher:** Timotheus Kampik

- **Objective 1 (engineering perspective):** Integrate goal-driven agents and bleeding-edge automated reasoning approaches into modern software engineering processes.

- **Objective 2 (theoretical perspective):** Formally analyze automated reasoning approaches by systematically relaxing the formal properties of economic rationality.

- **Example application domains:** Healthcare, enterprise systems



Multi-armed bandits in the wild: Pitfalls and strategies in online experiments

Objective:

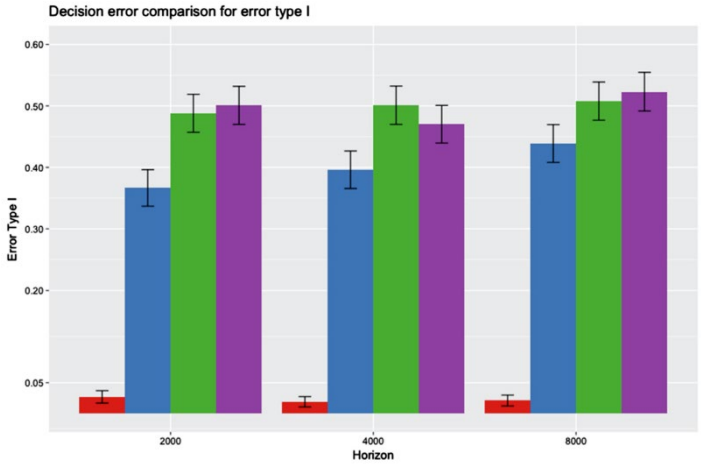
- Understand the pitfalls and restrictions of using MABs in online experiments, as well as the strategies that can be used to overcome them.

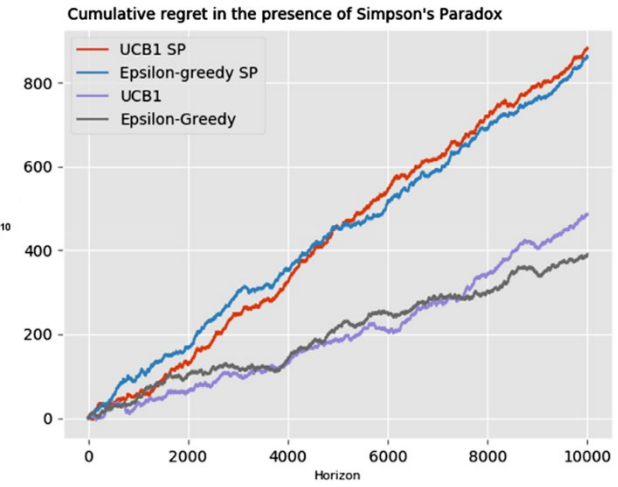
Researchers: David Issa Mattos (CTH), Jan Bosch (CTH) and Helena Holmström Olsson (MAU)

Results:

- MAB algorithms have the potential to deliver faster results with a better allocation of resources over traditional A/B experiments.
- Potential mistakes can occur and hinder the potential benefits of such approach.
- The paper and guidelines are aimed as reference material for practitioners during the design of online experiments

Mattos, David Issa, Jan Bosch, and Helena Holmström Olsson. "Multi-armed bandits in the wild: pitfalls and strategies in online experiments." Information and Software Technology 113 (2019): 68-81.





Guidelines to select and experimentation techniques.

Question	Decision
1. What is the goal of the experiment?	• Learning: A/B/n, full factorial and fractional experiments • Innovation: A/B experiments • Optimization: A/B/n experiments, sequential A/B experiments and MABs
2. What is the cost of making type I and type II errors?	• If both types of error are costly: high power traditional A/B/n and full factorial experiments • If only type I error is high: traditional A/B/n, full factorial experiments • If only type II error is high: MABs
3. How well known are the problem and the assumptions?	• If not well-known traditional A/B/n and full factorial experiments • If the system needs validation: A/B/n experiments with pre-quality tests • If well-known analysis if it matches the assumptions of different MABs ○ If the context is well understood and validated: contextual bandits
4. Is there a single decision metric?	• If there is only one metric ○ And this metric is sufficiently sensitive, MABs can be used ○ Delayed metrics and less sensitive metrics: A/B/n experiments • If there are multiple metrics that cannot be grouped in single OEC: A/B/n experiments • Short-term experiments ○ If there are external deadlines regardless of sample size: MABs ○ Otherwise: traditional A/B/n and full factorial experiments
5. How long will the experiment run?	• Long-term experiments: ○ If it is to collect a sufficient sample size: A/B experiments ○ If there is no user-consistency requirement: MABs ○ If it is to adaptively change the variation with time: contextual bandits and non-stationary bandits

Measuring and Understanding Performance in Infrastructure- and Function-as-a-Service Clouds

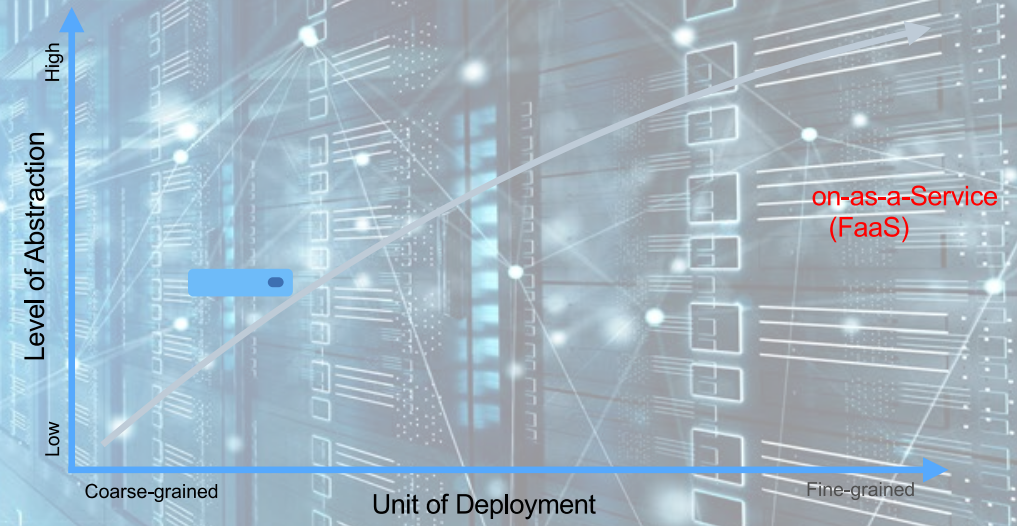
Objective: This project systematically quantifies performance in cloud environments and leverages this understanding to propose solutions for building performance-optimized cloud applications.

Researchers: Joel Scheuner (joelscheuner.com), Philipp Leitner (Chalmers) in collaboration with SPEC Research (https://research.spec.org/)

Problem: The persistent growth of established cloud services, such as Infrastructure-as-a-Service (IaaS), and the emergence of new services, such as Function-as-a-Service (FaaS), has led to a large diversity of cloud services with different performance characteristics.

Methods: Quantitative and qualitative research methods are used to guide performance-optimal cloud service selection, including experimental research, artifact analysis, and literature review.

Evolution of Computing Services



GPS-level accurate camera localization with HorizonNet

- **Targeted problems:** Localization for autonomous naval surface vehicles need to be independent of GPS, which is prone to attacks. The paper develops several steps to solve this challenging problem using images from autonomous boats using elevation models of the archipelago.

- **Researchers:** Bertil Grelsson (LiU/Saab), Michael Felsberg (LiU) and Gabriel Eilertsen (LiU)

- Methods tested in the WARA-PS arena

Data and model introspection for machine learning

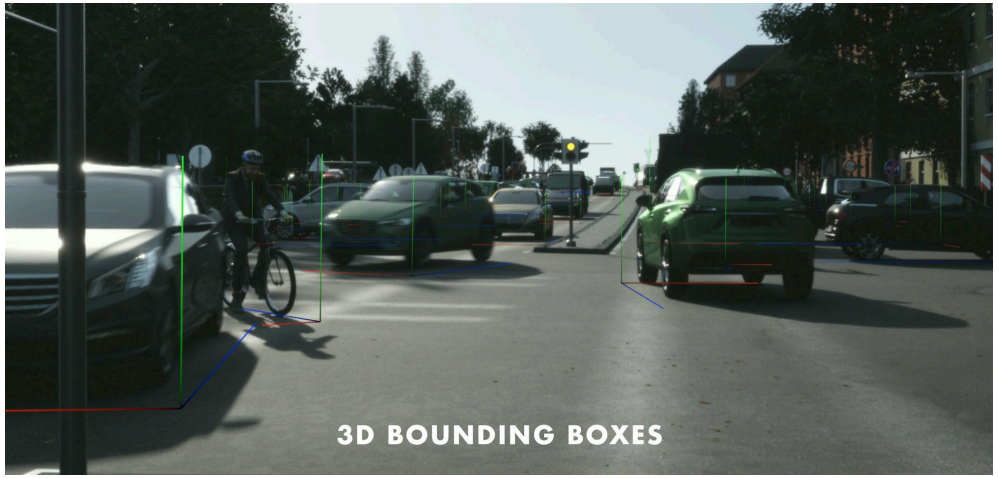
Objective:

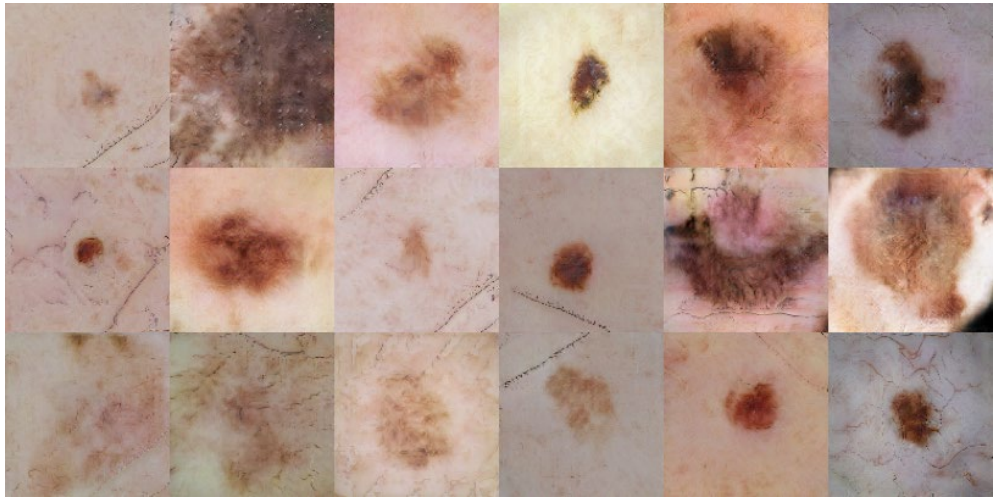
- Develop methodology for the generation of synthetic data for training and evaluation of machine learning algorithms.
- Develop tools for quantifying the information content in a data set and representations in which data sets can be compared to each other.

Researchers: Karin Stacke and Apostolia Tsirikoglou, Jonas Unger (LiU) and Gabriel Eilertsen (LiU)

Targeted problems:

- Develop tools for analyzing the weight space of the trained model and how the model evolves during training using different hyper-parameters and data.
- Develop methods for generating synthetic data using both direct simulation and generative models (GANs).
- Applications for autonomous vehicles (street scene parsing) and applications in the medical domain (digital pathology).





Examples of synthetic data for (top) street scene parsing and (bottom) detection and classification of skin liaisons.

5G mmWave SLAM for vehicular localization

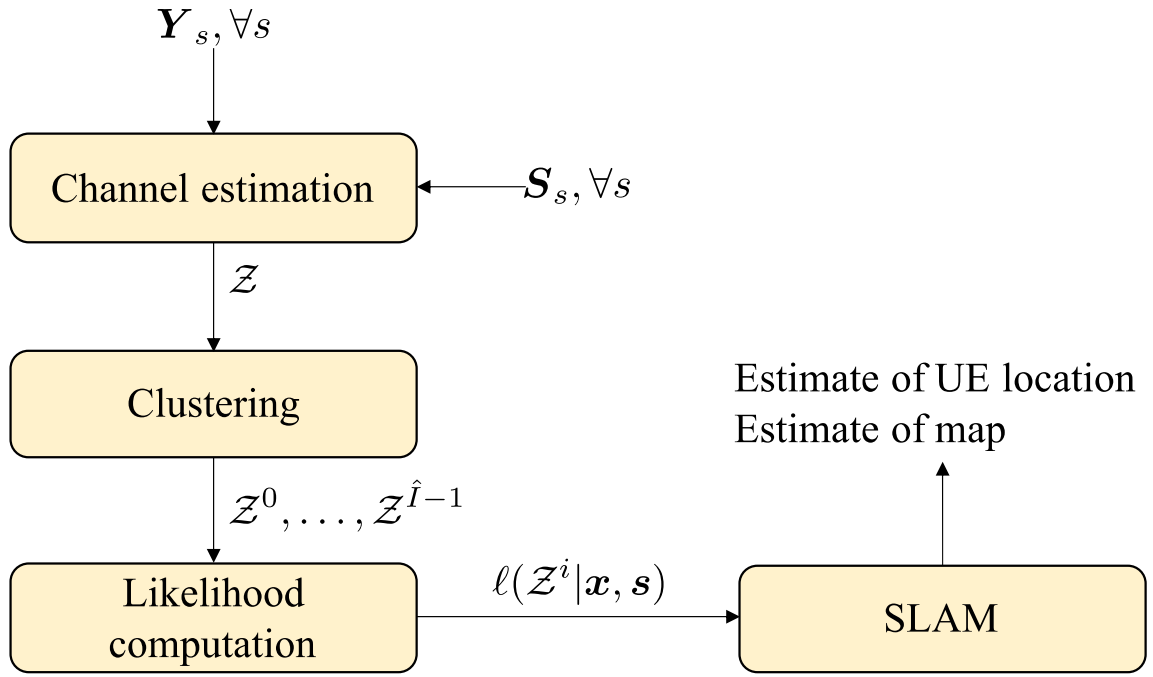
Objective:

- Develop an end-to-end framework for 5G SLAM, which can utilize 5G signals to localize the users and map the surrounding environment.

Researchers: Yu Ge, Henk Wymeersch, Lennart Svensson (Chalmers)

Targeted problem:

- 5G mmWave communication is very useful for localization and mapping, due to its geometric connection to the location of the user with respect to the base station.
- 5G mmWave signals from the base station can reach the user via multiple propagation paths.
- We are developing algorithms for solving the end-to-end problem, including four phases: downlink data transmission, multi-dimensional channel estimation, channel parameter clustering, and SLAM filter with a novel likelihood function.



Integrating motion planning and control

Objective: To combine state-of-the-art methods from motion planning and (optimal) control to develop improved algorithms and theory in terms of computational performance, solution quality and reliability.

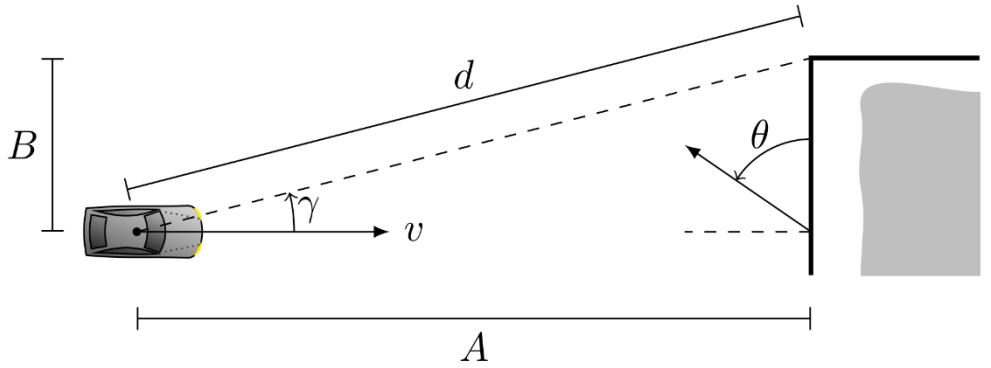
Researchers: Kristoffer Bergman (industrial PhD student Saab Dynamics) & Oskar Ljungqvist (Ph.D in May 2020), Daniel Axehill (LiU)

Targeted problem: There exist many powerful theoretical and algorithmic tools in control that have a large potential in the closely related area of motion planning. There also exist efficient algorithmic tools in the area of motion planning that are useful for (optimal) control. Can tools be exchanged between these two areas and be combined into new, even more powerful, tools?

Autonomous Avoidance Maneuvers At-the-Limit of Friction

Problem: Safety maneuvers are fundamental
- ABS does not require prior information about the road friction.
- What about passing maneuvers?

Background: For a simple single-mass model the optimal avoidance control is a constant acceleration/force vector in a fixed coordinate system (not vehicle centered).
- Similar is shown for a double track model with load transfer!



Victor Fors, Björn Olofsson & Lars Nielsen (2020) “Attainable force volumes of optimal autonomous at-the-limit vehicle manoeuvres”, In Vehicle System Dynamics, 58(7):1101--1122.

Victor Fors, Björn Olofsson, & Lars Nielsen (2019) “Formulation and interpretation of optimal braking and steering patterns towards autonomous safety-critical manoeuvres”. In: Vehicle System Dynamics, 57(8):1206--1223.

Result: A controller capable of handling situations close to the limit of friction
- without any estimation of the friction.
- low computational demand (all computations are explicit).

Victor Fors, Björn Olofsson, Lars Nielsen. “Autonomous Wary Collision Avoidance”. Under journal review.

Architectural consequences: Indicate low-level (safety) control should be
- environment centric rather than vehicle centric.
- acceleration/force based rather than path planning and path following.

Post doc: Victor is invited as a postdoc to Chris Gerdes at Stanford.

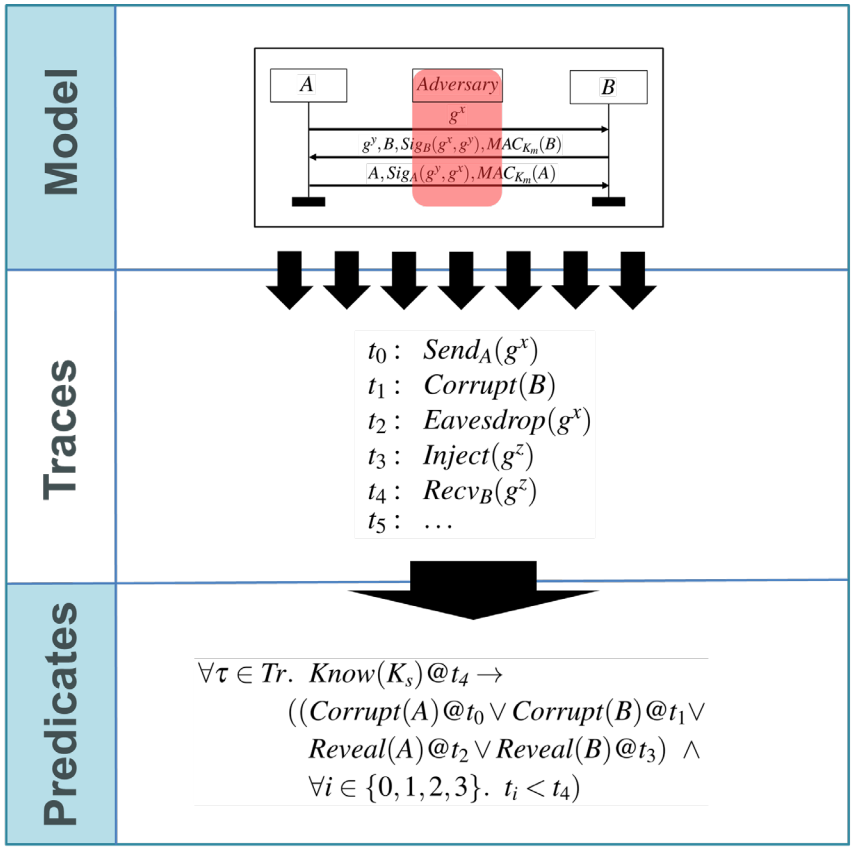
Video showing avoidance control

Secure Cryptographic Protocols and Systems

- **Objective:** Develop protocols for secure communication and methods for designing them with high security assurance levels for 5G mobile networks and IoT devices

- **Researchers:** Karl Norrman (KTH, Ericsson), Mads Dam (KTH), Ben Smeets (Ericsson)

- **Targeted Problem:**
  - Cryptographic protocols are essential for the security of current and future communication infrastructures.
  - Producing properly validated and verified cryptographic protocols is, however, a highly delicate and error-prone task. Tools and systematic methods are needed to aid protocol engineers.
  - We develop both the security protocols themselves and methodologies and theory for defining what security means in different settings, and how to ensure that a given protocol formally meets those definitions and criteria.
  - Part of the project, developing a secure federated learning solution for 5G, is a cross-cluster activity between the security cluster and the ***AI and ML for AS*** cluster



Engineering Trustworthy Self-Adaptive Autonomous Systems

Objective:

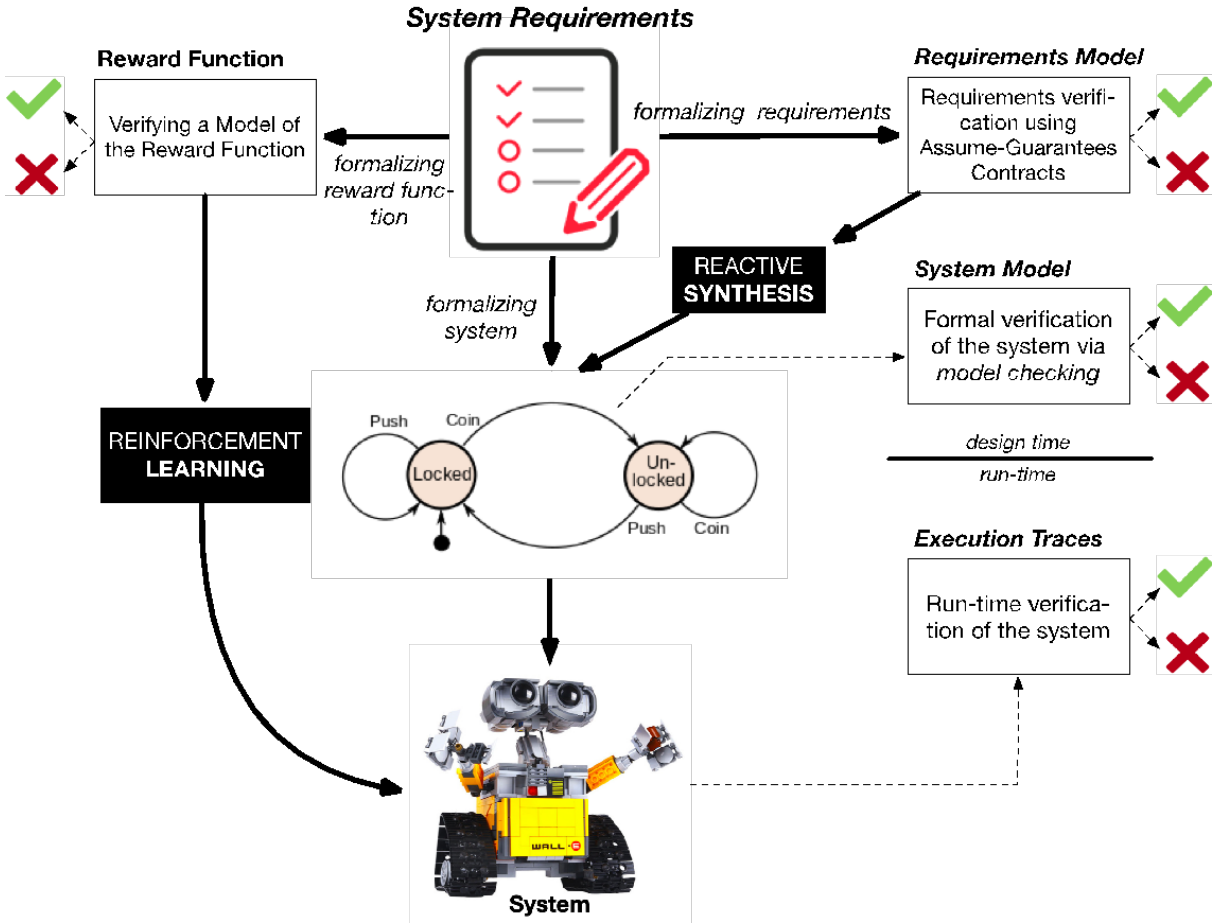
- Engineering Trustworthy Self-Adaptive Autonomous Systems

PhD student will graduate in 2020

- Piergiuseppe Mallozzi (advisor Patrizio Pelliccione)

Targeted Problems:

1. Formalizing system requirements
   a) As assume-guarantee contracts and verify consistency and completeness
   b) with reward functions that train a reinforcement learning agent to achieve its goals
   c) with formal models (e.g. timed-automata)
2. Verifying system requirements
   a) by model checking a formal model of the system
   b) by generating a correct-by-construction model via reactive synthesis
   c) by monitoring the execution traces of the system



New Cluster Structure

Cluster types

- Core Technology Clusters
  - Focus on some core technology, theory, tool, or method that several PhD students are interested in and need to learn more about.
  - Managed by PhD students
- Application Clusters
  - Gather students and WASP faculty that work with the same application.
  - Managed by WASP faculty
- Area Clusters
  - Gather students and faculty that are interested in a particular technical area.
  - Managed by WASP faculty

Cluster Selection Form

- Email with link for selection sent out Jan 5
- Deadline for selection Jan 20
- Cluster participation is voluntary
- Filling in the selection form is mandatory