85th IFIP WG 10.4 Meeting

Summary for Session 5 - Industry Panel

Long Wang (Tsinghua University)

Feb. 3, 2024

Assessing and Mitigating Risk in Dynamic Environments for Safe Driving

- Saurabh Jha, IBM
- Autonomous Driving is not safe enough yet
  - AVs 15-4000x worse than humans
- Proposal
  - Ensuring safety with inter-actor interactions
  - Human's intuitions of using backup plans (escape routes)
  - Design risk metric that captures escape routes
- Preliminary results show significant reduction in accidents

Trustworthy AI in the Bot & Fraud Space

- Yi Han, F5
- Use of AI for bot & fraud detection and mitigation
  - 65%-85% recall
- LLM-backed automated code implantation
- AI Engine
  - Real-Time ML, <= 20ms
  - GNN

Challenges of Using AI in Automotive CPS

- Ramon Serna Oliver, TTTech
- CPS operations from fail-safe to fail-operational
- focusing on the timeliness issue of autonomous vehicles
  - Design should be mathematically proven to meet time deadline
  - Global system planning
  - Number challenge: with growing system size, it is challenging to plan when/where software executes
  - Challenges in integrating timeliness into AI-based systems: AI accelerator management

Open Discussion (1)

- AI systems as copilot, as it is, say, 99% reliable
  - 100% is very difficult to achieve
- Specification is key for AI systems
  - What if AI does not do its mission?
  - Specification should depend on the fault domain/use case.
  - Specification is important also because of the CPS part of the system
- Have to have a plan B when AI system fails
- The reliability is not only that of AI and the system (car), but also the reliability with the user counted in
  - Particularly when AI is used as copilot
  - Should also consider the risk a human feels

Open Discussion (2)

- From the driver’s view, from L2 to L4 (L3 does not have an important position)
  - L2 requires the continuous driver's attention
  - L2+ and L4 allows the driver to be some kind of disengaged
  - Either L2 or L4, because either continuous driver's attention or no need for driver's attention
- Dealing with customers’ privacy (e.g. in GDPR) in AI-enabled systems
  - Not all signals or data are related to privacy
  - Generally, user data should and can be removed upon the user’s request
  - How to remove data from AI models which already learned the user data?