Autonomous Vehicle Safety and Security: An Information Processing Imperative

Our distinguished panelists

Background

- **Panel organized** by members of the **Intelligent Vehicle Dependability and Security (IVDS)** project of IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance
- **Co-organizers**
  - Homa Alemzadeh, University of Virginia, US
  - Jay Lala, Raytheon Technologies, US
  - Chuck Weinstock, SEI Carnegie Mellon University, US
- **IVDS Project**
  - Various activities since its initiation in 2019, including
    - Publication of viewpoints in professional and public media
    - First IVDS Workshop (virtual), held January 2021
    - This panel

WG 10.4 Concern with Autonomous Vehicle Safety and Security -- Why?

- Since its founding in 1980, this WG has been engaged with
  - identifying and integrating methods for achieving highly dependable computer systems and networks
  - this includes all aspects of a system's evolution from specification through deployment
  - many of the applications involve safety-critical autonomy
- Realization of dependable (especially safe) intelligent autonomous road vehicles is therefore well-suited to experience within the WG, precipitating the IVDS project
- More generally, this is an information processing imperative for a myriad of ICT disciplines under the IFIP umbrella

Conduct of the Panel

- Remaining time will be evenly divided (roughly) between
  - Opening remarks by panelists
  - Moderated discussion among panelists (followed by a poll of the audience)
  - Q&A between audience and panel members
- Throughout the session, feel free to ask questions using the Webinar's Q&A
  - **Please address each question to a particular panelist**
  - Selected questions will then be answered during the Q&A period
- At the end of the session, you will be invited to continue your participation via a Slack channel and a mailing list

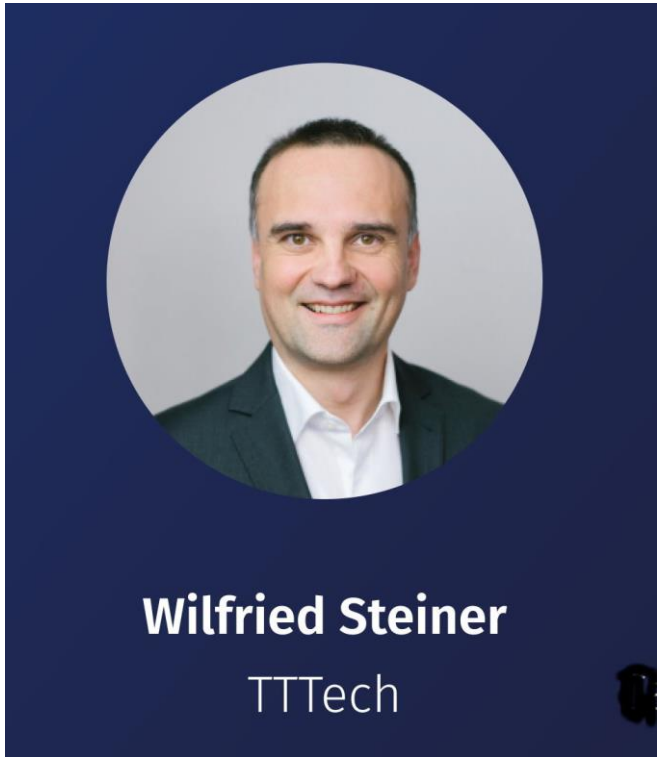
Dr. Philip Koopman

- Professor
- Department of Electrical and Computer Engineering
- Carnegie Mellon University, US

Removal of Human Driver & Deployment Governance

- No human driver in a fully automated vehicle (AV)
  - Automation must handle #DidYouThinkofThat? surprises
  - No human to blame for failures
  - Beware the moral crumple zone
- Deployment governance is a pressing ethical problem:
  Who decides when it is time to deploy?
  - Companies have existential pressure to hit milestones
  - Current AV regulations take company's word for safety
  - Industry push-back on standards, e.g. testing safety (SAE J3018)

Dr. Wilfried Steiner



- Director
- TTTech Laboratories
- TTTech Group AG, AT

The Need for a Conceptual Architecture in Autonomous Driving Systems (ADS)

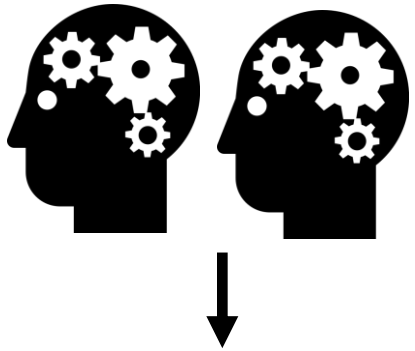
- ADS are highly complex b/c of environment, dependability, security.
- They must be fail-operational – to continue operation upon failure.
- Fail-operational system design is non-trivial as many components (software, chip, hardware, network, I/O) may fail in many ways.
- A Conceptual Architecture (CA) is key in solving this problem.
- CA decomposes the ADS in Fault-Containment Units (FCUs). FCUs fail as a whole and independent. CA also defines FCU interactions.
- ADS properties are ensured in two steps:
  i. Analysis on FCU-level shows that the system-level properties hold.
  ii. Analysis shows that a concrete system is a refinement of FCU abstraction.

Dr. Mary (Missy) Cummings

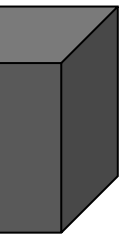
- Professor
- Department of Electrical and Computer Engineering
- Duke University, US

The Myth of All-Powerful AI

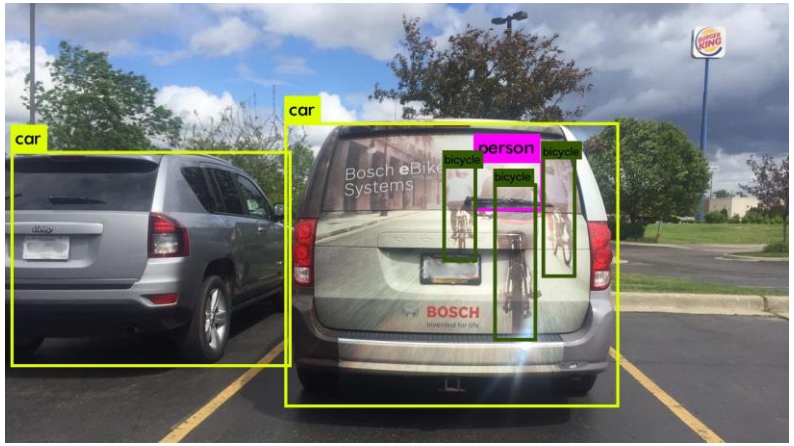
- Which algorithmic approach should I choose?
- How do I set parameters?
- What labels should I choose & where are my thresholds?



1011
1101
1001
1010
…



- How do I interpret the results?
- How do I adjust various parameters for the “best” sensitivity?



- How do I certify this system as safe?

Dr. Ravi Iyer

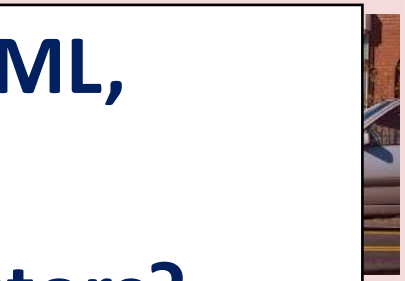
- Professor
- Departments of
  - Electrical and Computer Engineering
  - Computer Science
- University of Illinois at Urbana-Champaign, US

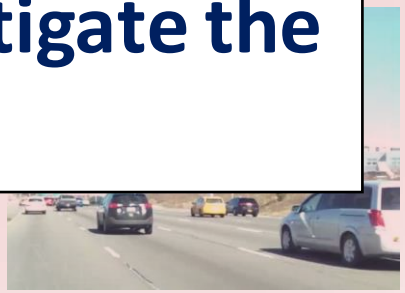
Watch out for the risky actors: Dynamically assessing and mitigating risk

Driving Scenario

- How do we identify safety-critical faults in ML, software and hardware?
- How do we identify safety-critical (risky) actors?
- How do we quantify rate of change and mitigate the risk at runtime (<100ms)?

Driving/trajectory propagation





Temporal propagation

Poll

- To get all of you more involved prior to the Q&A, we'd like to conduct a poll concerning the use of safety-related functions (features) in Level 2 **Advanced Driving Assistance Systems (ADAS)**.
- Such functions include adaptive cruise control, lane keeping assistance, automatic emergency braking, blind spot warning, etc.
- ADAS also provides functions that are conveniences such as automated parallel parking – these are **not** being questioned.

Follow-up

- If you are interested in continuing today's discussion, we have set up a **Slack channel workspace** and a **mailing list** to join for this purpose
- These are accessible via the link bit.ly/ifip60-ivds
- Please note this now if you wish to join these for immediate follow-up when this session closes
- This link will also be sent to you in a follow-up email from us via our IFIP coordinators sometime next week

Wrap-up

- Again the follow-up link: bit.ly/ifip60-ivds
- **Sincere thanks** to all involved in the **organization of** and **participation in** this event
  - Our IFIP coordinators
  - Our panel organizers
  - Our distinguished panelists
  - And our audience, whose size and active participation were necessary conditions for the success of this panel session