BREAKOUT DISCUSSION ON SAFETY AND DEPENDABILITY

SHIGE WANG (GENERAL MOTORS)
YASER P. FALLAH (WEST VIRGINIA UNIVERSITY)

Goals and Approaches

- Defining safety goals and achieving safety goals
- How to define or quantify safety (to set target levels)? How is that related to eventual system design
  - Understanding societal expectations for safety
- Different transportation domains will have different requirements, and solutions (trains, airplanes, vehicles)

New Safety Issues, Heterogeneity of The Transportation System

- **New hazards and unforeseen situations due to autonomous driving,** mixed autonomous and manned driving, (**Heterogeneity of the system**)
  - How do we relate this to safety goals/targets that are defined using current data/systems/understanding.
  - Driver behavior will be different from what we know today
  - Drivers are not particularly trained to take over in situations where the automated (part of the) system fails.
  - Heterogeneity sources: automated/non-automated , different manufacturers, pedestrians, bikes, vehicles will share the road…

Failure and Uncertainty

- **Failures and uncertainty have many sources**, how do they impact overall safety
  - How to quantify or identify the impact of these failures on the certifiability of a design, assuming design correctness (failure sources: mechanical components, sensors, communication)
  - Uncertainty in “human” related models are even more . Average driver is not the target of many safety systems,

Modeling, Model unification or integration

- We are dealing with a system of systems, with uncertainty in multiple levels
- Models, specifications and target quantities for different components (also levels) of the system are already defined in different "languages", how to **integrate** ?
  - Safety and dependability properties should be defined at all of these levels

Software

- **Software dependability, Confidence in software** (would model-based design help here?)
  - Software design methods -> so that software bugs should never be an issue
  - Verification and certification -> to certify the correctness of the design and not the correctness of software
- Security/Privacy impacts and implications on safety and dependability

Testing, evaluation and certification

- **Testing, evaluation and certification** of safety **systems** (events are rare),
  - can we design testing strategies or set of tests that a system should pass before being certified.

Potential Research Strategies:

- Simulation, co-simulation models for testing and verifying designs
- Modeling and specification methods/languages, model **unification**
- Model Based design – are the models too simple, too abstract now?
- Fault tolerance methods, at multiple levels

PLEASE EMAIL

Shige.wang@GM.COM

If you want to add anything please email us

yaserpf@gmail.com

Shige.wang@gm.com