Session Summary: Safety Assurance

Computer Science Laboratory
SRI International
Menlo Park, California, USA

Talk 1: Johan Karlsson, Chalmers

- Safe and Unsafe Disagreement in Vehicular Ad-hoc Networks
- Example: Virtual Traffic Light (VTL)
- Implement using group membership, leader election
- Number of participants unknown
- Despite strong assumptions, oracle, rather weak results and guarantees
- Question: instead of oracle, would some other infrastructure function be more useful?
- Question: is there a better way to implement VTL?

Talk 2: Jonny Vinter, SP

- Assessment and Certification of SEooC Components
- SEooC: Safety Element out of Context
- Compositional safety assurance through safety contracts
- Example: Green Cruise Control
- Described impact on ISO 26262
- And tools they have developed
- Question: hazards(A) + hazards(B) = hazards(A+B)?
- Also described SHADES HMI project
- Inject failure, what do drivers do? Not well!
- Question: how to coordinate transfer of control to out-of-loop operator on failure?