Scenarios and architecture world-café table

The topic of this table is the role of scenarios, assumptions and architecting for safety assurance. To concretize the discussion, the discussion was based on a case study on whether highly automated vehicles need an independent active safety (crash avoidance) system. According to the safety reports of Waymo and GM Cruise, Cruise has a crash-imminent braking system calibrated to work as a backup to the self-driving system; while Waymo claims that it is equipped with a series of redundancies for critical systems, such as sensors, computing, and braking. Therefore, the discussion was mainly about the evaluation and comparison between system level redundancy (Cruise's approach) and component level redundancy (Waymo's approach).

Main discussion points:

- **Which is better?** Almost everyone agreed that this is not a simple question and it should not have a binary answer. The brief agreement after the discussion is that the independent safety channel can be considered as an architectural pattern but the decision of the final architecture should be based on the risk analysis.
- **Independency between the two channels.** In the system level redundancy approach, it should be assumed that the nominal channel has better perception performance for most of the cases. During the discussion, the majority believes that the two channels should not share sensors. They also believe that independent development is important but it is difficult to define independency between different sensor pipelines. Several people also pointed out that the negotiation (or arbitration) between the two channels will be a challenge.
- **Experiences from avionic domain to draw upon.** Experts from avionic domain mentioned that in avionic systems, it is normal to have redundant controllers sharing the same sensors and actuators (similar to the simplex architecture). In addition, they also mentioned that most people in avionic domain believes that comparing to human pilot, autopilot makes better decisions but worse perception. In other words, most of the mistakes made by the autopilot were caused by the flaws on the perception.