# Meeting with Arash 01-23-2017

Below we can find the notes of the meeting with Arash. These are not grouped.   
  
1. Regarding the steering HARA, Arash mentioned that 0.3 s reaction time might be too optimistic. He suggested to also include the maximum amount of steer torque that a driver can apply.  
  
2. Arash doubts if controllability 1 is correct. If we think so, we should make sure that we perform validation checks on the assumption of reaction time. This needs to be explicitly recommended to NXP for future research!

3. REPORT: change “FSC” to “partial safety case”, since now it is more than an item definition.   
  
4. For the HARA Arash mentioned to follow a checklist. This checklist consists of 6, 7 statements regarding the input, output AND process.   
(e.g. too much, too little, too late, too soon, no.. etc) (search for the remaining ones !)  
  
5. If there is actual communication between blocks/functionalities in the architecture then checking the arrival of data is correct. However, if it is software on the same CPU, then checking arrival does not make sense.   
  
6. It is recommended to show in the architecture which combination of blocks run on the same CPU (@Davide: image processing versus control)  
  
7. We should add extra safety measure to the message itself. This can be for example, “the message can determine its priority on the line” or “lane detection signal should be transmitted via this connection ….”  
  
8. We should split requirements and decomposed requirements. They should not be build up by means of AND, OR statements. (e.g. shut down and warn the driver…., send and check correctness….)

9. REMARK: Decomposition is not really obliged. It is recommended to do so, since this reduces the testing costs of your final system.   
  
10. It is indeed not allowed to run ASIL C hardware on an ASIL B component. 🡪 Lane detection algorithm not allowed to run on the NXP bluebox. So we need to further decompose to reduce the ASIL level further.   
  
11. REMARK: decomposition happens on the requirements, not on the blocks!  
  
12. We should make a FSC for each individual safety goal.

13. Example of TSC:   
 TSRs can be split in hardware and software requirements. These are derived from the FSRs.   
  
 e.g. FSR: The message should be sent from…. To …  
 🡪 TSR: 1. parity check  
 2. Acknowledge  
 3. ……….   
14. The HARA is always checked by an external company. Furthermore, each ASIL D FSR should also be checked by external companies.

15. It can be a safety state/mechanism to come to a degraded functionality. For the ALC system an example can be:  
 if you have redundant cameras and one fails. Then switch to ALKA.   
or   
 when the actuator fails, switch to LDW  
  
16. A typical way for latent fault checking is memory checking after initialization.

**Anshuman:**

17. If we desire we can place requirements on external systems like steer actuator as well.

18. ASIL of off shelf components in ISO part8.9 or 8.12.

**Sharad:**

19. The communication message gets the same ASIL level that of the highest elements from receiving component.

20. Actuator shouldn’t be part of FMEA.