



Support for amendments to UN R79 to
allow approval of ACSF, in particular LKA
and LCA

Mervyn Edwards, Matt Seidl on behalf of EC

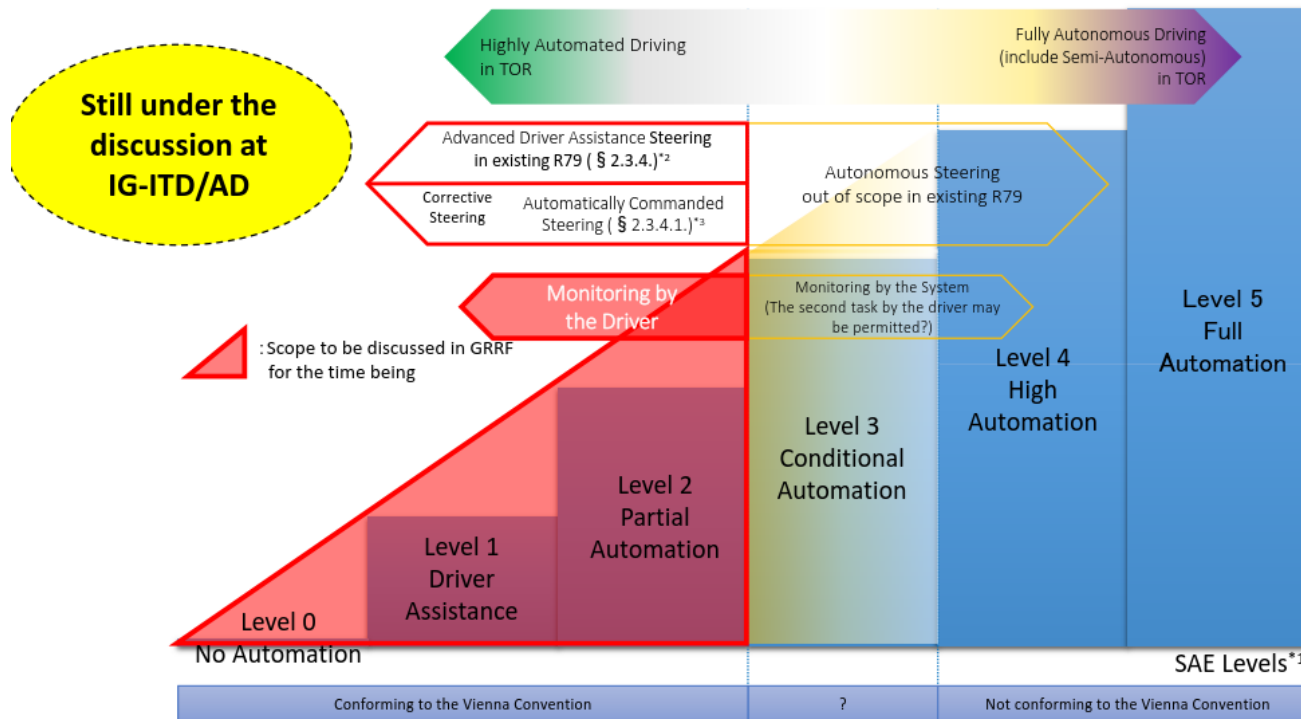
28-30th June 2016

Project objectives / timescales

- Support IWG to develop and build current proposal
 - Focus on identification of additional requirements to ensure safe system function in all real world driving situations
- Other
 - Investigation of safety assessment in other industries
 - Initial investigation of OTA updates
- Timescales aligned with IWG, end Sept.

General questions

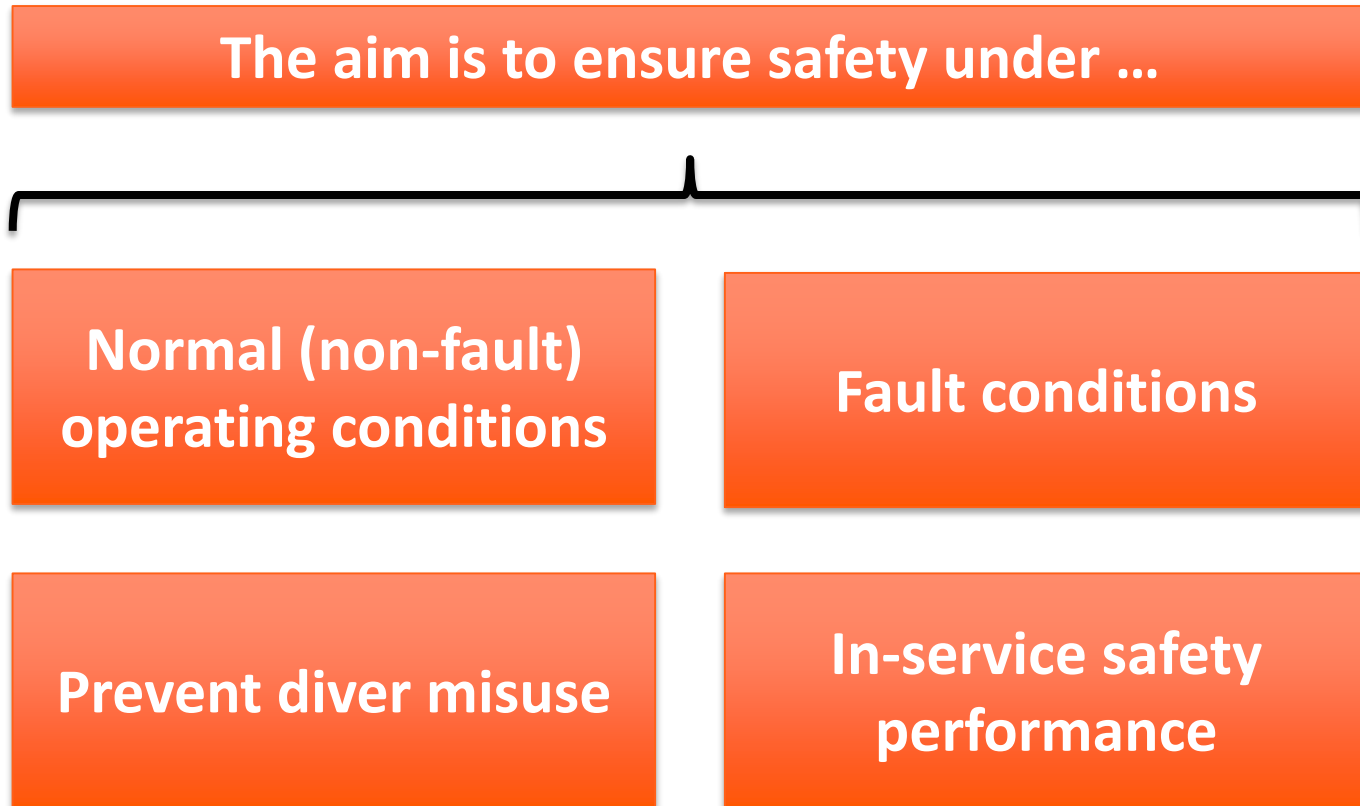
- What SAE level systems is it intended to allow; level 2 or greater?



Doc ACSF-01-11
Japan concept paper

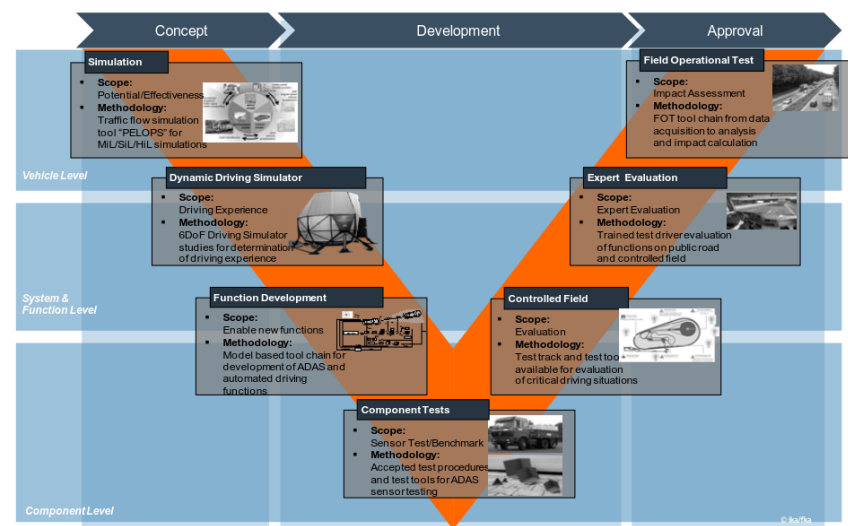
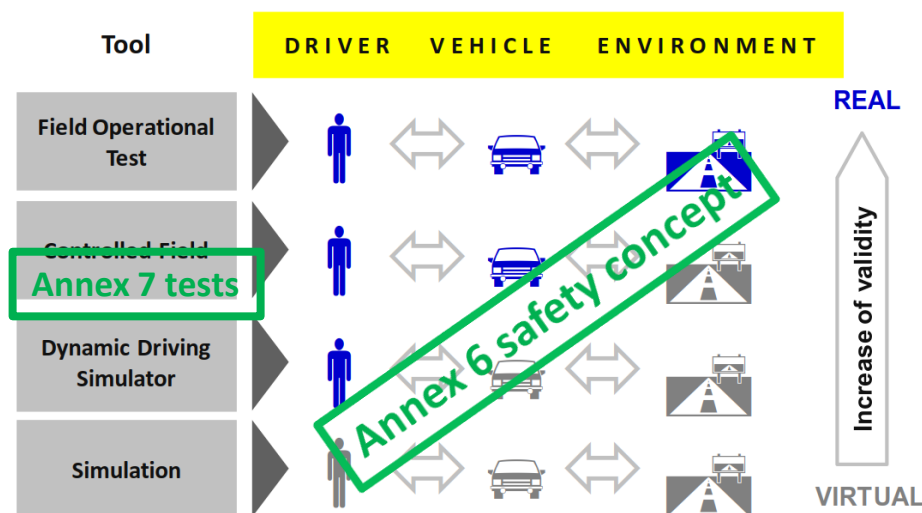
- Scope of R79, M, N & O
 - Consideration of heavy vehicles (N2 / N3 & M2 / M3)?

Develop and build on IWG proposal: Initial review of ACSF-06-28



Normal (non-fault) operating conditions

ADAS design approach



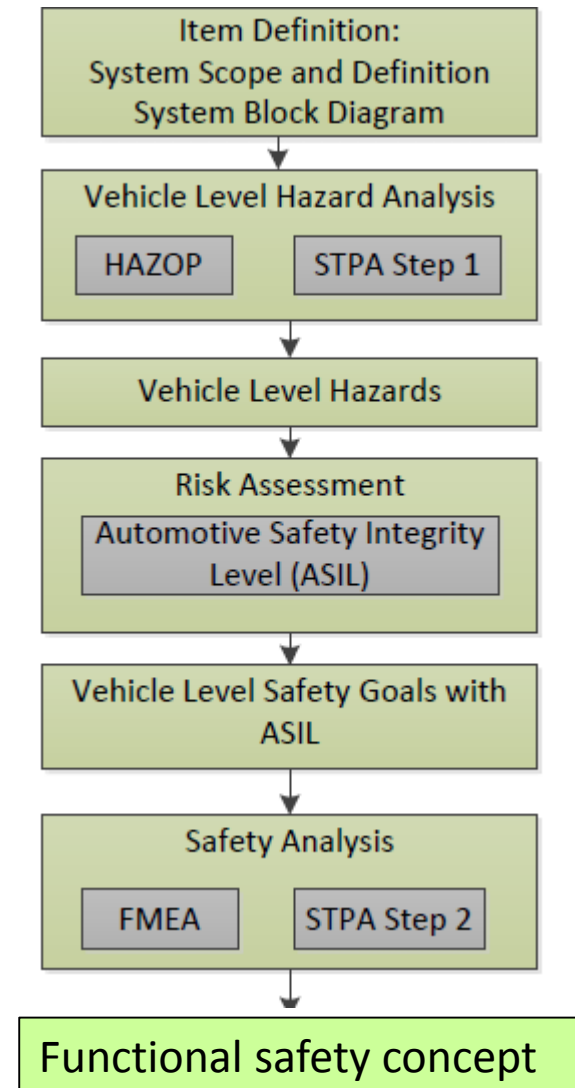
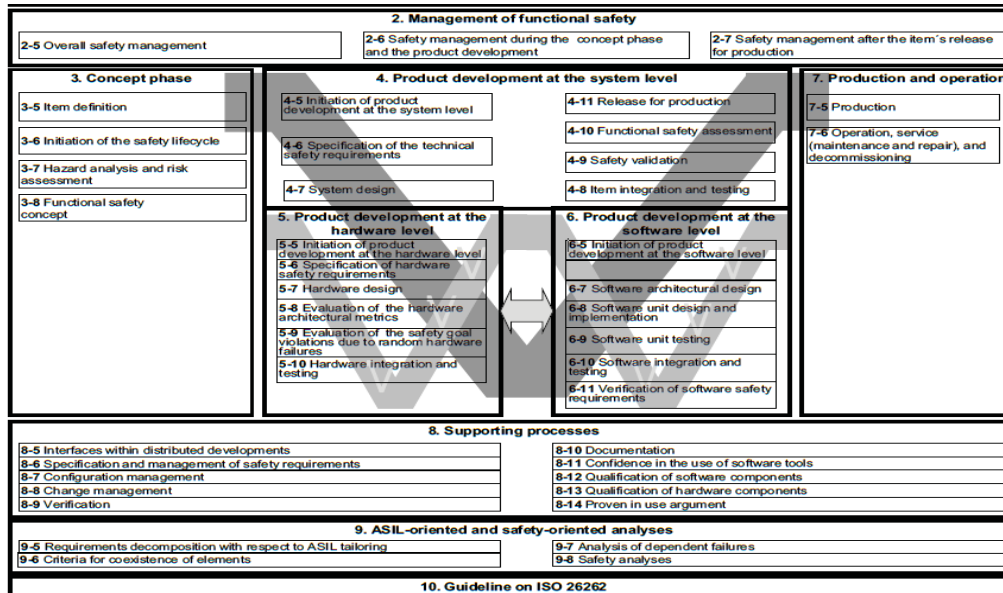
- Suggest OEM supply data as part of Annex 6 to demonstrate safe function in full range of real-world operating conditions for normal operation?
 - Guidelines for data supplied?
- Data supplied assessed by technical service
 - Guidelines for assessment?

Guidelines for data supplied?

- To include evidence of safe operation for full range of real-world conditions, including:
 - Different environmental conditions, e.g. road, weather, etc (minimum level, FOT)
 - Infrequent/emergency cases (minimum level, HIL simulation & sensor evaluation)
 - Infrequent, e.g. roadworks, LCA high-speed vehicle in adjacent lane
 - Emergency, e.g. animals, pedestrians or obstacles on road
 - Variations to configuration of Annex 7 physical tests, e.g. speed, vehicle type, lane markings, etc. (minimum level, HIL simulation & sensor evaluation)

Fault conditions

- ADAS design approach usually based on ISO 26262



- Suggest more comprehensive hazard analysis, e.g. bottom up (FMEA, HAZOP) and top down (FTA, STPA)?

Prevent driver misuse: How to ensure the driver is in-the-loop?

- Potential issue: What is the driver's role in Category E ACSF?
 - Is driver supposed to monitor the driving environment (SAE Level 2) or only be available as fallback (SAE Level 3)?
 - Current draft requires 'driver *availability* recognition system' → appropriate for SAE Level 3.
 - If SAE Level 2: Driver might need to intervene and has to be kept in-the-loop (no secondary tasks allowed).
- Options for monitoring/ensuring that driver is in-the-loop:
 - Hands on steering wheel
 - Direction of head (forward and not down towards a hand-held device)!
 - ~~Direction of gaze: Technically difficult to monitor~~
- Tests or assessment/design principles for driver monitoring systems are not currently available: Best placed in separate annex or separate regulation?

How to ensure safe in-service performance?

- Potential issue: Would problems in real-world performance become apparent before a large number of collisions happen?
- Current draft requires data recording (DSSA) only in case of a road accident.
- Potential solution:
 - Trigger DSSA recording also by other safety-relevant incidents when ACSF active (e.g. near miss events, unplanned system disengagements, emergency disengagements by the driver).
 - IWG ACSF to agree on suitable triggering criteria: e.g. braking deceleration $>.x\ g$, brake pedal force $>y\ N$, brake pedal speed $>z\ mm/s$, system disengagements due to hardware/software discrepancy).

Potential future interaction: Type-approval tests and in-service performance reporting

- The ultimate aim of the group is to ensure safe performance of ACSF in the real world with real drivers.
- What's the best way to achieve more safety?
 - Add more scrutiny up-front (more tests, simulations, documentation of development process, ...)?

OR

- Ensure that safety issues in real world use are detected and resolved early (rapid reporting of in-service safety performance by OEM)?



Do You Have Any Questions?

Mervyn Edwards; email: medwards@trl.co.uk

Matthias Seidl; email: mseidl@trl.co.uk