KARYON Kernel-Based ARchitecture for safetY-critical cONtrol

Functional Safety Applied to Cooperative Automotive Architecture

4S Group
Technology for Sustainability

4S s.r.l. - C.so Peschiera, 146 - 10138 Torino (Italy)
Phone: +39 011 0203762/3 – Fax: +39 011 0203764/5 www.4sgroup.eu

Motivations

Problem:

- Cooperative driving not well addressed in ISO 26262
- High rate of communication failures; fault or operational condition?

Target:

- Justify Safety Kernel (SK) according to ISO 26262
- Identify ISO 26262 improvement lines

Approach

Challenges:

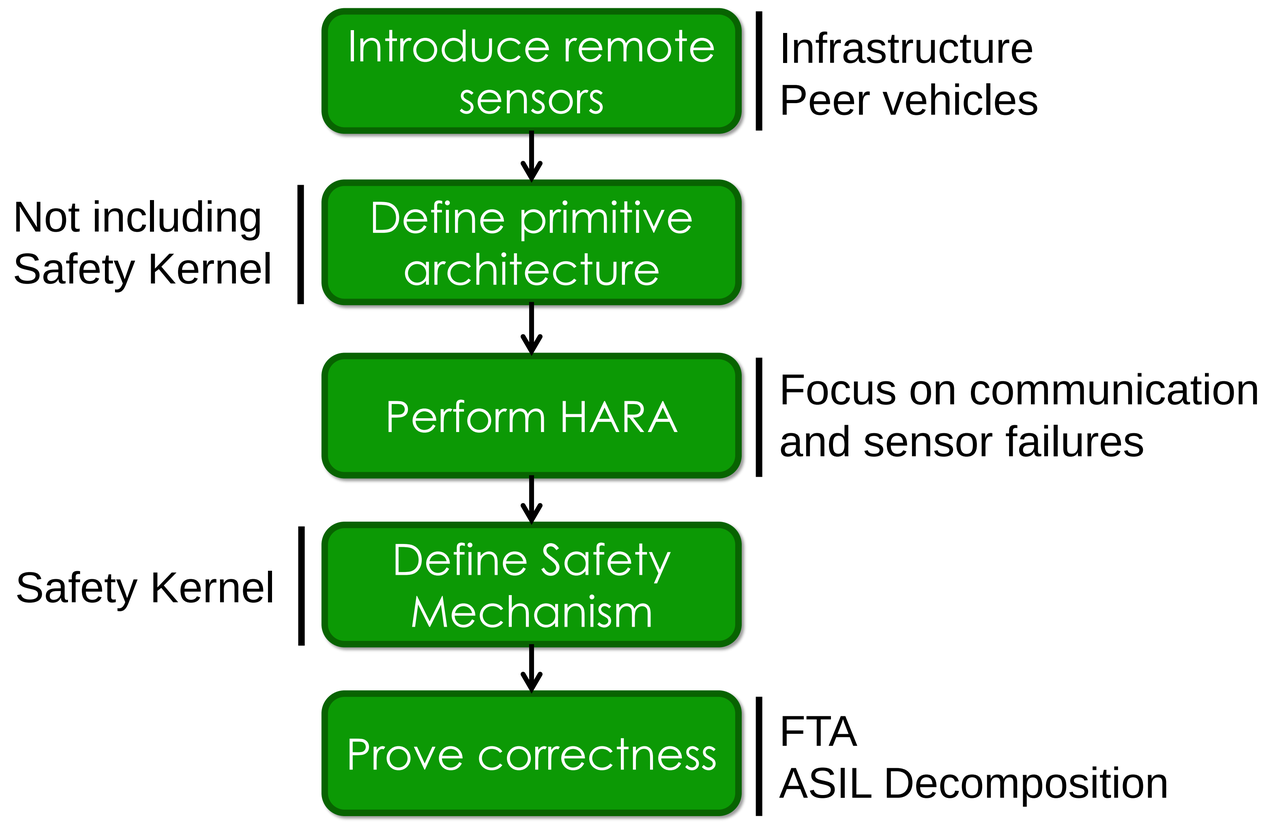
- Communication failures be taken into account
- The solution be reasonable versus market constraints
- Keep adherence to ISO 26262

Key Idea:

- Communication classified as QM

Steps:

- Introduce remote sensors
- Start from primitive architecture
- Perform HARA taking into account communication and sensor failures
- Define Safety Kernel as Safety Mechanism
- Prove correctness and effectiveness



Results

Proof Method:

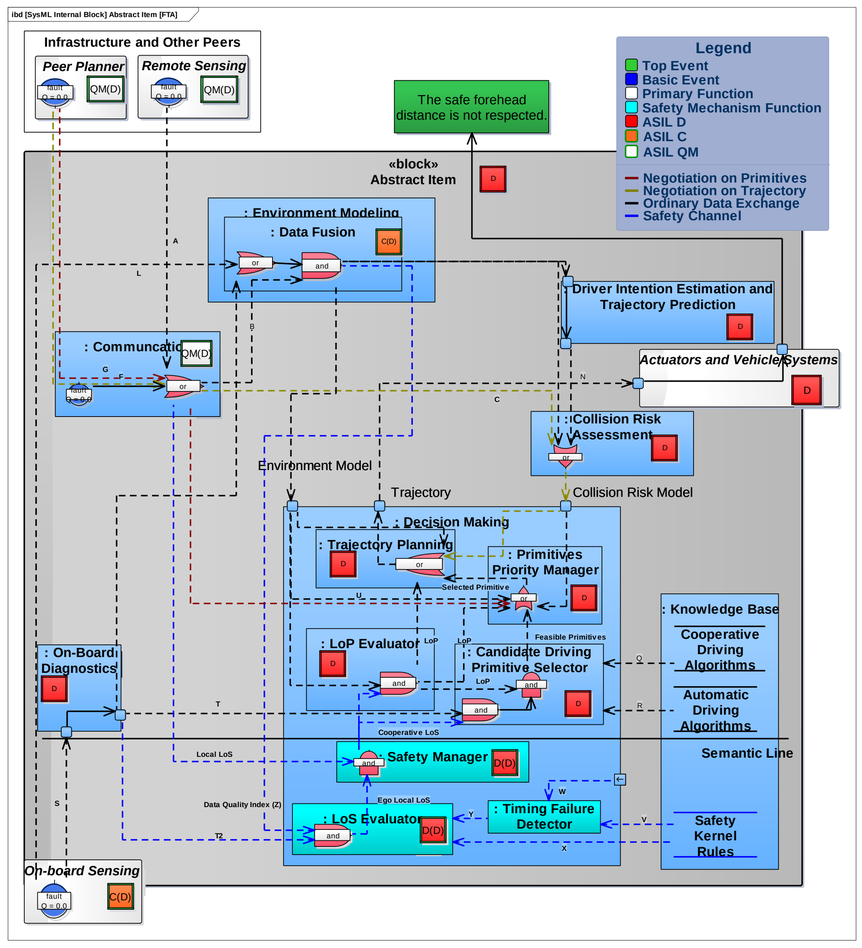
- Fault Tree and Error Propagation analysis
- ASIL Decomposition

Results:

- Safety Kernel Elements (ASIL D): Such safety critical systems needs a high level of integrity.
- Data Fusion (ASIL C): Having innate redundancy concept, the level of integrity is reduced whilst the element is still critical.
- Onboard Sensing (ASIL C): The presence of onboard diagnostics and data fusion lets failure mitigation.
- Remote Sensing (QM): The vehicle can still work safely in the absence of communication.
- Safe states: Correspond to automation levels.
- Recommendations to improve ISO 26262: Shared SM, ASIL E, Comm. faults.

FTA Notations

Application in KARYON



This work was partially supported by the European Unions' Seventh Programme for research, technological development and demonstration, through project KARYON, under grant agreement No. 288195