KARYON: Kernel-Based Architecture for safetY-critical cOntrol

Functional Safety Challenges

KARYON Workshop, Borås, Sweden, Dec 11, 2014

Kernel-Based ARchitecture for safetY-critical cONtrol

Functional Safety

- Hazard Analysis and Risk Assessment
  - For each 'function'
  - Result: 'Safety Integrity Level'
    - Needed risk reduction
    - DAL / ASIL
- Allocation onto Architectural Elements
  - DAL / ASIL on 'safety requirements'
- Evidence of fulfilling 'Safety Integrity Level'
  - According to SotA as specified by standards

Performance vs. Functional Safety

- High performance of a function
  - Customer value
  - Often implies higher demands on risk reduction
    - 'high' DAL / ASIL
- Example: Cooperative Adaptive Cruise Control
  - High speed and/or short distance between cars
    - High road capacity
    - High risk
      - High need for risk reduction ('high ASIL')
  - Low speed and/or long distance between cars
    - Low road capacity
    - Low risk
      - Low need for risk reduction ('low ASIL')

Data Quality vs. Functional Safety

- DAL /ASIL Allocated to all elements
  - Computation
  - Communication
  - Sensing
  - …
- 'Reduction of DAL /ASIL' by redundancy
  - Especially in autonomous and cooperative functions
- What if designed redundancy not appears redundant
  - A redundant source temporarily unavailable
  - Redundant sources temporarily not consistent
  - One source not consistent with expectation
- 'Reduction of DAL /ASIL' only if redundancy is guaranteed to always hold
  - Functional safety shown in design time

Solving the Paradox

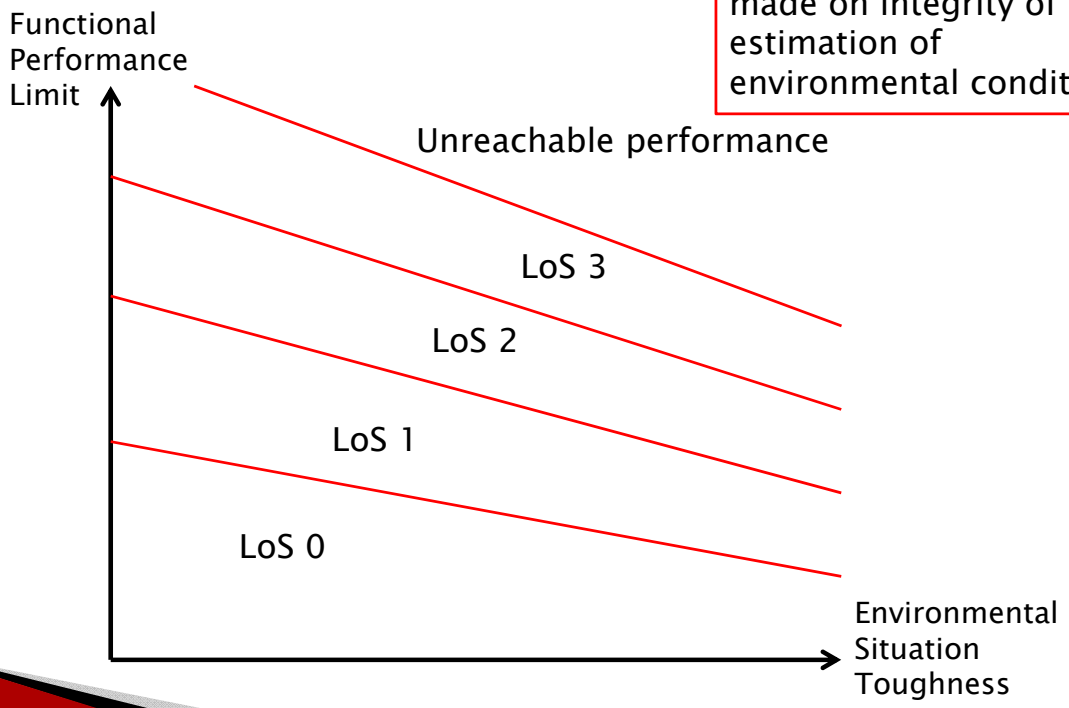
- For each function
  - Define several levels of service (LoS)
- For Each Level of Service (LoS)
  - Perform HA&RA – determine set of DAL /ASIL
  - Define set of 'safety requirements' for architectural elements
- At Design Time
  - Assess functional safety for each level of service separately
- At Run time
  - Adjust Level of Service dynamically to actual DAL /ASIL of all architectural elements

Levels of Service – Functional Perspective

- What is LoS
  - Capability level of the system to provide a service under all conditions
  - Functional performance adjusted to internal system conditions
- What is not LoS
  - Functional performance adjusted to external environmental conditions
    - Local Dynamic Map (LDM) and other environmental sensing systems gives input to functions on how to behave

Levels of Service – Functional Perspective

When assumptions are made on integrity of estimation of environmental conditions



Levels of Service – Functional Perspective

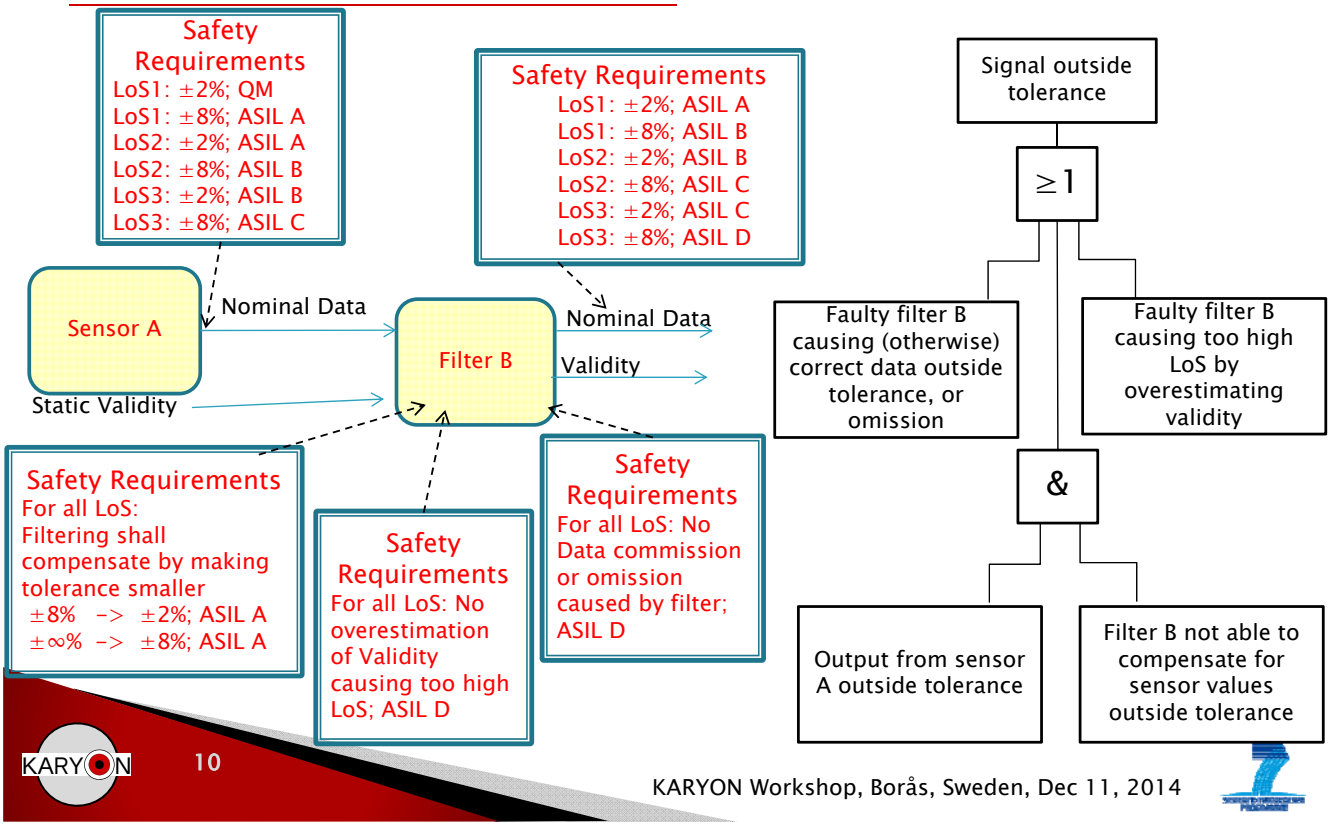
- Properties of the Levels of Service (LoS)
  - Each Level (LoS) has its own Hazard and Risk Analysis (HA&RA)
  - A HA&RA is valid for the entire LoS
    - Even if the performance limit is dependent on environmental conditions
  - Choice of appropriate LoS is only dependent on guaranteed integrity levels of the system elements

Exploitation Use Cases

- The Architectural Pattern possible to apply for several use cases:
  - Highly Cooperative Functions
    - The use cases considered inside the KARYON project
    - Lot of inherent redundancy
    - Lot of inherently low integrity elements
      - Sensors
      - V2X Communication channels
    - Cooperative LoS
  - Non-cooperative autonomous functions
    - Lot of inherently low integrity elements
      - Sensors
    - Vehicle centric LoS
  - Non-cooperative ADAS functions (lower degree of automation)
    - Significant amount of inherently low integrity elements
      - Sensors
    - Vehicle centric LoS

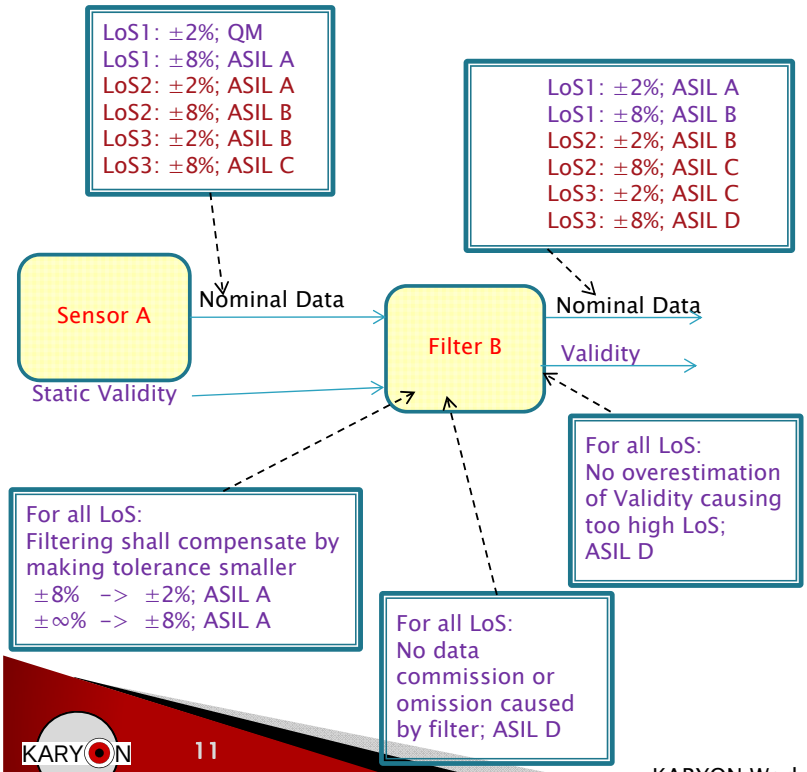
Example –Complex Sensor

Safety Requirements and Fault Tree views



Example –Complex Sensor

Considering also Validity – Run Time View



- At Design Time:
  - Unconditionally assess
    - Sensor A data tolerance
      - ±2%; QM
      - ±8%; ASIL A
    - Filter B Capability
      - ±8% -> ±2%; ASIL A
      - ±∞% -> ±8%; ASIL A
      - No comission; ASILD
      - No omission; ASIL D
    - Filter B Data output
      - Fulfilling LoS1 requirements
      - Validity calculation; ASIL D
- At Run Time:
  - Conditionally assess
    - Filter B Data output
      - Matching validity with
        - LoS2 / LoS3 requirements

Summary

- Achieve high functionality with low cost solutions
- We define several levels of service (LoS) for each function
- Then we perform HA&RA for Each Level of Service (LoS), from which safety requirements are derived
- Separation of safety assurance into
  - Design Time: assess functional safety for each level of service separately
  - Run time: adjust Level of Service dynamically to actual DAL /ASIL of all architectural elements