Working Group-Safety

Functional Safety Activities

Huzaifa Saadat

17.6.2021

AHK Meets AUTOSAR – June 2021

Virtual@AHK

BMW Group BOSCH Continental DAIMLER Ford GM PSA GROUPE TOYOTA VOLKSWAGEN AKTIENGESELLSCHAFT

Table of Contents

Activities in Working Group-Safety‘s Subgroups

1. WG-SAF-E2E (Safe Communication)
2. WG-SAF-PHM (Safe Execution)
3. WG-SAF-FSA (Safe Architecture)

Safe Communication

Types of Communication Faults According to ISO 26262-6 (Appendix D)

- Faults during exchange of information:
  - Repetition of information
  - Loss of information
  - Delay of information
  - Insertion of information
  - Masquerade or incorrect addressing of information
  - Incorrect sequence of information
  - Corruption of information
  - Asymmetric information sent from a sender to multiple receivers
  - Information from a sender received by only a subset of the receivers
  - Blocking access to a communication channel

Safe Communication

End-To-End Protection

- Profiles help to detect the communication faults
- Profiles 1, 2, 4, 5, 6, 7, 8, 11, 22, 44, 4m and 7m have been standardized by AUTOSAR so far
- Each Profile consists of different lengths of the following parameters:
  - Length (e.g. 16 bits, 32 bits)
  - Counter (e.g. 4 bits, 8 bits, 16 bits, 32 bits)
  - Data ID (e.g. 8 bits, 16 bits, 32 bits)
  - CRC (with different standards and polynomials)
  - Message Type (2 bits)
  - Message Result (2 bits)
  - Source ID (28 bits)

Safe Execution

Platform Health Management and Watchdog Manager

- One of the safety mechanisms for error detection in ISO 26262-6 (7.4.12) is:
  - “Monitoring of programme execution by an external element such as an ASIC or another software element performing a watchdog function. Monitoring can be logical or temporal monitoring or both”
- That‘s where PHM (in AP) and WdgM (in CP) come into play:
  - Types of Supervisions offered:
    - Alive Supervision (checking whether the process is still responding)
    - Deadline Supervision (checking whether the process performs tasks within time)
    - Logical Supervision (checking whether the program flow is correct)

Safe Architecture

Functional Safety Architecture

- Verify the impact on functional safety and vote for the changes and bugs in the Change Control Board (CCB)
- Assess the impact of the incoming concepts on functional safety
- Providing ISO 26262 high level guidance towards AUTOSAR
  - EXP_SafetyOverview:
    - SEooC
    - System Description
    - Hazard Analysis (Abstract)
    - Safety Goals (High Level)
    - Functional Safety Concept
  - RS_Safety:
    - Top Level Safety Requirements
    - Functional Safety Requirements
    - Technical Safety Requirements

AUTOSAR™

Thank you for your attention!

BMW Group BOSCH Continental DAIMLER Ford GM PSA GROUPE TOYOTA VOLKSWAGEN AKTIENGESELLSCHAFT