Standards of Functional Safety

Functional Safety of cars is covered by the standard ISO 26262 (2018).

The number of ECU devices in cars is growing. AUTOSAR is a platform for software in these devices. That implies that AUTOSAR must handle safety topics.

Functional safety cannot be „implemented“ afterwards into an unsafe system. Safety starts with the beginning.

An AUTOSAR stack supports safety relevant SW applications by safety standards. AUTOSAR depends on ISO 26262.

By Stefan Meerwald 2024

AUTOSAR Standards for Functional Safety

- Supervision during runtime

  Logical (prog flow), alive, deadline
- Safe communication
  - End-to-end protection of messages and RMI
- Functional safety architecture
  - Architecture and its impact on safety
- Coding guidelines
  - Based on MISRA with many extensions
- Others
  - RUST

By Stefan Meerwald 2024

Safety Topics not covered by AUTOSAR

AUTOSAR is a universal standard. It is independent of special ECU or vehicles. It cannot cover project specific topics.

Not covered:

- Hazard analysis and risk assessment (HARA).
  - Project specific and independent of technology.
- ASIL
  - None of the requirements is ASIL rated.
- Identification of processes, messages, values.
  - Which processes to be supervised? Which messages to be protected?

By Stefan Meerwald 2024

Functional Safety Example

An ECU computes a highly safety relevant output values (ASIL D). This could be a power steering or a brake system. To compute these values it needs the vehicle speed – also in ASIL D quality.

Tasks for the safety manager:

- Get the speed from various sources, f.e. from the speed sensors of each wheel. Four separate sources => Redundancy.
- Communication safe up to ASIL between the wheels and the ECU. How to protect the speed messages.
- Safe computation of output value.
- Availability of output value … in time.

By Stefan Meerwald 2024

ALTEN

Functional Safety Example

How does AUTOSAR support on safety issues?

Safe communication.

The messages to be transmitted cyclically may have a length of 25 bytes. Decide if a CRC checksum of 16 bits is good enough for ASIL D. If not then 32 or 64 bits are. If the decision is done then select an AUTOSAR E2E profile with a checksum of needed length. Define tolerance values on receiving side (might be strict for ASIL D).

By Stefan Meerwald 2024

Functional Safety Example

How does AUTOSAR support on safety issues?

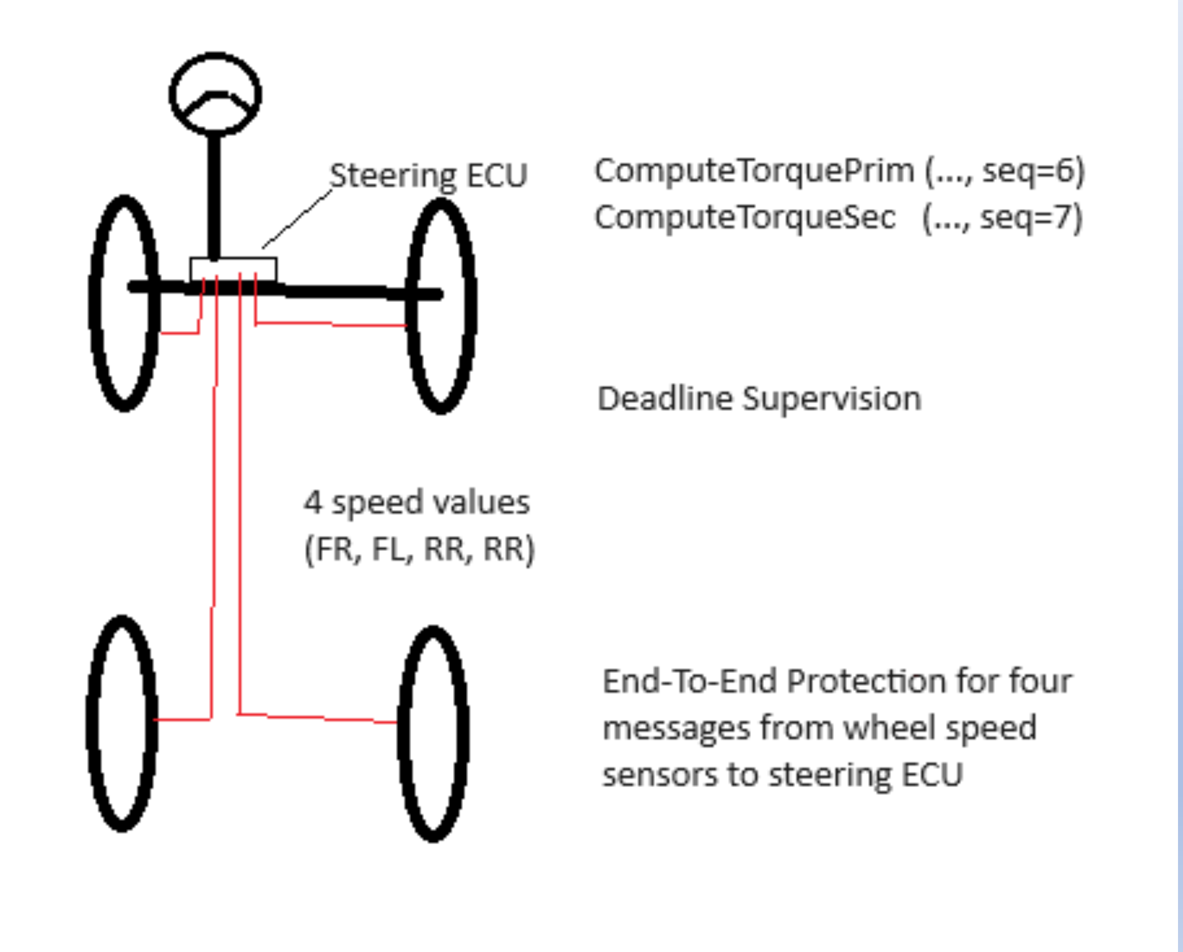
Safe calculation of values.

- Redundant calculation.
  Perform a primary and a secondary calculation of output value and compare the results. Here AUTOSAR PHM offers a logical supervision of subsequent process. Primary shall be followed by secondary.
- Availability of calculated value.
  Here AUTOSAR PHM offers the deadline supervision to monitor the calculation time.

The supervision modes of PHM include the triggering of the necessary actions if failures are detected (f.e. watchdog).

By Stefan Meerwald 2024

Functional Safety Example



ComputeTorquePrim (..., seq=6)
ComputeTorqueSec (..., seq=7)

Deadline Supervision

End-To-End Protection for four messages from wheel speed sensors to steering ECU

By Stefan Meerwald 2024

ALTEN

WG-SAF

WG-SAF is one of many working groups in AUTOSAR and consists of four subgroups (PHM, E2E, FSA, RUST)

- Weekly meetings of subgroups.
- Several F2F meetings of the whole group per year.
- Discussion of tickets.
- Reviews of concepts.
- Consult other working groups and clients in Europe, USA and India.
- Vote on tickets.
- works worldwide (sounds like bureaucracy?)

By Stefan Meerwald 2024

Who did it?

- Stefan Meerwald, born 1968 in Roth, Germany.
- University degree in computer science.
- Certified SW tester and requirements engineer.
- SW engineer in Germany and South Africa.
- Experience in telecommunication, defense, aerospace and automotive systems for various engineering companies.
- In AUTOSAR WG-SAF since 2020, document owner since 2021, speaker of WG-SAF since 2023.

ALTEN

Any Questions?

Thank you very much for your attention.

Any questions?

By Stefan Meerwald 2024

ALTEN