

ASIL Classified SW Apps on Vehicle Servers – A Safety Analysis Experience

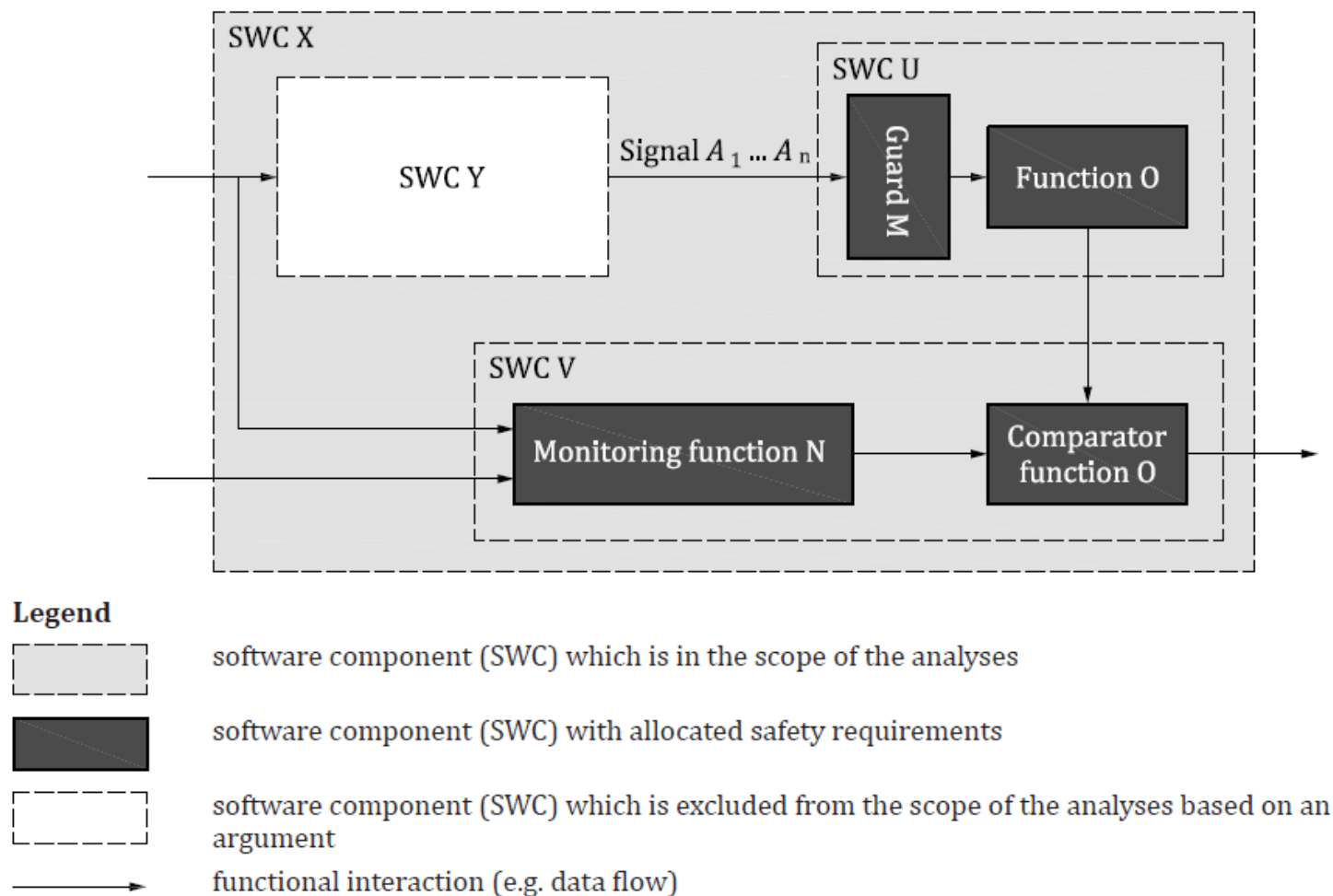
EuroSPI TechDay 2026
3rd September 2026

Richard Messnarz, Andreas Riel, Georg Macher
Supported by SOQRATES group

- AI/Strategy App at vehicle server running as a service
- An App to manage 300 vehicle parameters to optimise the electric motor control to reach the maximum distance in km. The app runs on a performance host (server). The same app recommends requesting a specific current and torque for the motor. Also the app can recommend the optimal electric axle torque actuated by the motor control. This pure software-based optimisation function can now also lead to
 - Too much torque for e-motor
 - Too low torque for the e-motor
 - Sudden unwanted torque.
 - Sudden loss of torque.
 - No torque for the motor after request.
 - Blocked torque.
 - Etc.
- Question: if it only a SW App and no hardware, can this SW App have an ASIL? Answer: Yes.

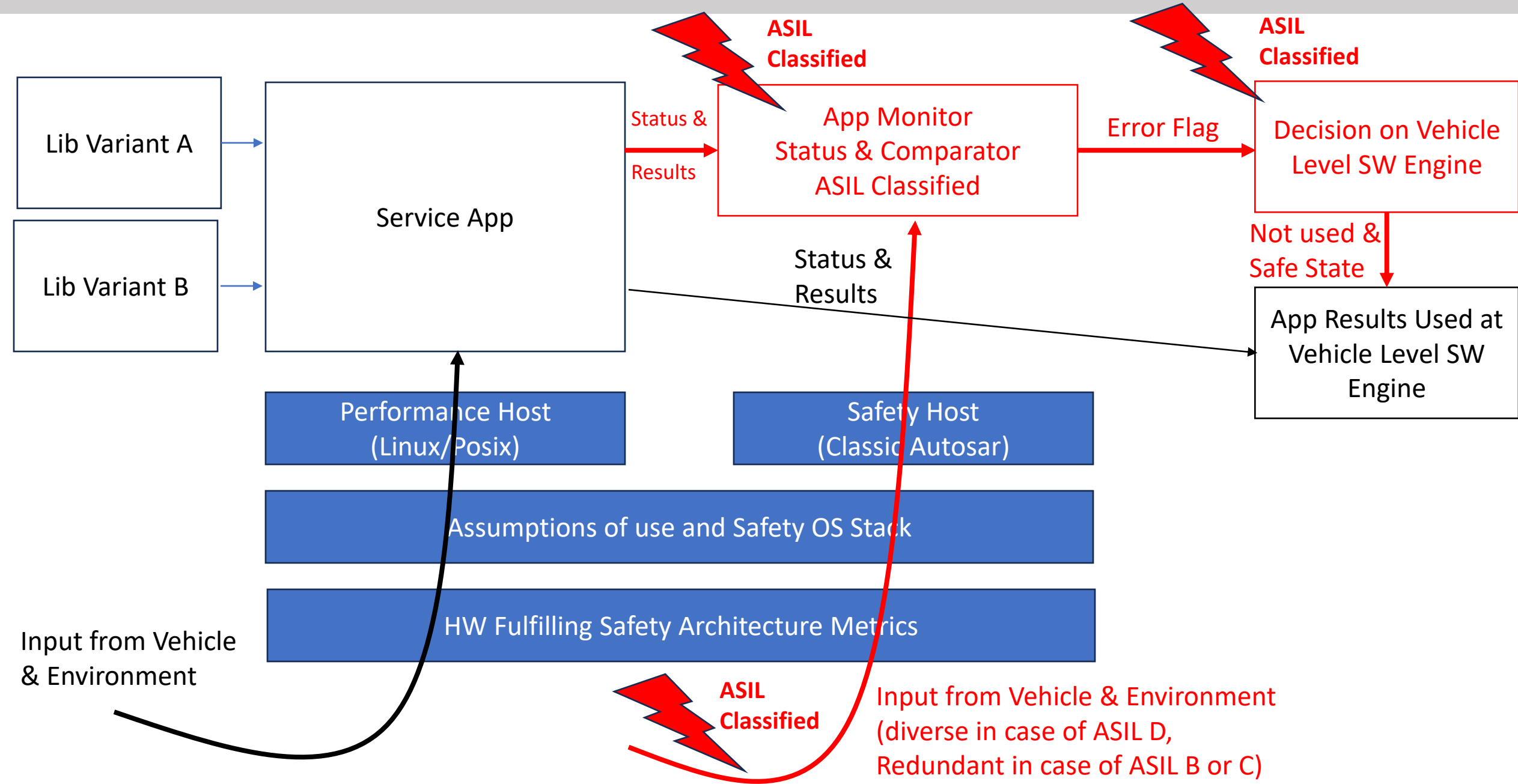
- Some of the suppliers' opinions were that you can just develop the **entire SW app as ASIL C or D, one block of SW and all is ASIL C and D. Safety is only about hardware faults**, and since the SW app is pure SW, no decomposition needs to be done.
- Especially in ISO 26262:2018 part 6 annex E there are recommendations for a **software safety analysis**, clearly **outlining decomposition guidance** for software as well.
- This finally led to an architecture where **SW apps with an ASIL still need a freedom from interfere monitor concept which can be mapped onto the SOA (Service Oriented Architecture)** architectural framework.

- SW Safety Analysis



- The app is having a monitor. The monitor runs on a freedom from interference, task and memory. The monitor includes a status check and a comparator function.
- If the status check or comparator fails a safety critical error flag is set, and the vehicle level SW engine decides about how to reach the safe state. The safe state can also mean to ignore the app output until it delivers results that do not violate the safety checks in the monitor. However, there are more modes the vehicle engine can take.
 - e.g. to ignore the app outputs and heal after some time
 - e.g. to bring the vehicle to a safe state by deactivating a function and warning the driver
 - e.g. to reduce the speed, warn the driver and still continue to use the app output.
 - Etc.

Implemented Finally



- The biggest challenge is the comparator design for the app developer. How would a comparator of the app work?
 - Example:
 - Example 1: Optimisation Example
 - The app is considering many parameters to optimise the motor control and correct the torque request. The app runs per optimisation tasks in 5 refinement cycles to calculate the optimised value.
 - Example 1 Torque related app comparator:
 - The first idea was to use a limiter and allow optimisations within limits. **However, you also expect a reliable and stable torque and then the limiter alone was too rough. Then the team realised that in the 5 cycles of refinement the target value followed a specific converting function behavior if it was correct. And then beside the limiter the gradient of the function expected was used to check safety and stability at the same time.**

- In the next years the complexity of a software will lead to a discussion if the definition of a system is right: “A system contains at least two different subsystems e.g. electronics and SW, electronics and HW, etc.”
- **The authors predict that soon in the future the term System of Systems in SW** will be accepted and the term software system **will be recognised** by all car makers or manufacturers.

Thanks

Thank you for cooperating with ISCN.



1. ISCN is INTACS certified training provider for Automotive SPICE assessor courses
2. ISCN is certified by VDA to hold provisional and competent ASPICE assessor courses
3. ISCN moderates the German task force SOQRATES (<https://soqrates.eurospi.net>) since 2003 where >20 Tier 1 collaborate on ASPICE, Safety and Security.
4. ISCN organises the EuroSPI conference since 1994 where e.g. VW is organising a workshop community, and VW, Rheinmetall AG, EB, MAGNA, Cariad, VALEO, AVL held key notes. <http://www.eurospi.net>
5. EuroSPI certificates are issued by EuroSPI Certificates & Services GmbH (www.eurospi.net) in cooperation with DRIVES and the Automotive Skills Alliance (ASA). The ASA was founded by the EU Blueprint Project Drives and ALBATTIS with support from the European Automobile Manufacturers' Association (ACEA). <https://www.eurospi.net>. ISCN is founding member.

Thanks

Thank you for cooperating with EuroSPI Certificates GmbH.



1. Academy – Courses and Training Platform
2. Certification – Exam system and certificates
3. EuroSPI Conference Series
4. Assessment Tool – ISO 330xx based