Functional safety in road vehicles


(Source: Adobe Stock)

Last decades have proved that safety is crucial in automotive applications. Digital Core Design (DCD) has added the FMEDA (Failure Modes Effects and Diagnostic Analysis) and safety mechanisms to its DCAN (FD) IP core for standalone CAN (FD) controllers.

Complexity of modern cars is growing rapidly without a doubt. A lot has happened since Ford T and the times when car was just a "fully mechanical" experience. Last few decades prove that safety is crucial. There's no wonder then, that the safety ecosystem based on proprietary certification is a must. But even the best engineer is not capable of taking care of every single design detail. Everyone makes mistakes. That's why the automotive industry has adopted stringent processes throughout the supply chain. The final product is modularized, but every submodule, consisting of multiple submodules must be properly documented as well. Why? Because every lifecycle detail must be traceable. The most common automotive standard is the ISO 26262 (see Figure 1) that indicates the whole safety development lifecycle, from the item definition up to the decommissioning.

Evaluation of functional safety

On the other side, is the new design and verification flow really not excessive? Let us consider a simple case – a Tesla car accident. Tesla is a manufacturer that can be described easily – from zero to… hero. Built from the scratch, with keen-on learning engineers, ready to find solutions to encountered problems. Tesla has focused on autonomous cars. But their cars still had some crashes, where the car did work as expected, but still an accident occurred. Why? Due to the wrong design assumptions. The engineer cannot rely on the design itself, but the design must consider the working environment context and consider random faults. To gather an objective evaluation of the functional safety of a product, the Automotive Safety Integrity Level (ASIL) has been introduced. In one sentence – it shows if the design provides a reasonably low level of failures in time (FIT). This one depends on systematic failures and random hardware failures. The systematic failures can be omitted by a change in design, proper design procedures, and testing. Random hardware failures cannot be omitted, but the risk caused by a hazard can be mitigated.

Safety design flow

DCD has introduced the safety design flow. As an IP (intellectual property) core provider, the company does not consider the whole design, but only the IP design, testing, and safety analysis. The DCAN IP core for Classical CAN and CAN FD implementations is developed as an ISO 26262 Safety Element out of Context (SEooC). The SEooC (the soft IP SEooC in the case of DCAN) is an element developed and analyzed in an assumed context of use,

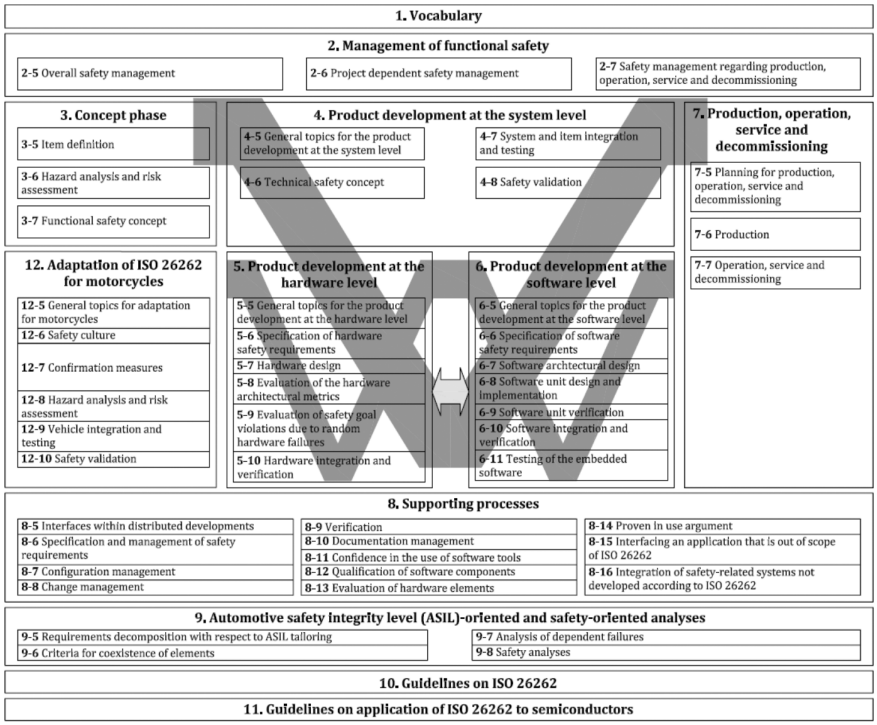

Figure 1: ISO 26262 standards overview (Source: ISO)

Figure 2: The autonomous car design must consider the working environment context and random faults (Source: Adobe Stock)

e.g. target FPGA (field-programmable gate array) board, memory used, etc. The SEooC is delivered with complete ISO 26262 required documentation. Why? To help the system integrator, who must reevaluate the safety analysis based on the target system and the safety analysis of other system elements. The SEooC provides deep knowledge about the DCAN IP, its failure modes, safety mechanisms that enable to reach the required ASIL level, complete Failure Modes Effects and Detection Analysis (FMEDA) with step-by-step instruction to help to integrate the IP into the customer's system and to conduct the system-level safety analysis.

Call for Papers

The 18th international CAN Conference (iCC) aims to foster collaboration, knowledge exchange, and networking among professionals at the forefront of CAN technology. Join us as expert and submit an abstract showcasing your latest developments, whether they are based on classical CAN, CAN FD, or the emerging CAN XL.

- CAN implementations
- CAN device design
- CAN system design
- CAN diagnostics
- CAN higher-layer protocols
- CAN-related research studies
- CAN applications in vehicles
- CAN applications in industry
- CAN in general-purpose applications
- Other CAN-related topics

18th international CAN Conference
iCC

Baden-Baden (DE), May 14 and 15, 2024

Important date:

- Abstract Submission Deadline: **September 15, 2023**

Please consider that the iCC Program Committee, chaired by the CiA Managing Director Holger Zeltwanger, considers technical-oriented papers only.

For submission guidelines, sponsorship opportunities, tabletop exhibition details, and further information, please contact CiA office: conferences@can-cia.org

Figure 3: A well-tailored design process with traceable steps and work products brings benefits for the IP provider and the integrator (Source: Adobe Stock)

Safety analysis

Let's now focus on the safety analysis. The main work product is the Failure Modes Effects and Diagnostic (FMEDA) analysis (see below). As the input product to the FMEDA analysis, we need to do a Hazard Analysis and Risk Assessment (HARA). We need to define the Safety Goal(s) of our design and then ask: what can go wrong? We need to detect most functional failure modes, that can lead to a Safety Goal violation. To do so, one should estimate these three factors:

- Exposure – how likely is the case to happen? How possible is the system to fail?
- Controllability – what is our ability to control the failure? Is the driver able to handle it?
- Severity – how harmful can be the occurrence of the hazard? What harm can be caused to the driver?

Knowing what can endanger the Safety Goal, we need to formulate the functional safety requirements to avoid any unreasonable risk for each of the hazardous events. Based on functional safety requirements we need to formulate then, the technical safety requirements, that indicate the safety mechanisms needed for detection of the failure modes.

FMEDA analysis

The FMEDA analysis gathers all the information together. FMEDA is done in a form of a table. There is a plenty of dedicated software solutions that should help in the analysis. But all of them have one common disadvantage – the price, which is (not only) relatively too high.

The use of the forementioned software is not the only way as a simple Excel sheet is good enough for the analysis. Each failure mode in company's FMEDA must have a unique ID assigned to it and a description of the possible effect on the analyzed item. In next columns we need to estimate the distribution of permanent and transient failures to calculate their failure rates measured in FIT. This is the failure rate for the particular failure mode in the absence of any safety mechanisms. Then we need to assign whether the failure leads to a single point fault or to multiple point faults. After that we think of the safety mechanisms that can detect the fault and estimate their diagnostic coverage.

The failure rate (λ, see Formula 1) of a safety-related hardware element (i.e. SEooC) consists of safe faults failure rate, single-point faults failure rate, multi-point faults failure rate, and residual faults failure rate.

The ASIL level is determined by the Single Point Fault metric (SPFM) and Latent Fault metric (LFM).

$$\lambda = \lambda_S + \lambda_{SPF} + \lambda_{MPF} + \lambda_{RF}$$

Formula 1: Failure rate of a safety-related hardware element

$$SPFM = 1 - \frac{\lambda_{SPF} + \lambda_{RF}}{\lambda}$$

Formula 2: Single Point Fault metric (SPFM)

$$LFM = 1 - \frac{\lambda_{MPF,L}}{\lambda - \lambda_{SPF} - \lambda_{RF}}$$

Formula 3: Latent Fault metric (LFM)

Table 1: Required metric values to achieve the proper ASIL level (Source: DCD)

	ASIL B	ASIL C	ASIL D
SPFM	≥ 90 %	≥ 97 %	≥ 99 %
LFM	≥ 60 %	≥ 80 %	≥ 90 %

At this moment DCD cannot share more information about the details of the analysis and the safety mechanisms added to DCAN SEooC and metrics calculation. This is company's know-how combined with the ISO 26262 knowledge. Contact DCD's team, who can help you to find the most appropriate solution related to safety analysis.

And, last but not least, here are some tips why it's worth to integrate a SEooC in your design instead of to conduct the safety analysis on your own:

- Easy integration
- Comprehensive IP knowledge by the DCD team
- Support (really helpful in possible safety anomaly resolution process)
- Time to market
- Costs

Conclusion

A well-tailored design process with traceable steps and work products is obligatory today. But despite the necessity, it brings also benefits both for the IP provider and integrator. The formalized design procedures at every design lifecycle step, traceable changes, and responsible people, testing and verification as well as the quantitative evaluation, all of these provide best quality products with a lot of added value. It also helps in project maintenance. The integrator benefits from lower time to market, better safety analysis results, easier integration, and support.

Author

Robert Nawrath
Digital Core Design
robert.nawrath@dcd.pl
www.dcd.pl