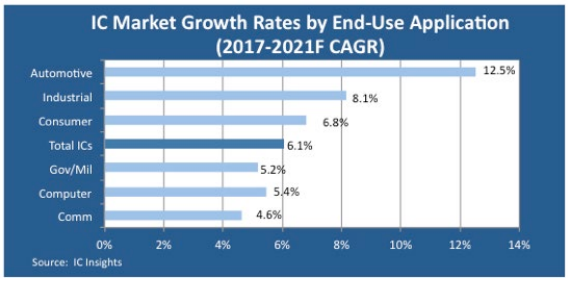
Automotive Safety and ISO26262 Compliance

Safety - The absence of unreasonable risk

Author: Mike Bartley, T&VS founder and CEO

In a recent Design and Verification Europe meeting (DVClub) organised by T&VS a wide range of expert speakers shared their experiences on how to ensure automotive ICs are compliant with the safety requirements of the ISO 26262 Standard. In this article Mike Bartley summarises the key points made in each of the presentations.

Automotive is currently the fastest growing IC market and is attracting interest from several potential new entrants. However, there are significant barriers to entry and one of those is compliance to ISO26262 which governs how automotive ICs must be developed to be demonstrably safe.



Meeting Functional Safety Requirements for Automotive Applications

Adam Sherer from Cadence explained the importance of identifying the appropriate ASIL (Automotive Safety Integrity Level) before starting any new automotive IC development. For this to occur it is necessary to identify and classify the risks based on 3 factors: severity; exposure; and controllability.

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

ASIL:
Automotive Safety Integrity Level

ASIL A = lowest
ASIL D = highest

The severity identifies the potential impact of any risk and the exposure identifies the probability. These two factors define the classic risk analysis, however we also need to consider how much control the driver has over the risk. For example, if the car decides to apply the brakes and there're no override by the driver then that has very low controllability. The higher the ASIL then the more rigorous the development

process needs to be (e.g. higher levels of coverage) and the higher the level of fault detection. To view the full presentation Click Here.

Developing Safe ICs - Mentor Safe IC for ISO 26262 & IEC 61508

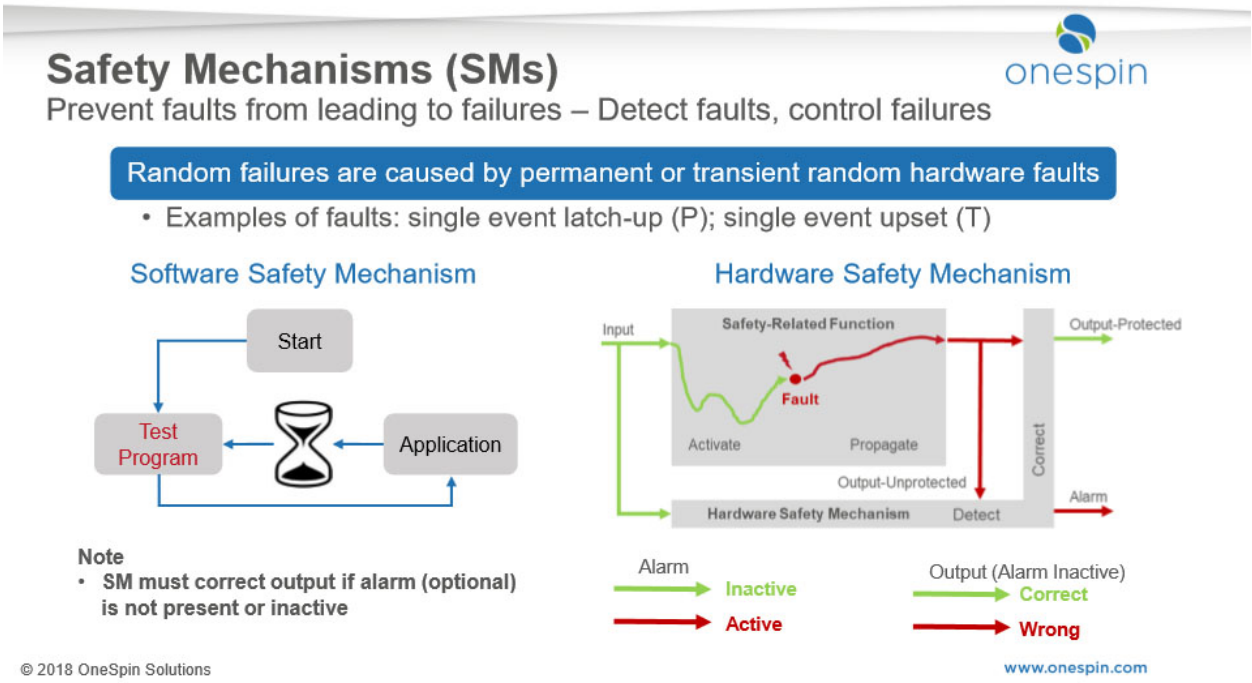
Alex Grove from Mentor Graphics highlighted that ISO26262 is about driving down the risk of faults because cost of failure is so high. In his presentation he identified two main types of faults: Systematic and Random. Systematic faults are the usual bugs that we try to find through functional. These can generally be avoided through greater rigor in the verification process using techniques such as FMEA/FMEDA and requirements-driven verification, with the higher ASILs requiring more rigor, e.g. through higher structural coverage targets. Random faults maybe permanent (e.g. stuck-at) or transient (e.g. EMI electro-migration) and the IC in development is required to detect such faults and either correct them or fail-safe. Once again, higher ASILs require higher detection rates. Alex outlined the Mentor automotive solution Polarion which has 4 key components: lifecycle management; safety analysis (based on the Austemper acquisition); design for safety; and safety verification. To view the full presentation Click Here.

Functional Safety - The Absence of Unreasonable Risk

Olivier Bocquillon fromSynopsys reminded us that safety is defined as the absence of unreasonable risk. He underlined the issue of random faults by highlighting the Toyota 2011 single bit flip which was caused by a cosmic ray and led to unintended acceleration. This was not only costly to Toyota but more importantly caused several deaths. In his presentation Olivier outlined what functional safety is, how it should be done and what needs to be done differently so that we will be able to relax in our autonomous cars? He concluded by outlining the Synopsys Z01X solution for running a fault injection campaign which is required to measure fault detection rates.

Hardware Safety Metrics for ISO 26262 Compliance

Finally, Sergio Marchese from OneSpin Solutions went into detail on the Safety Mechanisms that are required to prevent faults leading to failures and the different types of faults. For example, some faults are deemed “safe” if they cannot lead to an error, for example a stuck-at-0 on a signal that is tied low (the categorization of faults is explained more in Section 5.8 of the ISO26262 standard). He then provided an overview of single point and residual faults, multi-point faults, latent faults and the fault metrics that can be used to reflect on the effectiveness of the safety architecture to protect against these faults leading to failures.



Sergio went on to explain that once a fault that can lead to an error is detected then the IC must either correct the Raise alarm or fix the fault and concluded with a summary of the automated tools and expertise Onespin have to offer for ISO 26262 safety analysis. To view the full presentation Click Here.

About DVClub Europe

The principal goal of DVClub is to have fun while helping build the verification community through quarterly educational and networking events. DVClub membership is free and is open to all non-service provider semiconductor professionals. T&VS are the local organizes for events in Europe and India. For additional information, including past and future meetings, visit: https://www.testandverification.com/conferences/dvclub/