Automotive iQ

14th Annual
AUTOMOTIVE FUNCTIONAL SAFETY WEEK 2024
Implementation of ISO 26262 & SOTIF

FUNCTIONAL SAFETY PRIORITIES FOR 2024:

IN CONVERSATION WITH NXP SEMICONDUCTORS

NXP

UNCOVER THE KEY SAFETY PRIORITIES FOR NXP SEMICONDUCTORS IN 2024

- HOW IS NXP FAST-TRACKING FUSA
- ISO 26262 FOR NEWER SDV APPLICATIONS
- WHAT TO EXPECT FROM ISO 26262 3RD EDITION

FRANCK GALTIÉ
FUNCTIONAL SAFETY FELLOW, CENTRAL TECHNOLOGY OFFICE

CARMEN KLUG-MOCANU
SENIOR PRINCIPAL HARDWARE & SYSTEM SAFETY ARCHITECT, FUNCTIONAL SAFETY TECHNICAL ASSESSOR

MARCUS MÜLLER
FUNCTIONAL SAFETY ARCHITECT

MAT BLAZY-WINNING
DIRECTOR FUNCTIONAL SAFETY




WWW.AUTOMOTIVE-IQ.COM/EVENTS-AUTOMOTIVE-FUNCTIONAL-SAFETY-WEEK

Ahead of the Functional Safety Week Europe 2024 conference, Automotive IQ spoke with a panel of experts from **NXP Semiconductors** to delve into the latest developments and challenges in functional safety. Franck Galtié, Carmen Klug-Mocanu, Marcus Müller, and Mat Blazy-Winning provided invaluable insights into NXP's functional safety priorities for 2024, shedding light on the company's strategies amidst the automotive industry's shift towards autonomous driving and electrification.

From navigating evolving standards landscapes to streamlining functional safety processes and reinterpreting ISO 26262 for complex software architectures in Software-Defined Vehicles (SDVs), the conversation covered the most pressing FuSa challenges for 2024, outlining their key priorities to learn and discuss at the Automotive Functional Safety Week conference.

NXP PRIORITIES FOR 2024

Q: Electrification and autonomous driving are creating new challenges for the functional safety community. How is NXP dealing with evolving safety requirements, and what are NXP's functional safety priorities for 2024?

FRANCK

Listening to the market trends is key to defining the right strategy for safety within NXP. After the hype around autonomous driving, we are back into a more realistic timeline towards SAE levels 4 and 5. The new highly trending topic around Software-Defined Vehicles (SDVs) combined with the perspective of a drastic evolution of the vehicle architecture towards central compute and zonal architectures brings the safety community into a new hype curve.

Although this will not be in the field from tomorrow, the work is happening now to shape NXP products with the applicable safety concepts for the SDV. This new challenge pushes us into the Software-Defined Safety (SDS) with a more balanced HW/ SW safety concept, higher isolation requirements, increased maintainability and improved availability of the system.

In addition, the electrification era has come and NXP is fully focused on providing the best system safety solutions to support charging, energy storage and energy management challenges.

Q: How is the evolving standards landscape impacting these priorities? What key standards are you paying attention to right now?

FRANCK

For the past couple of years, safety related standards (ISO, IEC, IEEE), Technical Specifications (TS) and Technical Reports (TR) have been growing like mushrooms in the autumn. Besides the complexity to follow and/or contribute to all these standardisation initiatives, the highest risk is to create more confusion by the inconsistencies that spring up between them all. We are closely monitoring and contributing to several activities around Artificial Intelligence, autonomous driving, interoperability, but inevitably, we are paying more attention to the third Edition of ISO 26262, including (but not exclusive to) New Electric Vehicle architecture (NEV), predictive maintenance and others.

Looking more and more in the direction of System Safety Solutions to deliver the best "ready to use" safety concept, Safety of the Intended Functionality (SOTIF) is becoming more and more included in our scope of attention.

FAST-TRACKING FUSA LEARN NEW METHODS AND PROPOSALS TO MAKE THE FUSA PROCESS RAPID & STREAMLINED

Q: What new methods are NXP Semiconductors applying to make processes more efficient & cost effective, without compromising on safety and integrity?

FRANCK

In terms of process efficiency, the Waterfall development model defined in ISO 26262 is very often challenged by a more "Agile" development model. NXP is fully engaged in such process evaluations and improvements - especially for SW

development. As such, we are very focused on maintaining the same efficiency and cost effectiveness despite the rapid increase in product complexity of the past 2-3 years. Particularly because the new vehicle architecture and SDV approach requires NXP to further improve the way of working and introduce more and more Model Based System Engineering (MBSE) to our development flow.

To tackle the higher complexity of the HW/ SW interface, modelling supports static and dynamic architectures to implement a more and more complex set of requirements. On the other hand, pushing left and virtualising the HW/ SW integration is a key factor to support SW development at the integrator side and therefore improve time to market. Of course, there are other advantages of moving to MBSE and NXP believes that this is the path to an efficient and safe development flow for new highly complex challenges of SDV.

Q: What solutions are there to optimise the interface between companies in the supply chain, and how is NXP working to reduce pain points in the interface between NXP, Tier-1s and OEMS?

FRANCK
The major pain points when interfacing safety work products between Tier-2 and Tier-1 companies are generally around safety analysis, safety documentation and SW integration. As mentioned before, the modelling can support a better and earlier SW integration on a virtual representation of the SOC.

Regarding the safety analysis, the complexity comes from the very large amount of detail in the safety analysis like FMEDA at SOC level. As known, this level of detail is a must-have to demonstrate the safety integrity of the chip. However, this is far too much to include into an already large FMEDA performed at system level. Working more and more on system safety concepts helps NXP to ultimately better abstract the failure modes and corresponding metrics to the right level and therefore ease the integration into the final system FMEDA.

Regarding the safety documentation, the increasing complexity also drastically impacts our documentation (like user manuals, safety manuals). Verification of Assumption of Use (AoU), safety mechanisms usage and configuration by the integrator can highly benefit from the system safety concepts developed by NXP as well as from the SysML modelling previously mentioned.

The combination of the different changes introduced in the NXP way of working should highly reduce the most known pain points in the interface between NXP and Tier-1/ OEMs.

UNDERSTAND HOW TO RE-INTERPRET AND APPLY ISO 26262 FOR NEWER, COMPLEX SDV APPLICATIONS

Q: Software-defined vehicles introduce an uparalleled level of complexity for the safety community. How can ISO 26262 be applied to the software architecture in SDVs?

CARMEN
One of the main challenges in future vehicle architectures will be to accommodate on the same platform, complex and diverse functions, e.g., service oriented vehicle smart capabilities and highly personalised functions, extended car connectivity features with autonomous driving, where safety, security and availability play a central role. A vehicle centralised brain-controlled architecture combined with a layered approach may help to manage and control the complexity.

To reduce and control the complexity, the software executable components could be handled as black box components, not tied to a list of HW components, but tied to an agnostic HW resource set to fulfill the feature set required for the proper execution (e.g., performance timing, safety integrity level).

The entire SW architecture is layered and built on these simplified black box components, with predefined input and output interfaces developed based on ISO 26262 from the concept to implementation, testing and release phases. An additional advantage of this architecture paradigm is that with an extended concept to support sharing and redistribution of the HW resources, could also increase also the availability of critical functions.

MARCUS AND MAT
As ISO 26262 covers system, hardware and software, the overall scope fits well to defining vehicle safety architectures including SDVs. The challenges that SDVs bring is through the integration of what were previously independent vehicle functions on separate ECUs onto powerful automotive compute platforms

– allocated across central compute, domain and zone processing. This requires that safety functions of different criticality, as well as non-safety functions are isolated from one another on the same compute platform. These platforms must ensure that if one function fails, it does not impact all other functions that are running, in order to take into account the more advanced availability requirements of these super-integrated systems.

Q: How can over-the-air and continuous software updates be used to ensure safety during the vehicle lifecycle?

CARMEN
One of the main prerequisites will be to assure data transfer integrity from a security as well from a safety point of view. Another one would be to provide the environment which enables a proper testing and validation of new software updates and of the new added functionalities, taking into account the specific vehicle physical environment and corner cases of the defined use cases.

Having digital twins to model and predict certain behaviours and device reactions could be part of the solution of testing and prediction of the effect on the system behaviour due to software updates or added new features.

MARCUS AND MAT
When software updates are performed over-the-air, both safety and security requirements need to be met. Authentication of updated SW images is a critical step, and both the security & safety integrity need to be established before running a safety application, as security becomes a precondition for safety. This is where it is important to have an aligned safety and security concept and architecture throughout the hardware and software.

Q: What solutions are there for risk management of cloud-hosted systems, when ISO 26262 cannot be applied to anything not installed in the car?

CARMEN
The solution for risk management of cloud-hosted systems depends on the functionality provided in the cloud and the impact on the vehicle state. In general, the main risks are to data integrity, data availability, how to guarantee that the right processing is executed, and the right control input is provided to the vehicle, when required.

Building strong checker points to the end-user (e.g. software installed in the car) to identify the data corruption or data misused may be a solution for this problem.

EXPERT VIEWS ON HOW FUNCTIONAL SAFETY IS EVOLVING, THE DIRECTION OF SAFETY STANDARDS, AND WHAT TO EXPECT FROM ISO 26262 3RD EDITION

Q: Working group members are on the cusp of decision making for the 3rd edition of ISO 26262. What next steps should the functional safety community be aware of before the next standard gets released?

FRANCK
As far as I am involved today, the current activity mostly focuses on Topic Groups (TG) to discuss the proposed new topics/ updates from all the ISO 26262 country committees that could be considered for the ISO 26262 Edition 3. Then the selected topics will be addressed in the update of the corresponding ISO 26262 parts following the normal ISO standards development flow (CD, DIS, FDIS, IS).

Q: Which technologies do you expect to impact the direction of functional safety in the future?

FRANCK
Artificial Intelligence/ Machine Learning is clearly an ongoing challenge for functional safety and safety in general. NXP is focusing on Safety for AI including HW, SW and tools. Although there could be a quite simple approach to ensure the safety integrity level of an HW accelerator, the major challenge is to make it happen without a huge increase in cost.

Last but not least, the next upcoming challenge will be AI for safety. Additional questions arise as well when considering the systematic aspects of this technology, as the development process is completely different to our known and trusted V-cycle, and brings to the table new questions like biases, trustworthiness, transparency, etc. How can we leverage Artificial Intelligence and Machine Learning to support the safety concept of highly complex system?

JOIN NXP SEMICONDUCTORS AT

AUTOMOTIVE FUNCTIONAL SAFETY WEEK EUROPE 2024!

REGISTER FOR THE CONFERENCE TAKING PLACE AT THE MERCURE MOA BERLIN, GERMANY FROM 15TH - 18TH APRIL, 2024.

Register using code NXP10 to join Franck, Carmen, Marcus & Mat alongside 40+ expert speakers at Automotive Functional Safety Week.

14th Annual

AUTOMOTIVE FUNCTIONAL SAFETY WEEK 2024

Implementation of ISO 26262 & SOTIF

REGISTER HERE

DOWNLOAD THE AGENDA

Alice Andrews
Senior Conference Producer
Automotive IQ

Steven Wicks
Online Content Manager
Automotive IQ