Automotive iQ
a division of IQPC

INTERVIEW

"The interpretation side is really too open and therefore it's necessary to discuss the state of practice - how we could apply the standard in a common sense."

Automotive IQ **spoke with Helmut Martin of the Virtual Vehicle Competence Center to discuss the ISO 26262. He is working on a European Project called SafeCer that focuses on safety and reliability.**

Automotive IQ

Could you tell me about your background and your role at the Virtual Vehicle Competence Center?

Helmut Martin: From the background side, I can tell you that I've been working in the automotive industry and engaged in the field of Functional Safety for about three years. Before I started working at the Virtual Vehicle Competence Center, I was working for an automotive supplier here in Graz. There I was responsible for several functional safety aspects by supporting the development of safety relevant products, e.g. different process activities to integrate the functional safety requirements into company-wide processes. Since March 2011, I've been working at the Virtual Vehicle Competence Center for Area E – Electric/Electronic and Software to research on the topic functional safety for embedded systems. My role here is also to coordinate the contribution of the Virtual Vehicle to the European Union project, called SafeCer and also other different core activities in our embedded system group, also concerning the different aspects of functional safety.

Automotive IQ

We'll come back to the European project, in a little bit. To start with, what do you feel are the biggest challenges to the auto industry in terms of functional safety?

H.M.: At the moment, I think the new standard has been out since November 2011 and the different companies have to get more into the standard, because some aspects of the standard are specifications that are beyond current practice so that's a little challenging to fulfill all those requirements. The other aspect is that not all of the requirements can be fulfilled at the moment, so it's also a case of working on the standard and its applicability to the different phases of development life cycle.

Automotive IQ

Is there any particular section of the ISO 26262 that you feel is particularly challenging at the moment to the industry? I know it's divided up into about ten parts, if I remember correctly.

H.M.: Yes, let's start with the concept phase from part 3. This first phase is very vital in the overall development because that's where you set your automotive integrity level (ASIL) for the rest of the development activities. In terms of all the significant parameters to classify your system and your functions there, these are not really objectives defined and it depends on different scenarios, in my opinion. If you make the HARA with a group of people in Asia, you could get different parameters there in contrast to making this happen with people from Austria who live in a region with mountains and hillsides for example. This is very tricky in my opinion.

Automotive IQ

You think the interpretation side is a bit too open?

H.M.: Yes. The interpretation side is really too open and therefore it's necessary to discuss the state of practice - how we could apply the standard in a common sense. So, in another way, it could be a shift between different strategies and different market impacts. For example, your HARA results in a highly safety critical systems with ASIL D but another company says our system with the same functionality is only an ASIL A or B . So a common classification is really tricky in my opinion, so that there is no disadvantage for the different suppliers of the automotive market.

Automotive IQ

I've never thought about it that way.

H.M.: And if you have the wrong starting points in the concept phase it affects the overall development and then you have to deal with this problem and this would have a very big impact on your development effort and on the cost side.

Automotive IQ

And the worse thing is finding out later along the line that indeed it should have been a different ASIL category and you haven't prepared for that.

H.M.: Yes. That could be a real problem.

Automotive IQ

Automotive IQ: To continue on that a little bit, say five years down the line, when everybody's managed to implement this to one extent or another, how do you feel the ISO 26262 standard will actually impact the industry once it is implemented in a relatively robust manner?

H.M.: I think in five years from now there will be the first update of the ISO 26262 available. We will have a new version that is set out in such a way that we could actually apply the standard, I think. These actual on-going discussions about the ISO 26262 will provide a feedback loop for the second version of the ISO 26262 and I think it's necessary to have the standard near to the development and I think the second version will really be the applicable one.

Automotive IQ

Automotive IQ: So you definitely see a refinement going on in the process over the next few years?

H.M.: I think the processes of the different levels have to be extended. They're all very good quality approved processes at the moment but these safety concepts and the safety aspects have to be integrated in a better way and harmonized with the different roles in the supply chains. From OEM to the lower side of different suppliers and the whole chain, in five years, will be integrated and will have their overall integrated safety development and quality process.

Automotive IQ

Automotive IQ: Could you tell me about the European project you're working on regarding functional safety?

H.M.: Yes, the European project I'm working on is from the ARTEMIS JU European project (www.artemis-ju.eu). It's the Advanced Research and Technology for Embedded Intelligence Systems (ARTEMIS) and this joint undertaking focuses on different embedded system aspects. Embedded systems are integrated into everyday devices at the moment and their interconnection is increasing more and more. These networked systems bring us to the point that we have to consider all the different aspects from safety and security, because unknown fault scenarios are possible and security holes shall be avoided already during the development.
The focus of the ARTEMIS project is to research for useable methods and tools to improve the safety certification and reuse aspect for future generations of embedded products. One aspect here is that our project is called SafeCer (www.safecer.eu). It's one of the parallel ARTEMIS projects that are focusing on the topics safety and reliability. The title of SafeCer comes from the Safety Certification of Software Intensive Systems and we are working on methods and tools for the reusability of variable components. The elaborated methods should improve the development process by supporting the qualification and certification of safety-relevant products and tools for the development. We are working on the integration of methods for verification and validation to support these compositional designs for certification of different components in the system and software development process.

Automotive IQ

Automotive IQ: You mentioned the term reusable. Would you mind expanding on that?

H.M.: Yes, reusability in this context has different aspects. One side, in the ISO 26262, we could have the so called safety elements out of context (or SEooC) and we can use this SEooC approach for different software parts, for hardware parts, and also on the system level for system elements on the sub-system side. And then you could take these elements and integrate them to a higher-level system called an in-context system and you could use these components for system development of the item.

Automotive IQ

Automotive IQ: Because in theory the safety has already been checked?

H.M.: Yes. In the context system, you have to check all the aspects, if the integrated system fits in your overall system and if you could use it as it is certified. The concept there is to have smaller parts to the elements of those contexts which would be pre-certified or pre-qualified so they could be used in different safety systems for the higher integration level. That's a very interesting point and that's one aspect that we are working on here also for the reuse of components for different domains. It's not only for the automotive domain but some partners also want to use their components for the railway or for the avionics domain and I think that is very interesting.

Automotive IQ

Automotive IQ: But in this case we are talking about software architectures?

H.M.: It's not only for software. The concept could be used for different levels, for the basic software level, you could use the AUTOSAR approach for example, or for the functional software side or for different hardware parts, as well.

Automotive IQ

Automotive IQ: What are you hoping and aiming to get out of the conference?

H.M.: My hope and aim for the upcoming conference next month is to discuss all these aspects we are focusing on here in our project with the participants there and to get their feedback about their opinion about the possibilities of reusing of safety relevant software or components. Whether it's possible, what they think, where's the gap, what could be done, what could be improved from their side and I want to interact with the contributors there and have a little chat about other interesting functional safety topics.