Certification of Safety-Relevant Systems and Development Tools

Interview with Günter Glöe, TÜV Nord AG (Technical Inspection Authority)

Glossary:
IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PES)" is an international standard for functional system safety. Although the standard's stipulations and requirements are not prescribed by law, they must be observed as generally accepted technical procedures in the implementation of the appropriate functional safety of systems. Derived from IEC 61508, the new ISO 26262 "Automotive Safety Integrity Level" (ASIL) standard is being formulated by the ISO TC22/SC3/WG16 working committee.

Mr. Glöe, how would you describe your responsibilities at TÜV Nord?
As the person in charge of the certification office for software and electronics at our Technical Inspection Authority, I am responsible for all of the certifications required in the area of electronics and associated software. And this has been my profession for well over 30 years.

What is the function of the Technical Inspection Authority, or TÜV, as it relates to the certification of electronics and software?
Despite our location in Germany, we are an internationally recognized organization active in the area of quality assurance of both products and work processes. Known in our homeland as "the TÜV", we look back on a long tradition. In fact, the TÜV is an independent third-party service provider vested with the authority to verify that products or processes are being developed and/or carried out in accordance with requirements or specifications defined in advance. Our work complies with statutory law. By issuing its certification, the TÜV provides a service as contemplated by a free market economy as part of its relationship with the customer. This service is provided in accordance with the customer's wishes. There is no dictate saying that certification is mandatory.

Is the application of the IEC 61508 standard a statutory requirement or is it voluntary?
IEC 61508 is a basic standard concerned with reliable and safe technical systems and/or controls. If an enterprise claims to maintain the state of the art in its work, compliance with the IEC 61508 must be an integral part of that work.

What is the significance of the IEC 61508 certification of ASCET for ourselves as ETAS and for our customers?
For your company in its capacity as a manufacturer, a certificate combines two aspects. On the one hand, you can use your certificate for marketing purposes. On the other hand, by virtue of doing business in Germany, you are under an obligation to obtain quality verifications acceptable to the market as soon as you are selling safety-relevant products. It's not only typical in the context of electronics, and the regulations we use as a yardstick are not formulated by ourselves but set forth in the international IEC 61508 standard. Seen from the customer's standpoint, it is clear that a certificate quite naturally gives him the confidence that – to use an example – your ASCET tool represents the state of the art in this technology, and that it may be safely deployed for developments that fall into the framework of IEC 61508, for example.

Would you say that a verification that's not issued by an independent third party carries less weight?
Yes, indeed I would, and here's why. In Europe, generally speaking, one sees the following degrees of valence where examiners or testers are concerned: The lowest rung on the ladder is the first party, this being the manufacturer himself. The next higher step in terms of believability is the second party, that is, the customer himself. Needless to say, the highest degree of trust belongs to the third party, the independent organization.

Are there any differences between independent testing facilities?
There are some among the independent third-party testers who simply test for testing's sake, and then again, there are those who are known to possess recognized competence. In the context of the IEC 61508, our organization, the TÜV Nord, is recognized for its competence, that is, it is accredited. Organized under the auspices of the German Accreditation Council, the country's technical accreditation body (Deutsche Akkreditierungsstelle Technik e.V.) has confirmed to us that we possess the competence to certify adherence to the specifications of the IEC 61508 standard.

How does a certification take place?
In the first step, an agreement is reached regarding the requirements against which the certification will be compared. In our cooperation on ASCET, the IEC 61508 is the standard containing the requirements agreed upon, where the IEC 61508 determined which requirements must be met not only by the product, but also by the process used for the development of the product in question.

Is it necessary to submit the entire development documentation together with the request for certification?
Yes, it is. From the requirement and design documents, to testing specifications to internal working instructions, everything is checked by us, and it must be shown as part of the certification process. In other words, the first thing checked in the course of the IEC certification is whether suitable work procedures are being used.

What is the difference between a certification and the validation of a product by the customer?
In the course of a validation, a customer may discharge his obligation of due diligence independently of both certificate and manufacturer and satisfy himself as to the quality of a tool. In doing so, the customer is required to place his emphasis on the type of examination that he can conduct without input from, or dependence on, the manufacturer. When it is done by the customer, a validation examines the finished product. This process quite naturally involves the use of black-box testing methods whose scope is limited to examining the executable tool. And here's where the IEC 61508 makes a difference because it is based on the assumption that quality is generated in the development process. For example, a validation does not allow for any assessment of the consistency of maintenance instructions, operating manual, and coding guideline, all of which are looked at in the context of the certification.

Do you foresee a future increase in the need for certification?
If our observations serve as an indicator, the demand for certifications is on the rise. The same can also be said with regard to the automotive sector, for which a separate standard, known as ISO 26262, is being developed. Future certifications will therefore be based on IEC 61508 to a lesser extent, and to a greater extent on its derivative automobile-specific standard, the ISO 26262. Compliance with standards does more than address the safety aspect; it gives automakers a product that is both more reliable and more easily maintained. When you pay attention to the state of the art in terms of vehicle safety, you also ensure customer satisfaction. With many companies, the motivation for their safety-consciousness is not a knee-jerk reaction to tough safety requirements. Instead, they do this in order to raise the overall quality of their products.

Would you say that the availability of reusable AUTOSAR software components diminishes the significance of modeling tools such as ASCET?
No, not at all. The basic idea, which is to use tools like ASCET to develop with greater efficiency and maintainability at an abstract level, will remain valid. That way, at least a few segments of the certification of the overall system can be handled at the model level instead of the code level. By comparison, the certification of individual software components by means of a source code review is quite inefficient. We need good tools for deployment in the development process. The approach of measuring the development outcome in order to see whether the development was successful is unsatisfactory. What we need is a good development environment.