Q & A: Webinar “Top Misunderstandings about Functional Safety”

1. **How does TÜV SÜD look at the safety of wireless control medium?**

[Answer] Wireless medium can be handled from a safety point of view using a black-channel approach and an end-to-end safety layer. We have experts who could evaluate the safety layer protocols/devices and assess those with respect to the standard for safety communication layers e.g. IEC 61784-3.

2. **Are TÜV SÜD safety reports and certificates still valid if electronic components have to be changed because of obsolescence? What is the process to be followed in this case?**

[Answer] During the certification process typically a list of critical components will be created. Changes of such critical components require an impact analysis from the customer with related documentation (i.e. change records, test reports, design documents, ...). Based on this documentation the required re-assessment activities will be defined.
Changes of non-critical components require an impact analysis as well from the customer but no re-assessment. Means also the safety reports and certificates will stay valid. The related documentation (i.e. change records, …) will be typically checked by the annual factory inspection.

3. **How to determine SIL for system level since SIL can be determined for safety function - if SIL 3 what can be meant for hardware, software?**

[Answer] As you stated, the SIL is assigned to safety function and not to a complete system. However, the safety functions are performed by specific systems/elements and it is common to speak about SIL 3 hardware/software. A SIL 3 hardware/software element is a component which fulfil the related requirement of the standard (i.e. PFH and SC according to IEC 61508, SIL 3). Furthermore, according to IEC 61508 2nd edition the term element safety function was introduced to give clearer options of definition.

4. **Can the manufacturer of a product calculate the PFD/PFH, review the systematic aspects and provide the statement: "The following safety functions of our product meet the SILX" to the customer? Or only ISA can perform official statement that will be valid?**

[Answer] This depends on the industry. For safety components (e.g. according to Annex IV of the Machinery Directive) a statement (EC type examination certificate) from a Notified Body (as i.e. TÜV SÜD) is mandatory. In other industries a manufacturer statement might be sufficient in some cases for lower SIL (see table 4 and table 5 of IEC 61508-1), but usually a statement from a third party (or ISA) / notified body with the required accreditations supports the acceptance in the market. Eventual liability aspects depending on the industry domain should be regarded in such a context too.

5. **What is the relation between SILs and ALARP tolerability region? Can you really say that when you applied all the recommended and highly recommended measures for a specific SIL and you met the failure rates for it, that you reduced the risk of your system to a tolerable level?**

[Answer] SILs are the results of risk analysis, while ALARP is a way of handling risk management. The presence of systems which fulfils specific functional safety requirements, can be an argumentation to reduce the risk in the “broadly acceptable region”. Such decisions are of course specific to the risk analysis process and it is not correct to make a general statement, but the specific risk/safety function shall be analysed.

6. **Are there particular industry standards in Europe defining mandatory hardware requirements for an E-STOP circuit? Can solid state components be used for STOP switching mechanism or should they always be proven safety relays?**

[Answer] For emergency stop, the IEC 60204 could be a good starting point if we are talking about machinery. Depending on the risk analysis and the required integrity level/performance level, the hardware requirements can then be derived from standards like the ISO 13849. Having solid state components is not forbidden from a functional safety point of view. Sometime however there are additional requirements coming from customers/authority/industry practices. To provide more concrete answers, we would need to know more information about the system/industry considered.

7. **My company is system integrator and control panel manufacturer in railway & transportation automation industry. Does my company need IEC 61511 Functional Safety Management Certification for control panel production and/or software development as SIL compliant?**

[Answer] The IEC 61511 is the standard for the process industry, so the applicable standards for railway are the EN5012x series or (more generic) the IEC61508. A functional safety management certificate could be of course a benefit, but it is not mandatory.

8. **For proven in use can this also be applied to a compiler such as GCC?**

[Answer] For tools like GCC you can generally apply the proven in use argumentation as additional argumentation for claiming that the tool is fit for its purpose. However also for GCC the proven in use argumentation is only valid for specific version and usage (including command line parameters, option, etc.). This makes in practice the evidence for proven in use for software elements usually quite complicated.

9. **In which situations, can you relate performance level of a safety Function and the SIL Level required?**

[Answer] Performance levels are terminology part of the ISO 13849 and the machinery industry. It is possible to make some comparison and relationship (especially about the probabilistic failure targets), but no general direct relationship without further detailed investigation.

10. **What is meant by MTBF?**

[Answer] It means Mean Time Between Failure. It is usually used to calculate the reliability of a system/component and can be an input to calculate safety parameters like the PFH/PFD (see IEC 61508-4 definitions)

11. **Currently, IEC 61508 2dn edition dated in 2010 is still used. Is there any news regarding its 3rd edition? If so, what would be the potential updates?**

[Answer] The maintenance process for the 3rd edition of IEC61508 started recently, so the new edition is expected maybe 2021/2022. So, it is definitely too early to talk about updates. TÜV SÜD will prepare a seminar with the most important changes in the 3rd edition, but this may be available in Q3 of 2019.

12. **What is meant by SFF?**

[Answer] This means Safe Failure Fraction and defines in general the robustness of the Safety architecture against failures. The SFF is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. Usually the value is provided in percentage like 90%.

13. **If we have received different temperatures for doing the FMEDA, shall we do the FMEDA in the average temperature?**

[Answer] The FMEDA calculation should consider the operating conditions. If the operation conditions can include the highest temperature scenario, then you should perform the calculation also for that temperature range.