WHITEPAPER

IN SEVEN STEPS TO A SAFE PRODUCT

Introduction to Functional Safety

The demand for functional safety products in factory and production automation is growing exponentially. Consequentially the requirements for component manufacturers are increasing at the same pace. At the same time, standards compliance challenges the market newcomer. For example the IEC 61508, the relevant sector standards IEC 62061, IEC 61511 und ISO 13849 or the product specific standards EN 61800-5-2, EN 61496. These standards influence the technical requirements on the product as well as the development process and quality management system of the participating company.

The combined goal of functional safety is the prevention of negative consequences to life and limb. However all technical systems can malfunction. A 100% safety is not achievable. In the standards that's why the probability of failure is graded into levels. Exceedance of a certain level is not permitted – depending on the actual risk of hazards.

Many field failures can be traced back to errors in the specification. Therefore the standards specify extensive supporting measures for the prevention of systematic failures, associated to the various phases of the product life cycle – i.e. from product definition, encompassing product development right up to decommissioning.

Seven Steps to Product Functional Safety

The strict adherence of the standards base requirements, including the associated documentation, are the prerequisites for the concluding Assessment of the Functional Safety and a means to the minimization of liability risks in the event of damage or loss.

For beginners the following steps are recommended:

1. The Kickoff-Workshop
2. The Basic Training Course
3. Safety Plan, V&V-Plan und SRS
4. The Concept Approval
5. Design & Integration
6. Tests
7. Certification / Assessment

Step 1: The Kickoff-Workshop
Based on the product requirements it is possible at or even before project start to work out some possible solutions at the architectural level. If the product requirements are not yet formulated well enough, possible alternative solutions or options can be derived from the target application's key requirements.

During this process as early as possible one should consider the development process. Some requirements are already covered already through the company's standard processes. Possible gaps in the process can be identified and therefore avoid later delays in the realization of the process.

TIP: Is the product pursuing Certification through a Notified Body then get them involved early on. Practical experience shows us that the construction of the standards leaves room for interpretation.

Step 2: The Basic Training Course
If in the company there is no or little functional safety competence available, it is recommended to participate in a basic training course. On the first day, it makes sense that all the relevant company departments are represented. For R&D personnel it is worth participating in a further two to three day specialist course.

Step 3: Safety Plan, V&V-Plan, SRS
The *Safety Plan* is the central planning document for the project. It lays down the process to be applied, describes

the necessary qualifications and names the responsible persons in the project. As a rule of thumb, the smaller a Safety Plan can be correctly constructed by referencing company processes, means the better formulated the company's own process is.

In the *V&V*-Plan the development process's provided verification and validation activities as well as the associated responsible person shall be defined. Given this, it shall be ensured that later in the project the required inspections and approvals are performed the necessary diligence.

The *Safety Requirements Specification* (SRS) is comparable with the product specification. By a Safety Product there are however further parameters to be specified, like the to be reached SIL, the reaction time or maximum failure rate.

TIP: write down possible solutions in this phase and let them undergo a concept check, together with the other created documentation. In particular by new and complex development projects! The formulation of the technical concept is not as such required by the standards yet is very helpful in reducing project risks (*see also step 4: The Concept Approval*).

Step 4: The Concept Approval

The fundamental idea of the concept approval is to create a stable, viable fundament as prerequisite for later project success. Exactly because of the varied requirements contained in FS-Projects the project risks are not to be underestimated, which can lead to longer timescales, cost overruns or even to project cancellation.

After the concept approval the implementation can be tackled.

TIP: Involve as many experienced personnel as possible in the concept approval in order to minimize risks.

Step 5: Design and Integration

In this step comes a further fundamental idea of Functional Safety into action. As mentioned, supporting measures for the prevention of systematic failures must be embraced. A typical source for a systematic failure is too greater complexity. The standard required therefore a stepwise refinement of the product requirements / SRS, so that for the HW-/SW-developer more and more manageable requirements are created.

Subsequently the SRS will bind the following levels of a typical SW path:

- (System) Design Requirements Specification (SDRS), with device architecture
- Software Safety Requirements (SWRS)
- Software Architecture
- Software Design
- Coding

Forward and reverse requirements traceability between each level must be proven. Dedicated requirements tracking tools make the complexity of today's product development manageable. For the verification of the source code there are suitable Code-Reviews – including the use of static code analysis, against which predefined coding rules are checked.

The hardware path is more usually more granular. From the SDRS, the common umbrella document for the SW and HW development follows the creation of a Hardware Design Specification (HWDS). In this document the single blocks of the product architecture are precisely specified, for example the powers supply. Also the technical implementation is formulated. Finally, once this is completed the technical implementation of the circuit diagram and layout can occur.

The circuit diagram and the parts lists are used as input to the FMEDA, from which the important safety parameters PFH and PFD can be calculated.

Step 6: Tests

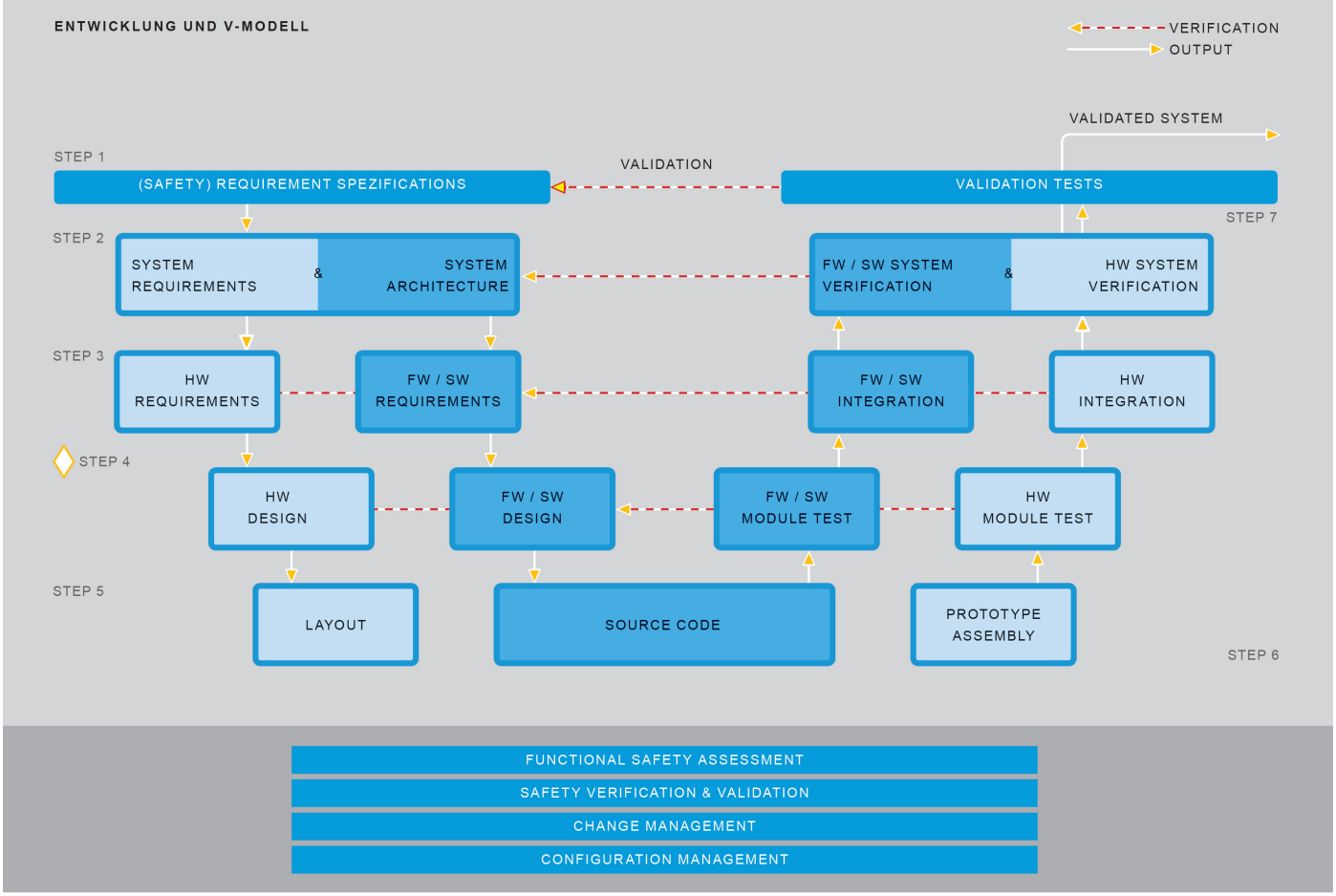
The tests stand – diagrammatically represented – on the right side of the V-Model and run from bottom-up. By the product development in the Industry automation mostly in three levels: Module tests, Integration tests and Validation tests. These tests are in theory always exactly performed against their associated level Requirements-/i.e. Design document on the left side of the V-Model.

This produces the typical pairs:

- Product Requirements / SRS – Validation tests
- Architecture – Integration tests
- Design – Module tests

At the Module and Integration tests level there is also a differentiation between HW und FW/SW-Tests.

The effort for the tests is high and therefore not to be underestimated. For the SW-Tests alone experience shows



that 80 to 100% of the SW-development effort may need to be applied. Therefore it is economically very sensible to go from the state “Quality will be added later into” to the state “Quality will be designed into” the code.

When all tests are passed and protocolled then the product can be submitted for Certification.

Step 7: Certification / Assessment
During the certification the whole development documentation is inspected and the fulfilment of the standards requirements re-enacted.

The assessor works mostly using individual checklists and then documents the results. Part of the assessment could have previously taken place during the development. This is definitely an interesting option for time critical projects.

In this case an attendance event can occur in which, partly in great depth, the details of the project are discussed, and here parts of the assessment are carried out.

In practice deviations can often not be prevented. The hand-in organization makes the necessary improvements and is then sufficient after.

After closing all open points the certificate is issued.

…where ideas turn into success!