FUNCTIONAL SAFETY

System FMEA in a safety project

Series of articles Functional Safety, Part 6

Introduction

The development of functionally safe components poses additional challenges for the developer. Unlike standard product developments, this puts forth normative requirements, which further increases the complexity of product development. These include architectural requirements of IEC 61508-2. Depending on the safety integrity level to be achieved, this standard sets concrete specifications as regards the hardware fault tolerance (HFT) and safe failure fraction (SFF) to be achieved. In addition to failsafe design principles, diagnostic measures of keys contribute to a high SFF.

Since the standard does not depend on the application and is abstract, users often face problems with the interpretation in practice. The presentation should help in mastering the progress from normative requirements to practical application. The professional article defines the typical requirements for factory automation (max. SIL3, requirement rate: High Demand).

Background

IEC 61508-2 calls for measures to avoid or rectify faults.
Faults can be classified as systematic and random. Systematic faults can occur in various phases of the product lifecycle. The standard accordingly formulates procedures and measures to avoid systematic faults such as application of project management, structured draft, documentation and tests on several levels.
These methods hence fall under quality assurance. These should be used to ensure that faults are not introduced into the product at all.

Methods for rectifying faults are different from these.
The rectification of faults is responded to by increasing the robustness of the product, e.g. against EMC influences, on the one hand and by identifying faults (during operation) and then taking subsequent fault measures on the other.
A typical measure is to switch the system to a safe mode. The key for identifying faults (during operation) are diagnostic measures that are implemented in addition to the desired safety function of the product.

This article describes the basic steps of identification, implementation and assessment of diagnostic measures on the basis of IEC 61508-2. A suitable tool for this is the Failure Mode and Effects Analysis – FMEA.

FMEA in the safety project

FMEAs are diversely used in practice and designated with a lot of different terms (process FMEA, design FMEA, …). The System FMEA is the most appropriate option to attain the objective of this article.

Further considerations are based on the following:

- System is understood as the product to be developed. From the point of view of IEC 61508, Subsystem would be the formally correct term because the product is generally only a part of the entire safety chain.
- System elements are parts of a high-level product-architecture. Individual components are first monitored in the subsequent Failure Modes, Effects and Diagnostic Analysis (FMEDA).
- This method is mostly used iteratively because FMEA can lead to necessary adaptations being made to the original architecture.
- As outlined, the determination of measures necessary for preventing faults, and diagnostic measures is at the primary objective of the analysis. Other measures resulting from the FMEA such as determination of training needs for employees or usage instructions for the product are not considered in this case.

	HARDWARE FAULT TOLERANCE FOR SAFETY-RELATED ELEMENTS					
	HFT=0		HFT=1		HFT=2	
SHARE SFF	**TYP A**	TYP B	**TYP A**	TYP B	**TYP A**	TYP B
< 60%	**SIL 1**	—	**SIL 2**	SIL 1	**SIL 3**	SIL 2
60% – < 90%	**SIL 2**	SIL 1	**SIL 3**	SIL 2	**SIL 4**	SIL 3
90% – < 99%	**SIL 3**	SIL 2	**SIL 4**	SIL 3	**SIL 4**	SIL 4
≥ 99%	**SIL 3**	SIL 3	**SIL 4**	SIL 4	**SIL 4**	SIL 4

Table 1: Correlation between HFT and SFF

MESCO Engineering GmbH | Berner Weg 7 | 79539 Lörrach | Phone +49 7621 1575 0 | Fax +49 7621 1575 175 | info@mesco-engineering.com | www.mesco-engineering.com

Influential factors for development as per IEC 61508-2

An overview of the influential factors during product development as per IEC 61508-2 provides transparency. The functional requirements and the requirements for safety integrity can be seen in the Safety Requirements Specification, which is often compared with the requirements specification book in practice. IEC 61508-2 directly defines several requirements that are partially interrelated.

Architectural requirements

The standard defines a correlation between the hardware fault tolerance (HFT) of an element, the required SIL and the safe failure fraction (SFF). In addition, the standard also distinguishes between elements that contain only simple components (type A) and elements that contain at least one complex component (type B). The connections have been compiled in the following table.

For better understanding: An element in this content are, for instance, all switching parts of a product, which provide power supply.

Diagnostic test interval and process safety time (PST)

The following is applicable for the High Demand or Continuous Mode requirement rate:
In case of single-channel elements, only those diagnostic measures can be taken into account, which identify faults within the process safety time and switch the system to a safe mode. In case of multi-channel systems, the specified Mean Time To Recover (MTTR) may be used as the maximum diagnostic test interval.

Fault models and DC

With the increasing desired diagnostic coverage (DC) for an element, increasingly complex fault models must be considered and the system must be checked for effects. For example, in case of an intended DC of 60%, a digital output must only be considered in the Stuck-at Low and Stuck-at High simple fault models. On the other hand, in case of an intended DC of 99%, the DC fault model, drift and oscillation must also be taken into account over and beyond the simple fault model.
Again, the higher DC can be used only if it is proven that these complex faults are also detected.

Diagnostic measures and attainable DC

The standard defines concrete diagnostic measures and their highest attainable DC. As help, the specified diagnostic measures have been described in more detail in IEC 61508-7. Since the effectiveness of the diagnostic measures needs to be proved, it is advisable in practice to not always demand the maximum attainable DC all-inclusively.

Failure tolerances for a safety function in the High Demand / Continuous Mode operating mode

Depending on the SIL to be attained, concrete tolerances for the rate of dangerous failures must be complied with. If the operating mode is High Demand / Continuous Mode, the name is PFH (Probability of dangerous failure per hour).

Remark: The attainment of a certain percentage of PFH is generally assumed for products/subsystems.

	PFH	
SIL	max.	min.
3	100 FIT	10 FIT
2	1000 FIT	100 FIT
1	10.000 FIT	1.000 FIT

Table 2: Failure tolerances PFH

Correlations and process in practice

The variety and the interdependence of the influencing factors complicate the application, especially in case of newcomers and often lead to sub-optimal results if used incorrectly. Typical negative consequences in practice are the need for adaptation developments that are detected late in the development cycle, but also over-engineering of safety measures that not only impacts the availability of the product, but also increases the price of the product unnecessarily.

The system FMEA should be considered as a tool to be used early in the development phase.

The following procedure is recommended:
- Design of the system architecture (without diagnostic measures)
- Creation of associated Reliability-Block Diagrams (RBD)
- Execution of the system FMEA based on block diagram and RBD
- Determination of diagnostic measures and DC to be attained
- Supplementation of diagnostic measures in the system architecture. If necessary, changes to the architecture and RBD when meeting the architectural requirements does not seem realistic (e.g. multichannel execution of the elements to reduce the requirements of SFF)
- Re-execution of the system FMEA and estimation of whether all the requirements of SRS and the standard can be achieved

If the architecture is stable, it can be converted according to the hardware path as per IEC 61508-2. If software is used for safety-related parts, the corresponding software path is applicable here as per IEC 61508-3.

device	failure rate λ	failure mode	fraction	effect	failure rate / failure mode	λ_s	λ_{dd} = DC *λ_d	λ_{du}
R1	**10 FIT**					**4 FIT**	**5.4 FIT**	**0.6 FIT**
		short circuit	40%	safe failure	4 FIT			
		open circuit	**50%**	**dangerous failure**	**5 FIT**			
		drift	**10%**	**dangerous failure**	**1 FIT**			
R2		…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
∑						**650 FIT**	**800 FIT**	**78 FIT**

Table 3: Exemplary FMEDA

The failure rates of the (element) safety function are determined towards the end of the Design & Development phase, based on the circuit diagram and the material parts list, as part of the FMEDA.

In principle, the FMEDA can be considered to be an extension of the FMEA. If elements were considered to be a black box at the (system) FMEA level, details about the internal structure of these elements are now available.

The (base) failure rate of each used component can be found in the manufacturer datasheet or a suitable database. Depending on the individual failure modes of the component, a safe or a "dangerous failure is seen at the element level, which results in a distribution of the basic failure rate *λ* to *λ_safe* and *λ_dangerous*.

The diagnosis is now beneficial for the effect, since it detects a part of the dangerous faults and the product is switched to the safe mode as a reaction to the fault. From the point of view of functional safety, the detected dangerous faults are thus no longer relevant. For comparison with the required SIL failure rate threshold, only the dangerous undetected faults *λ_du* are relevant.

In the case of single-channel (sub)systems, the following simple relationship is applicable:

- *PFH=λ_du*

Author: Dr. Johann Pohany
Managing Director
Medidtcine Consultants
www.medidtcine.com

Author: Armin Götzmann
Managing Director
MESCO Systems GmbH
www.mesco.de