



A UL WHITE PAPER

# UNDERSTANDING KEY CHANGES IN IEC 61508:2010



# The Importance of Functional Safety Development

First published in 1998, IEC 61508 is the principal standard of functional safety. The second edition of the standard — IEC 61508:2010 — has been in effect since April 2010, and covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. This second edition cancels and replaces the first edition, as it constitutes a technical revision.

A major objective of this standard is to facilitate the development of product and application sector international standards by the related technical committees. This will allow all the relevant factors associated with the product or application to be taken into account fully and thereby meet the specific needs of users of the product and application sector. A second objective of this standard is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.

*The significant and basic aspects of functional safety development, evaluation, and verification remain in the second edition, including the overall safety lifecycle, use of the V-Model for implementation of software development in particular, and the assessment of performance using Failure Mode Effects Analysis (FMEA) and other probabilistic calculations. However, important changes have particular impact on component manufacturers, resulting in a higher degree of confidence for manufacturers, integrators, and end users alike.*

*This paper addresses key changes in five critical areas of focus:*

- 1) Traceability
- 2) Elements
- 3) On-chip redundancy
- 4) EMC requirements
- 5) Clearer definitions of failure types

---

## Traceability

The need for traceability is clarified in the new edition. “When we start looking through the whole product development process, all phases ultimately trace to one another,” says Anura Fernando, research engineer, predictive modeling and risk analysis, at Underwriters Laboratories (UL).





Viewed from a broader perspective, rather than as a single component or device that is being developed with 61508 compliance, the concept of traceability can carry through to the overall supply chain. When a component is integrated into a system, the end user can look at what has been done at the component level to see how all the developmental activities tie together at that level, as well as how they tie together at the sub-assembly level and the system level.

“When we talk about traceability from an individual product perspective, we’re looking at everything that goes into the development effort, all the way from the product concept to the validation of the product,” says Fernando.

All the stages of development are involved in traceability: developing requirements for the product, determining the product design, applying proper verification techniques to make sure that the product is being designed and implemented correctly, implementing the verified product, testing to assure that each process has been achieved according to specification, then finally testing to ensure that the product’s original requirements have been met — that the customer’s need for the product has been satisfied. “From a risk management perspective, these kinds of things help to minimize systematic failures and defects that can be introduced into a product,” explains Fernando.

From a supply chain perspective, the second edition provides additional guidelines about what is required from a traceability perspective for

components that feed into the supply chain. Understanding the requirements for components relative to the different safety integrity levels (SILs) can provide a level of assurance for systems integrators. By having visibility into the component development process, they understand that using the same types of processes to build a larger system provides a consistent mechanism for risk management.

“Traceability is probably the key element in building the overall safety case for a safety-related control system or subsystem,” says Thomas Maier, principal engineer, functional safety, at UL. “Only if you have full traceability — from requirements and hazard analysis through concept design, down through every single component and every single line of code that goes into the system or subsystem (and further traceability to all the test cases and test results) — do you have a chance to build a really conclusive safety case for these complex systems.”

Traceability is also essential if working change management processes are to be in place. Whenever a safety-related certified product has been released and a “bug” is discovered or some changes are indicated, it is important to discover what is impacted by the proposed change: which parts, elements, or software functions will be affected. “The only way to find that out is if you have thorough and detailed traceability,” Maier concludes.

### Elements

“Element” is a newly introduced concept in the second edition of IEC 61508; all the development and verification

*“Only if you have full traceability — from requirements and hazard analysis through concept design, down through every single component and every single line of code that goes into the system or subsystem (and further traceability to all the test cases and test results) — do you have a chance to build a really conclusive safety case for these complex systems.”*

*— Thomas Maier,  
principal engineer*

calculations are now performed based on this concept. An element can be considered the lowest-level item from which a safety-related system is composed; it is at the base of the functional safety hierarchy. “As the lowest-level item, elements are where you begin,” says Maier. For example, the SIL parameter “safe failure fraction” is now to be determined for elements, and no longer for subsystems.

At the top of the hierarchy is the system, a complete, safety-related control system consisting of inputs, some safety-related logic, and safety-related output. In IEC terms, this is called an E/E/PE system.

This safety-related control system can be decomposed into subsystems: an input subsystem, then the logic subsystem, and then an output subsystem leading to the actuators. So subsystems, connected in series, are what build a complete, safety-related control system.

These subsystems can be further decomposed into the elements. Elements implement, for example, redundant channels. They can be connected in series and in parallel, if they belong to different channels. For example, a microprocessor can be an element in a safety-related logic subsystem.

If you develop a programmable safety relay, you select an architecture — say a two-channel one. Each of these channels needs to have a microprocessor — a microcontroller; in IEC 61508 terms, each of these microcontrollers would be an element. So to fulfill a certain SIL of the subsystem or safety-related control system, you have to fulfill hardware requirements and provide probability calculations concerning reliability that address random hardware failures. You also have to fulfill requirements concerning the use of stringent processes and methods for the development of software. These requirements address systematic failures.

### Synthesis of Elements

“The equation, ‘SIL 1 plus SIL 1 equals SIL 2’ has to do with the synthesis of elements,” says Maier. This means that, if you have two elements that are redundant (two elements that implement two channels, each channel

being independent of each other), you may achieve a kind of bonus regarding the systematic capability these elements have to fulfill. For example, if the overall objective is SIL 2, then each of the two elements would only have to fulfill a systematic capability of SIL 1.

### On-Chip Redundancy

The second edition of IEC 61508 defines stringent requirements for on-chip redundancy. Special architectural requirements for integrated circuits (ICs) with on-chip redundancy are given in a normative annex of the standard. This requirement is being driven by emerging technologies such as Field Programmable Grid Arrays (FPGAs) and advances in Application Specific Integrated Circuits (ASICs) that are helping to drive down costs by incorporating more functionality onto a single chip. A group of techniques and measures essential to preventing the introduction of faults during the design and development of these components has been introduced in the new version of the standard.

### EMC Requirements

The focus on electromagnetic compatibility (EMC) has increased significantly in the second edition of IEC 61508. In the old standard, the EMC requirements were not expressed very explicitly. They were sometimes forgotten or not as respected as they should have been. Now this has changed. “You cannot do a functional safety evaluation without looking at environmental impacts, and electromagnetic phenomena are among the most important environmental impacts to consider,” notes Maier.

It is electromagnetic immunity that is of critical importance to functional safety. All the immunity phenomena that are known and specified in the standards need to be considered. What is important for functional safety — what is required by the second version of IEC 61508 — is that testing go beyond the normal levels so that higher levels of electromagnetic immunity are considered to decrease the probability that electromagnetic phenomena could cause loss of the safety function.

Emissions are also included with immunity; but, in the United States, the Federal Communications Commission (FCC) typically deals with electromagnetic emissions. A few areas of functional safety (e.g., the elevator industry) are required to look at emissions and immunity because a system can itself generate emissions that could exceed tested immunity levels. But this is the exception.

“One should be clear in making a distinction between emission requirements and immunity requirements,” says Maier. “Functional safety is overwhelmingly about immunity and being protected against any electromagnetic emissions that could be expected in a certain environment.”

EMC is critical because it is a major common cause failure. As noted above, if you design a functionally safe product, it often has a level of redundancy: two channels that perform the safety function. This is how fault tolerance is achieved. Electromagnetic impacts could destroy or disturb



both channels at exactly the same time, meaning the loss of the safety function. That's a "common cause."

"If you have a safety-related control signal, that signal is supposed to look a particular way," says Fernando. "Electromagnetic interference can distort the signal so that it looks very different, and this distortion (i.e. change in waveform or waveshape) has the potential to cause the system to respond in an unexpected, and possibly unsafe way."

Two IEC standards specifically address EMC requirements in relation to functional safety: the technical specification IEC/TS 61000-1-2 and IEC 61326-3-1. These are referred to in the second edition of IEC 61508.

### Clearer Definitions of Failure Types

The second edition of IEC 61508 has the same definitions of a safe failure and a dangerous failure; but, it goes on to define a new "no effect failure" and a "no part failure" that are important to understand. A no effect failure is the failure of a component that is part of the safety-related circuit, but which has no effect on the safety function at all when it fails — it doesn't make the system fall to the safe side or the dangerous side. A no part failure is a failure of a component that is somewhere in the system, but is not related to the safety related circuits.

The first edition of IEC 61508 allowed the consideration of no effect failures as being safe failures. Furthermore,

it was always a bit doubtful that no part failures could be considered for calculating the safe failure fraction. The second edition of IEC 61508 makes it very clear that these two types of failures must not be considered in doing the calculation of the safe failure fraction.

"Under the first edition, this was not clearly stated," says Maier. Component manufacturers could, in principle, embellish their figures. "You could make them look better by including no part failures and inventing some additional no effect failures to improve the percentage of non-dangerous failures," notes Maier.

Now you are only allowed to consider real safe failures and real dangerous failures. All other failures that are not part of the safety circuit or have no effect on the behavior of the safety circuit must not be taken into consideration.

### Something Else You Should Know

Since UL personnel have participated in the writing of the second IEC 61508 standard, we are ideally positioned to help you understand its nuances.

Whether you are an experienced manufacturer that currently has products certified under the first edition of IEC 61508 and are now looking to convert to the second edition, or you are new to the functional safety space and the second edition is your first involvement with functional safety certification, UL is here to help. What's more, UL has people who can assist every step of the way, from our functional safety mark, to certification,

to advisory consultative services that can train, coach, and educate your staff.

For more information on how we can help you with the second edition of IEC 61508 and other functional safety issues, please contact Kevin Connelly at 1.631.546.2691, or by e-mail at [kevin.connelly@us.ul.com](mailto:kevin.connelly@us.ul.com), or visit us at [ul.com/functionalsafety](http://ul.com/functionalsafety).