Top 5 Misunderstandings About Functional Safety

TÜV SÜD has more than 20 years of experience in testing and certifying functional safety related systems and components. During this time our employees have observed recurring issues arising from misunderstandings of some functional safety concepts.

1

SIL Does Not Mean Reliability of the Control System

A safe state of Equipment Under Control (EUC) is a result of the hazard and risk analysis and depends on its different operational modes. In this context, we frequently observe misunderstandings about strategies and concepts regarding fail safe scenarios. A SIL therefore is only a degree of reliability that the safety function will perform as intended when it is required to put the EUC in a safe state.

2

Watchdogs and Microcontroller

Watchdogs of microcontroller (µC) often just reset the controller but do not control any outputs in a direct independent way. It is not enough to use an internal watchdog, because it is not guaranteed that the output will go into the desired state: the internal watchdog is part of the defect microcontroller, therefore it cannot be guaranteed that it works correctly.

3

Definition of SIL

The definition of SIL (safety integrity level) applies to functions that have been in origin derived by some kind of risk analysis/classification. A more correct definition is that a “system is capable to implement safety functions up to SILx”.

4

SIL is Not the Same as SIL

The abbreviation SIL (Safety Integrity Level) is used by several standards. In each standard, it relates however to different process, architectural and technical requirements. Some of the standards use different abbreviations like ASIL (Automotive SIL). Some others use the same abbreviation (SIL), with the risk of confusion and misunderstandings.

5

Increasing SIL by Redundancy

It is not possible to raise the SIL level of a system combining systems having no safety evidence or using homogeneous redundancy. For example, it is not possible to increase the SIL to SIL4 by simply combining several SIL2 systems/channels (e.g. reach SIL3 on system level by several SIL2 Control Systems).

Learn more about more common misunderstandings and how to avoid such errors in future safety projects.

www.tuvsud.com/en-us/resource-centre/webinar/top-misunderstandings-about-functional-safety