Develop your functional safety signal chain application with Texas Instruments

Questions and answers

Answered during the webinar:

Q: Diagnostic circuit is generally 1 SIL level below the main channel, and even 2 SIL levels below if HFT=1?

A: Diagnostics may be SIL(x-1) in single channel system with requirement SIL(x). For redundant systems with HFT=1 diagnostic the SIL may be further reduced. Please verify your design with your preferred certifier.

Q: Do passive components like resistors and capacitors are considered affect functional safety functions and validation?

A: Passive components are also affecting functional safety, just like other components. Failure modes and FIT rates are available.

Q: How is EMC handled in such a system?

A: Influence of both channels at the same time not considered. This Common-Cause factor (CCF) needs to be addressed by design.

Q: What if one channel has a fault, but results are ok? And, what if two channels have faults, but results of both channels are the same?

A: Single fault leading to the same results is accepted. Double faults are not considered. Faults must not have CCF root cause. E.g. if only one channel has a fault, but the results are okay, this means the safety goal is not violated. This would not be a problem then. E.g. if the ADC has a gain error of 1% due to a random hardware fault, but the FS accuracy is specified at 3% then this would not be a problem.

Q: Is the comparison of channels not enough? Why all the additional diagnostics?

A: Some of the presented diagnostics may be removed, but when you do plausibility check between two channels then you can omit most of the ADC individual diagnostics. If "availability" is a care about. In that case you would need to figure out which device is faulty. Otherwise, please verify your design with your preferred certifier.

Q: You didn't mention double or triple failures (within a given test cycle) and the consequent Fault Tree Analysis, but only FMEDA for single failure. Is only FMEDA enough?

A: During this IEC61508 assessment only single faults were considered.

Q: Can I use any type of components (MUX, ADCs, etc.)? Or components need to be rated with functional safety standards?

A: Any component from TI portfolio may be used in a functional safety application. Failure modes of the component need to be addressed by diagnostic until the required Safe-failure fraction (SFF) is reached.