

Calculation of Failure Detection Probability on Safety Mechanisms of Correlated Sensor Signals According to ISO 26262

Wolfgang Granig and Dirk Hammerschmidt
 Infineon Technologies AG

Hubert Zangl
 Alpe-Adria University Klagenfurt

ABSTRACT

Functional safe products conforming to the ISO 26262 standard are getting more important for automotive applications wherein electronic takes more and more response for safety relevant operations. Consequently safety mechanisms are needed and implemented in order to reach defined functional safety targets. To prove their effectiveness diagnostic coverage provides a measurable quantity. A straight forward safety mechanism for sensor systems can be established by redundant signal paths measuring the same physical quantity and subsequently performing an independent output difference-check that decides if the data can be transmitted or an error message shall be sent. This paper focuses on the diagnostic coverage figure calculation of such data correlation-checks for linear sensors which are also shown in ISO 26262 part5:2011 ANNEX D2.10.2. This principle is widely used in automotive application like magnetic field sensing for steering-torque measurement, position detection of throttle-valve or current sensing of actuators. It is shown how the diagnostic coverage figures can be derived based on statistical evaluation using different typical failure-probability distributions of the analog and digital elements of the sensor systems. The incorporation of temperature and lifetime drifts that are part of the specification of all mixed signal systems and their influence on the diagnostic coverage will be discussed for different configurations of the safety requirements. These diagnostic coverage figures are essential for quantitative Failure-Tree Analysis (FTA) or Failure Mode, Effect and Diagnostic Analysis (FMEDA), which is the proof of the system capability to achieve its safety requirements.

CITATION: Granig, W., Hammerschmidt, D., and Zangl, H., "Calculation of Failure Detection Probability on Safety Mechanisms of Correlated Sensor Signals According to ISO 26262," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 10(1):2017, doi:10.4271/2017-01-0015.

INTRODUCTION

The ISO 26262 standard [1] was developed as functional safety standard of electrical and/or electronical systems for road vehicles and is getting more important for automobile development. The standard contains considerations concerning systematic failures which are addressable by methodologies for development, fabrication, operation and maintenance of a product and random hardware failures caused by arbitrary fault events during product lifetime. The random hardware failures are addressed by the statistical analysis in this paper with a special focus on dual channels sensors. The ISO 26262 standard defines several ASIL levels defining measures for systematic and random hardware faults; these levels are defined from A until D, where D represents the highest ASIL rating which can cause death of several people if a safety goal is violated. The standard contains a part which deals with the "Product development at the hardware level" (ISO 26262 part 5) in detail defining target metric values for the different ASIL Classification on vehicle system level (see Table 1). Even though this allows to balance between the metric contributions of sensors, controllers and actuators it is common practice to target the single point fault metric (SPFM)

and latent fault metric (LFM) for each device especially if it is a "System Element out of Context" (SEooC) which will be used in different systems. For the PMHF the target for the SEooC should obviously be below the value stated in Table 1 in order to leave headroom for other contributors on system level.

Table 1. This is an overview of requirements for different ASIL-Levels

Metric	ASIL B	ASIL C	ASIL D
Probabilistic Metric for Random Hardware Faults (PMHF)	10^{-7} h^{-1} (100 FIT)	10^{-7} h^{-1} (100 FIT)	10^{-8} h^{-1} (10 FIT)
Single Point Fault Metric (SPFM)	$\geq 90\%$	$\geq 97\%$	$\geq 99\%$
Latent Fault Metric (LFM)	$\geq 60\%$	$\geq 80\%$	$\geq 90\%$

The probabilistic value of random hardware faults (PMHF) value is related to common experiences with used devices of microchip integrated systems. Failure Rates are also defined as "Failure Rate in Time". 1 Fit is one fault in one device in 10^9 hours, or 1 fault in one

hour at 10^9 devices. Standards exist which define a FIT-rate related to a certain chip-area. These standard base failure rates are often taken as guideline for comparison of different integrated solutions of independent of manufacturer's field data (see Table 2). Considerations on the application of the ISO 26262 on semiconductor components for the use in automotive systems can be found in ISO/PAS19451 [4].

Table 2. This is an overview of different base failure rates for semiconductor products used in SPFM and LFM calculations.

Method	Failure Rate Calculation
IEC/TR62380	Based on used transistors in a certain mission temperature profile of operation and non-operation time. Chip Package considerations also defined in addition separately [2].
SN29500	Reference Failure Rate based on transistors, gates or bits with correction factors for operating voltage, temperature and drift. Chip-Package inherently included in given numbers [3]
FIDES Guide	Fault rates comprise the physical and the process contributions. Fit rates are scaled by annual life-profile and mission-duration. The fault rate is also scaled with acceleration factors like thermal, electrical and mechanical stress for real stress and additionally for overstress (induced stress) [4].
“Proven in Use” (ISO 26262)	Real numbers from hardware in use. Here real faults/h violating the safety-goal must be documented (eg.: ASIL D < 10^{-9} faults/h). This method is rarely used in practical field because most safety-analysis focus on new products

The possible hardware faults can be separated in several classes. An explanation including defined variables which are used in following equations can be seen in Table 3. The contribution to the overall fault rate is expressed in Equation 1.

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF,L} + \lambda_{MPF,DP} + \lambda_S \quad (1)$$

The Single-Point Fault Metric (SPFM) can be calculated according to Equation 2 considering Single point Faults λ_{SPF} directly violating the safety goal uncovered by any safety mechanism and residual faults λ_{RF} which are not detected by safety mechanisms.

$$SPFM = 1 - \frac{\sum(\lambda_{SPF} + \lambda_{RF})}{\sum \lambda} \quad (2)$$

The Latent Fault Metric (LFM) can be calculated according to Equation 3 using latent multi-point fault rate λ_{MPF} which considers faults which are not directly violating the safety goal, but if a second fault occurs subsequently it may be elevated by the undetected first fault to violate the safety requirement. For this calculation the single point faults and residual faults must be excluded, therefore λ_{SPF} and λ_{RF} are subtracted from the overall failure rate λ

$$LFM = 1 - \frac{\sum(\lambda_{MPF,L})}{\sum(\lambda - \lambda_{SPF} - \lambda_{RF})} \quad (3)$$

The diagnostic coverage $K_{DC,RF}$ of a safety mechanism detecting a fault of a hardware-part is expressed in percentage using the residual failure-rate according to Equation 4.

$$K_{DC,RF} = 100 \cdot \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \quad (4)$$

The same diagnostic coverage can be calculated for the latent faults. The latent fault diagnostic coverage $K_{DC,MPF,L}$ expressed in percentage can be calculated according to Equation 5.

$$K_{DC,MPF,L} = 100 \cdot \left(1 - \frac{\lambda_{MPF,L}}{\lambda}\right) \quad (5)$$

The ISO 26262 standard part 5:2011 ANNEX D provides several proposals to implement safety mechanisms to increase the diagnostic coverage and also gives a first idea for the achievable diagnostic coverage, which can be used in the initial analysis of complex, large or safety critical systems. This paper especially focuses on Chapter D.2.10.2 which defines mechanisms for sensors; examples are shown in Figure 1 and 2.

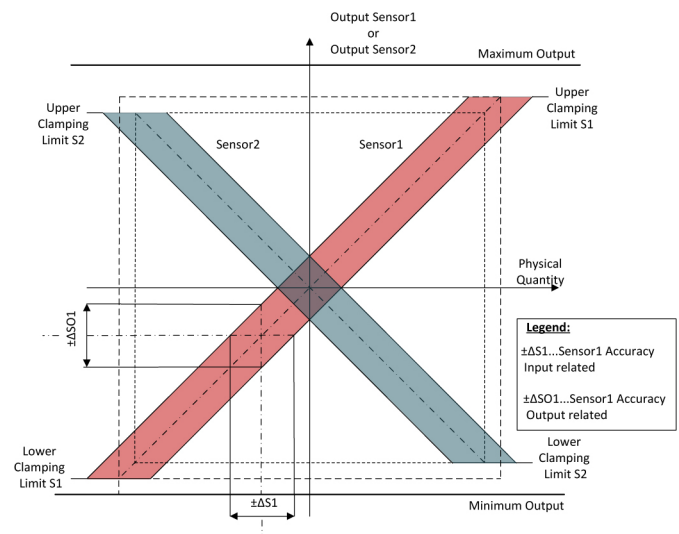


Figure 1. This is a more detailed figure of ISO 26262 part 5:2011 ANNEX D.2.10.2 [1] describing the safety mechanism for sensors to detect range drifts, offset or other errors using two redundant sensors. Here also the individual deviations of each measurement-channel are shown.

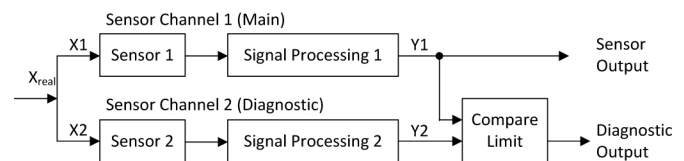


Figure 2. This is a block diagram of the signal processing chain of two independent sensor channels. Channel 1 is used for the sensor output and the redundant channel 2 is used for safety-comparisons and diagnostic output generation via the “Compare-Limit” block. X_{real} represents the real physical values and $X1$ and $X2$ the back calculated physical values from signal processing output $Y1$ and $Y2$.

The goal of this paper is to give a methodology to calculate the worst case diagnostic coverage of safety-mechanisms mentioned in the ISO 26262 for redundant sensor channels correlated via the measured property including real world example quantities. The calculation of the physical sensed value X out of the sensor output value Y of each channel can be modeled as linear dependent function according to Equation 6 via a transfer-coefficient k and d (index n shows the according channel).

$$X_n = k_n \cdot Y_n + d_n \quad (6)$$

This paper focuses on the diagnostic coverage calculations related to re-calculated physical quantities X_n out of each sensor output value Y_n .

Table 3. Fault classification and used symbol for following equations

Class	Symbol (rate)	Explanation
All Faults	λ	Total failure rate of a safety-related hardware element. Can be expressed according to Equation 1 and assuming all faults independent and following an exponential
Single Point Fault	λ_{SPF}	Single point faults directly cause a violation of the safety-goal. There is no safety mechanism implemented to detect this fault.
Residual Fault	λ_{RF}	The residual faults are faults that are not covered by an implemented safety mechanism.
Latent Multi Point Fault	$\lambda_{MPF,L}$	Latent multi-point faults are faults that do not directly violate the safety goal, but do so if another fault occurs. One example for this is a fault in a safety mechanism.
Perceived Multi Point Fault	$\lambda_{MPF,DP}$	These are multi-point faults that are perceived or detected by a safety-mechanism.
Safe Fault	λ_S	Safe faults do not lead to a violation to the safety goal.

DIAGNOSTIC FUNCTION

First we need to define a safety requirement as input for our diagnostic coverage calculation including clear pass and fail criteria of this safety-requirement. Statistical accuracy figures of the two redundant data paths have to be derived in order to allow calculate the final detection-probability of random faults.

Safety Requirement

The safety requirement must be broken down to the sensor element from the system safety-goal which is an assumption for a SEooC. At the end safety requirements for redundant sensor system come down to a form like the ones shown in Table 4.

Table 4. Example safety requirement broken down from a system safety goal

Sensor Technical Safety Requirement (Example)
Faults leading to an error of the measured magnetic field signal which results in a signal deviation of more than Δs_{af} of the full measurement range in either channel with respect to initial system calibration shall be detected and initiate a defined failure reaction.

Safety Mechanism

This requirement is important to define a safety mechanism to detect this failure and an according failure reaction in the safety-concept. In our case we choose the proposal of ISO 26262 part 5:2011 ANNEX D2.10.2 [1] and define two independent measurement signal paths using different output signal slopes and different clamping limits for both sensor signal channels. The independence of the channels has to be proven using a DFA (Dependent Failure Analysis) which is not the main focus of this paper which concentrates on the quantification of the probabilistic figures. Further we define a safety-mechanism which compares the two sensor output signals and initiate a failure reaction in case that their difference exceeds a certain limit. In case of independent ideal sensors having no accuracy tolerance, residual temperature dependence or lifetime-drifts, this safety mechanism would provide a 100% diagnostic coverage since the independence assures that a fault only appears in one of the channels. Consequently we could define a very small tolerable difference and any failure will be either detected immediately by the difference check or no deviation from the correct measurement is present. To reduce dependencies between the channels opposite slopes are defined. Faults leading to a manipulation of both output signals synchronously will be detected by the output comparison. Even if there is a large disturbance of both channels in one direction, the two independent different clamping limits of channel 1 and 2 will cause a difference in the output signals, which is detected by this comparison check.

Definition of Sensor Deviations

In real life we have to consider the limited accuracy of both sensor signal channels. We have to consider calibration inaccuracy, residual temperature dependence after compensation, lifetime and any other drifts (example: chip package related drifts caused by humidity or mechanically induced chip-stress). These influences are collectively described by uncertainty-offsets which can be expressed in the model Equation 7. X represents the sensor output in physical units, X_{cal} represents the ideal sensor output in physical units (could be also after end-of-line calibration value), ΔX_{unc} is the measurement-uncertainty modeled as offset and ΔX_{fault} the additive fault deviation in physical dimensions. The corresponding uncertainty-values of these deviations are usually specified as standard deviations in the data sheet of the device. It shall be recognized that these effects are unavoidable parts of the behavior of a sensor in absence of any fault.

$$X = X_{cal} + \Delta X_{unc} + \Delta X_{fault} \quad (7)$$

To fulfill the safety requirement the output-deviation to the ideal transfer-function is not allowed to be larger than the limit Δ_{saf} defined in the safety-requirement coming from customers or from a safety architecture according to Equation 8 with Δ_{saf} representing the safety requirement limit. Obviously the effect of the deviations defined in Equation 7 has to be below the limit that infringes the safety criterion. A visualization of this requirement is also shown in the Venn-diagram in Figure 3 [5].

$$\Delta X = |X - X_{cal}| < \Delta_{saf} \quad (8)$$

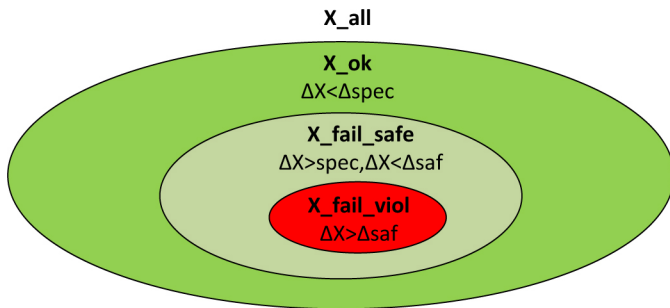


Figure 3. This is a Venn-diagram of all sensor output possibilities. If the output value-deviation is within the specification limit the output values are ok (X_{ok}). If the output-value deviation is larger than the specification limit but lower than the safety limit these faults are safe (X_{fail_safe}). The last possibility is an output value-deviation exceeding the safety limit (X_{fail_viol}).

Definition of Sensor Safety Mechanism Deviations

To detect this deviation from the main sensor channel output X_1 a second redundant sensor X_2 (Sensor 2 shown in Figure 1) is used to measure the difference dX of the two sensor outputs as shown in Figure 1, 2 and Equation 9. In case the difference of the measurements delivered by both channels exceeds a safety-mechanism-limit threshold ($dsml$) this should be indicated by a safety reaction. For an initial approach the threshold of this safety-mechanism limit is set equally to the safety limit ($dsml = \Delta_{saf}$). Equation 10 shows that inserting Equation 7 into Equation 9 results in dX only depending on the sensor uncertainties and faults.

$$dX = |X_1 - X_2| < dsml \quad (9)$$

$$dX = \Delta X_{unc_1} + \Delta X_{fault_1} - \Delta X_{unc_2} - \Delta X_{fault_2} < dsml \quad (10)$$

Figure 4 shows a tabular representation of the possible sensor output values including the described safety-mechanism [5]. In this combination we also get deviations of the main channel 1 (ΔX_1) larger than the safety-limit Δ_{saf} which are not detected (CASE 4). There are also situations where faults are indicated and the deviation of X_1 is smaller than the safety-limit, which represents a false-alarm (CASE 5 and 6).

CASE	$\Delta X_1 < \Delta_{spec}$	$\Delta X_1 < \Delta_{saf}$	$dX < dsml$	safety	availability
1	$\Delta X_1 < \Delta_{spec}$	$\Delta X_1 < \Delta_{saf}$	$dX < dsml$	safe fault	available - in spec
2	$\Delta X_1 > \Delta_{spec}$	$\Delta X_1 < \Delta_{saf}$	$dX < dsml$	safe fault	available - out of spec
3	$\Delta X_1 < \Delta_{spec}$	$\Delta X_1 > \Delta_{saf}$	$dX < dsml$	not possible	not possible
4	$\Delta X_1 > \Delta_{spec}$	$\Delta X_1 > \Delta_{saf}$	$dX < dsml$	undetected fault - not safe	available - out of safety limit
5	$\Delta X_1 < \Delta_{spec}$	$\Delta X_1 < \Delta_{saf}$	$dX > dsml$	safe fault	unavailable - false alarm
6	$\Delta X_1 > \Delta_{spec}$	$\Delta X_1 < \Delta_{saf}$	$dX > dsml$	safe fault	unavailable - false alarm
7	$\Delta X_1 < \Delta_{spec}$	$\Delta X_1 > \Delta_{saf}$	$dX > dsml$	not possible	not possible
8	$\Delta X_1 > \Delta_{spec}$	$\Delta X_1 > \Delta_{saf}$	$dX > dsml$	detected fault	unavailable

Figure 4. This overview shows all possible output situations of the main sensor X_1 and all possible situations in combination with the second redundant sensor channel X_2 . We distinguish between ΔX_1 smaller or larger than the specification limit “ Δ_{spec} ”, ΔX_1 smaller or larger than the safety limit “ Δ_{saf} ” and the difference between X_1 and X_2 (dX) smaller or larger than the diagnostic limit “ $dsml$ ”. Case 4 is the dangerous fault which is not detected and this is reducing the diagnostic coverage.

Figure 1 shows a real world implementation scenario for these two correlated sensor output signals for fault diagnostic reasons. Each of the individual signals consists of the ideal transfer-function with superimposed deviation-components modeled as offset contribution caused by residual temperature-drifts, lifetime-drifts, end-of-line calibration deviations and noise. Finally we can define a transfer-function band around the ideal transfer-function representing the real-life deviations. This kind of setup uses two different sensor channels with inverted output slope for easier detection of common influences on both sensor-channels and different clamping limits to easily detect short to VDD or GND of one or both sensor channels.

In general we have to distinguish between the safety requirements limit “ Δ_{saf} ” which defines the maximum deviation of the sensor module output channel, defined as allowed positive and negative deviation from end of line calibration to fulfill the safety requirement. The used safety mechanism to compare both channel outputs also has a limit called “ $dsml$ ” (Safety Mechanism Limit). It is also defined as positive and negative allowed tolerance between both channels (see Equation 9). Now the measurement channels have specified deviations of temperature and lifetime-drifts. An overview of possible combinations out of actual measurement values of X_1 and X_2 shown in Figure 5 can be seen in Figure 6 and 7. There you can see the resulting tolerated failure deviation limits “ d_lim_p ” for the positive allowed tolerance and “ d_lim_n ” for the negative allowed tolerance by the implemented safety mechanism (see Equation 11 and 12). These remaining tolerances are applied now to the deviation of X_1 (ΔX_1) and we get the detection gap (see Equation 13) where the diagnostic mechanism does not react but the safety-limit is violated. We also get the diagnostic gap on the other side of the distribution mainly when ΔX_2 gets negative (see Equation 14).