Diagnostic Coverage Estimation Method for Optimization of Redundant Sensor Systems

Wolfgang Granig[1], Dirk Hammerschmidt[1], Hubert Zangl[2]
[1] Infineon Technologies Austria AG
[2] Alpen-Adria Universitaet Klagenfurt
wolfgang.granig@infineon.com

***Abstract*—In this paper we present a method to calculate estimated values for diagnostic coverage and false alarm rates of two channel redundant sensor systems. Avoiding time-consuming methodologies going into detail of system-sub-block failure rates and detailed fault cases we show a worst-case approach based on statistical methods. Diagnostic coverage and false alarm rates are important to develop a safety concept and to perform a functional safety analysis for sensor systems in safety critical applications. The proposed methodology additionally enables global sensor system optimizations including these dependability requirements.**

Keywords—redundancy; diagnostic coverage; false alarm; sensor optimization; functional safety

I. INTRODUCTION

Today's sensor systems must be optimized according to several requirements to be competitive in the market. Typically, optimizations are done by comparisons of different sensor implementations with respect to the requirements [1] or by insertion of additional error-compensation algorithms [2]. Also statistical techniques [3] have been suggested to reduce sensor system deviations. Additionally, dependability requirements for functional safety [4] or availability requirements increase - especially for automotive and autonomous systems - and these requirements need to be met.

Research on defining the diagnostic coverage of systems for safety critical applications is done by fault injection simulations of each potential fault case [5]. This is the most accurate way to define the diagnostic coverage of safety mechanisms in sensor systems but it requires exact knowledge of the particular implementation and it is very time-consuming. Especially during concept definition of sensor systems we need to have good prediction of sensor performance and we need to define appropriate safety mechanisms to meet diagnostic coverage and maximum false alarm rates. In the following chapters we will present how the estimation of diagnostic coverage and false alarm rates can be performed even in early concept phase or without extensive fault-injection simulations. This work simplifies and completes the first ideas presented in [6], which were based on finding the diagnostic and availability gap first and then determine the probabilities of those. In this approach we directly start from probability density functions of specified sensor deviations and apply several statistical fault models by superposition. This methodology was successfully applied to the first monolithically integrated Hall-sensor based dual-channel magnetic field sensor concept for safety-critical automotive applications [7].

II. DUAL CHANNEL REDUNDANT SENSOR SYSTEM

A. Dual Channel Redundant Sensor System Setup

Basically, there are two options on how to combine two redundant sensor channel outputs for further signal processing. First option is to use the second channel only for detection of a fault in the first channel as described in [4] and [7]. The disadvantage in this case is that the second redundant channel does not contribute to improve the sensor output. In case of a fault in the second channel, the sensor output is correct but a false alarm is issued with quite high probability. In this paper we focus on the second option to use both sensor channel output signals for generation of the sensor output value as well as to use both for fault detection (Fig. 1).

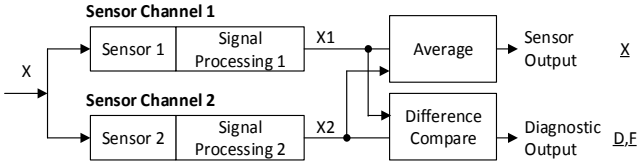

Fig. 1. Dual channel redundant sensor system setup where both channel outputs are used to determine the sensor system output and diagnostic output. X represents the sensor system input, X1 and X2 represent the converted signals and $\underline{X}$ represents the overall sensor system output. $\underline{D}$ represents the channel difference and $\underline{F}$ the binary diagnostic decision accoring to a certain safety mechanism dianglostic limit.

The calculation if the deviation is larger than a safety requirement limit "dsaf" is given in equations (1) (2). The safety mechanism however is used to detect a larger difference of both channels than a certain safety mechanism limit "dsml" (3) (4). Lower case letters represent the channel deviations from ideal values.

$$\underline{X}=(X1+X2)/2 \quad (1)$$

$$abs(X-\underline{X})<dsaf \rightarrow abs(x1+x2)<2*dsaf \quad (2)$$

$$\underline{D}=X1-X2=x1-x2 \quad (3)$$

$$If\ abs(\underline{D})>dsml\ then\ \underline{F}=1\ else\ \underline{F}=0 \quad (4)$$

B. *Sensor Deviation and Fault Modeling*

Each sensor channel output can be modeled as superposition of ideal calibration value X_{cal}, measurement uncertainty value X_{unc} and fault value X_{fault} as shown in (5) for channel 1. Channel 2 is modeled in the same way.

$$X1 = X1_{cal} + X1_{unc} + X1_{fault} \quad (5)$$

The measurement uncertainty of each channel has to be estimated or calculated according different systematic and statistic deviation contributions of offset, gain and noise. An example of possible sensor channel deviation distributions without a fault can be seen in Fig. 2 expressed relatively in Full-Scale-Range scaled parameters (FSR).

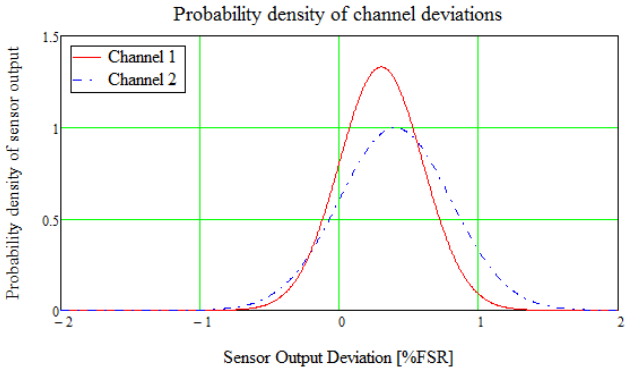

Fig. 2. Example sensor channel output deviations without a present fault. Channel X1: Systematic μ1 = 0.3%FSR, Statistic σ1= 0.3%FSR 1σ Channel X2: Systematic μ2 = 0.4%FSR, Statistic σ2 =0.4%FSR 1σ where μ represents the mean and σ the standard-deviation.

Faults are modeled as superimposed deviations according to (5) and (6) to the present sensor uncertainty shown in Fig. 2. Here we distinguish between Gaussian faults which are modeled as Gaussian distributions with mean μ_{fault} and varying standard-deviation σ_{fault} and finally taking the worst case condition of σ_{fault}. Additionally, we assume a uniform distribution of deviations caused by faults which lead to an arbitrarily distributed across the measurement range (Fig.3).

$$\sigma^2 = {\sigma_{unc}}^2 + {\sigma_{fault}}^2 \quad (6)$$

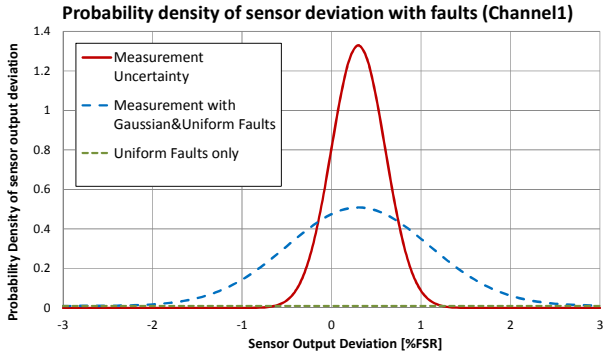

Fig. 3. Sensor measurement uncertainty with Gaussian faults modeled by superimposed varying Gaussian standard deviation including superimposed uniform faults modeled by equal distribution of faults.

The separation of Gaussian and uniform faults can be done using the relative contributions. As an example shown in (7) Gaussian (F_G) and Uniform (F_U) relative fault contributions were used for this separation.

$$p(x,\mu,\sigma) = \frac{F_G}{F_G+F_U} \cdot \frac{1}{\sqrt{2\cdot\pi\cdot\sigma^2}} \cdot e^{-\frac{(x-\mu)^2}{2\cdot\sigma^2}} + \frac{F_U}{F_G+F_U} \cdot \frac{1}{FSR} \quad (7)$$

III. DEPENDABILITY CALCULATION

A. *Joint Probability Densitiy*

Statistically the deviations of both sensor channels form a joined probability density function. Now we need to find all points in this graph resulting in a sensor system output value of 2*dsaf according to (2) representing the safety limit, which are drawn as border-lines from left top to right bottom. All deviations outside this region lead to a violation of the safety limit. On the other hand we use the difference of both channels as safety mechanism and here we show all points representing the safety mechanism limit according (4) which are shown as border-lines from right top to left bottom. All points outside this region are detected as "fault", see Fig 4.

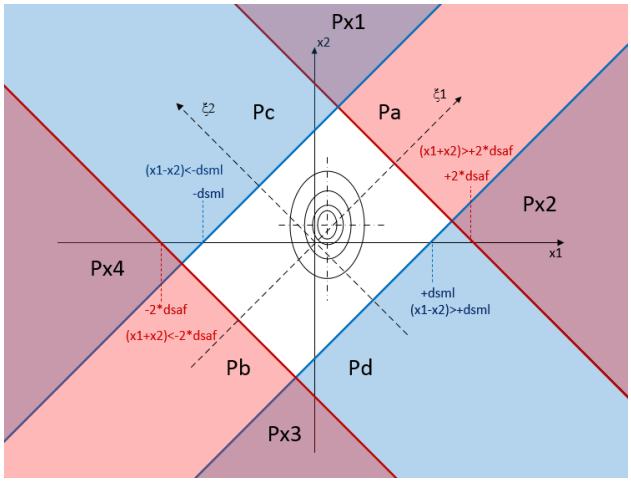

Fig. 4. Joint probability density function of the two channel output deviations. The red lines from left top to right bottom show the safety limit and the blue lines from right top to left bottom the safety mechanism limit. Situations in area maked as Pa and Pb are non detected dangerous faults, situations in the area marked as Pc and Pd are false alarm regions where the safety limit is not violated and Px1..Px4 situations are deteced faults.

The probabilities of Pa, Pb, Pc and Pd are extracted by a coordinate transformation by +45° according to [8]. Applied to Pa this leads to the expression shown in (9), Pb, Pc and Pd are calculated in a similar manner with corresponding changed integration limits.

$$Pa = 2\int_{\frac{-dsml}{2}}^{\frac{dsml}{2}}\int_{dsaf}^{\infty} p1(\xi_1 - \xi_2, \mu_1, \sigma_1)p2(\xi_1 + \xi_2, \mu_2, \sigma_2)d\xi_1 d\xi_2 \quad (9)$$

B. *Diagnostic Coverage Calculation*

The calculation of the diagnostic coverage can be performed by using probability regions where the deviation is larger than the safety limit and is not detected by the safety

mechanism marked as Pa and Pb as shown as red area in Fig. 4, then subtract these probabilities from 100% to get the diagnostic coverage as shown in (10). The distribution of diagnostic coverage versus varying deviation standard-deviations caused by faults can be seen in Fig. 5.

$$DC = 100 \cdot (1 - Pa - Pb)\ [\%] \qquad (10)$$

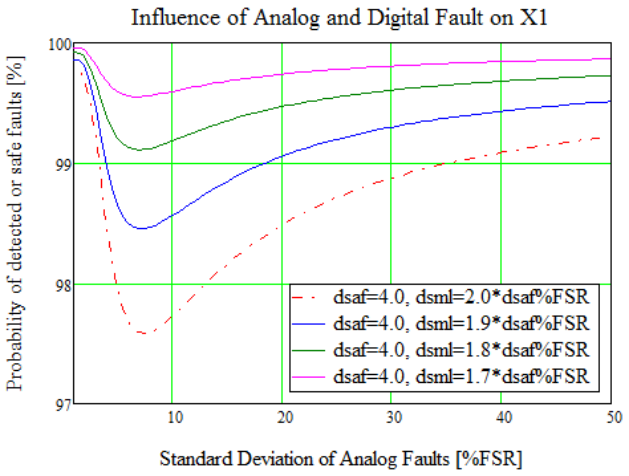

Fig. 5. Diagnostic coverage distribution versus Gaussian fault standard deviation with 25% uniform faults and 75% Gaussian faults and sensor uncertainties taken from Fig. 2.

C. *False Alarm Calculation*

The false alarm calculation of the datapath is dependent on the definition of a false alarm. In case of the definition where a false alarm is also present if any fault is present but the safety requirement is not violated the calculation is done in following way: The false alarm probability P_{FA} can be calculated using probability regions where the safety limit is not violated but an alarm is indicated represented by Pc and Pd shown in the blue area of Fig. 4. This probability in comparison to the diagnostic coverage increases with reduced diagnostic limit because the limits are met even earlier with lower sensor deviations. This probability of a false alarm only occurs in case of a present fault. In this case the probability of a false alarm must be multiplied with the fault rate λ of the device to get the false alarm rate "FAR" as shown in (11). But these detected faults do not lead to a violation of the safety requirement.

$$FAR_{fault} = \lambda \cdot (Pc + Pd)\ [1/h] \qquad (11)$$

On the other hand using a definition when all faults should be detected, also those who are not violating the safety requirement, these are detected faults and do not increase any already present false alarm rate.

D. *Optimization of Diangostic Coverage*

The resulting worst case diagnostic coverage for several relationships between the diagnostic mechanism limit "dsml" and safety requirements limit "dsaf" can be seen in Fig. 6. In addition we can also optimize the relationship of "dsml" and "dsaf" to achieve a certain required diagnostic coverage. For optimizations of redundant sensor systems this relationships can be used to calculate the required sensor performance to achieve certain diagnostic coverages.

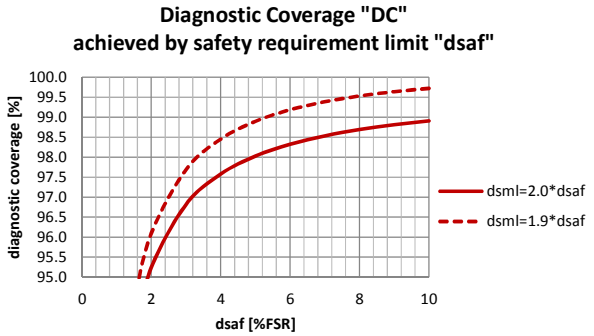

Fig. 6. Worst case diagnostic coverages at 25% uniform faults and 75% Gaussian faults and sensor uncertainties taken from Fig. 2 versus safety requirement. Here two different "dsml" limits are shown for comaprison.

IV. CONCLUSION

In this paper we presented a simple and efficient way for estimating diagnostic coverage and false alarm values of redundant sensor systems. This methodology can further be used in statistical sensor system optimizations, where additionally to performance optimization also dependability requirements must be fulfilled.

ACKNOWLEDGMENT

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia.

REFERENCES

[1] U.Ausserlechner, "The optimum layout for gigant magneto resistive angle sensors", IEEE Sensors Journal, vol. 10, no. 10, pp. 361-365, oct. 2010.

[2] M.Motz and U.Ausserlechner, "Electrical Compensation of Mechanical Stress Drift in Precision Analog Circuits", Springer International Publishing, pp. 297-326, 2017.

[3] H.Zangl, G.Steiner, „Optimal Design of Multiparameter Multisensor Systems", IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 7, july 2008.

[4] ISO 26262, „Functional Safety on Road Vehicles", International Standardisation Organisation, 2011.

[5] O.Karaca, J.Kirscher, A.Laroche, A.Tribusch, L.Maurer and Georg Pelz, "Fault Grouping for Fault injection Based Simulation of AMS Circuits in the Context of Functional Safety", IEEE 2016.

[6] 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.

[7] Granig, W., Rasbornig, F., Hammerschmidt, D., Motz, M.et.al., "Redundant and Diverse Magnetic Field Digital Linear Hall Sensor Concept for ASIL D Applications", SAE Technical Paper 2017-01-0053, 2017, doi:10.4271/2017-01-0053.

[8] Hwei P.Hsu ,"Theory and Probems of Probability, Random Variables, and Random Process", McGraw-Hill, 1997.