

Advantages of the Alternative Method for Random Hardware Failures Quantitative Evaluation - a Practical Survey for EPS

Kamil Svancara and John Priddy
TRW Automotive

Tomislav Lovric
TRW Automotive GmbH

Joseph D. Miller
TRW Automotive US LLC

Maciej Kudanowski and William J. Forbes
TRW Automotive

ABSTRACT

Two methods are allowed in ISO 26262-5 for hardware analysis of random hardware failures. The 1st method is called “Evaluation of Probabilistic Metric for random Hardware Failures”. The 2nd method is called “Evaluation of each cause of safety goal violation”. Advantages of the 2nd method during development of ASIL D Generation 3 Electric Power Steering are presented in this paper. A reliability analysis is one of the important prerequisite for the hardware analysis and this paper shows the best practice for hardware part failure rate estimation using industry standards such as IEC TR 62380. The equally important focus is on a diagnostic coverage of each safety mechanism with respect to residual faults and with respect to relevant dual/latent point faults because any safety design can either benefit from low failure rates or from high diagnostic coverage of safety mechanism to mitigate faults. FMEA is highly recommended by ISO 26262-5 as a part of hardware analysis. There is an analogy between the 2nd method for hardware analysis and FMEA. The 2nd method may be considered an extension of standard FMEA techniques that also analyze the system effect of faults including SW interactions.

CITATION: Svancara, K., Priddy, J., Lovric, T., Miller, J. et al., "Advantages of the Alternative Method for Random Hardware Failures Quantitative Evaluation - a Practical Survey for EPS," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 6(2):2013, doi:10.4271/2013-01-0190.

INTRODUCTION

Development of Electric Power Steering (EPS) is an iterative process. EPS is designed to meet its requirements followed by analysis. The analysis of design may result in design modifications. Engineers tend to do both steps, i.e. design and analysis, together especially in the early stage of development. The design and analysis are more clearly separated after the basic design is fixed and when details start to play a more important role.

A safety case is part of EPS development. The impact of changes required as a result of new safety requirements being identified late in the development cycle can be minimized if the safety design is analyzed early.

ISO 26262-5 [1] allows two methods for analysis of safety goal violations due to random hardware failures. The 1st method is called “Evaluation of Probabilistic Metric for random Hardware Failures” [1, 9.4.2] and the 2nd method is called “Evaluation of each cause of safety goal violation” [1, 9.4.3].

There are several work products that are required either as prerequisites for hardware analysis or in parallel with the analysis. The envisaged list includes:

- Hardware design specifications with drawings
- Electric Component List (ECL) as a part of Bill of Material (BOM)

- Reliability analysis for failure rate estimation
- Failsafe Manual (i.e. part of Safety Requirements) with list of safety mechanisms and estimated diagnostic coverage of safety mechanisms
- Safety analyses, especially FMEA of Electrical/Electronic HW parts

RELIABILITY ANALYSIS

Failures in time (FIT, failures per 10^9 hours) estimation is essential for quantitative safety analysis. Therefore it is important to correctly estimate failure rates of HW parts.

The basic split of failures can be made by nature of the failures [2]:

- Intrinsic failures (due to random error)
- Non-intrinsic failures (due to systematic errors of design)

Random Failures (Limitations of Analysis)

The aim of this paper is to focus on intrinsic random hardware failures only. These are failures for which FIT rate has to be estimated. This does not mean that non-intrinsic failures are not important but they are simply beyond the scope of this quantitative analysis - Systematic non-intrinsic failures are explicitly excluded from the analysis due to [1, Clause 9].

Paper assumes independent failures. It is assumed that analysis of dependant failures will reveal any common cause/common mode or cascaded failures which could invalidate the results for this quantitative analysis.

For example tin whisker on tin plated connector or metal debris causing short circuit in the connector are regarded as non-intrinsic failures for which reliability calculation is not usually provided. These failures (if present) will be reported during [2]:

- Either early failure period (i.e. first months of product operation)
- Or wear-out period (i.e. at the end of product operation)

The above mentioned systematic non-intrinsic failures due to design errors or manufacturing process errors may lead to design corrections or manufacturing process corrections. Care should be taken that the wear-out period for selected HW parts is far removed from the periods of use [2, 4.2.1.3] such that failures due to wear out are insignificant. The manufacturing process/burn-in process similarly should ensure that failures during early failure period in the field are also insignificant.

It could be argued that the focus on evaluation of random hardware failures metrics with the assumptions of constant failure rate over time risks understating the failure rate particularly in the product launch phase. The mitigation of this risk is typically handled by 'Safe Launch' strategies - for example, extended burn-in during the production ramp up phase - until sufficient confidence in product and process have been achieved.

In addition, due to the nature of failure rate estimation methods, some non-intrinsic failures are implicitly included in random failure rates. This should be seen as an additional benefit which helps ensuring that failures which are hard to foresee are not overlooked [2].

Mission Profile (Temperature Profile)

Failure rate depends on several factors - for example:

- Mission Profile (i.e. Temperature profile and field use conditions [2, 5.7])
- Stress environment (i.e. electrical voltage/current overloads, humidity, mechanical shocks and vibrations [2, 5.2 & 5.3])

It is generally accepted that a hotter environment leads to a higher FIT rates, however this dependence varies between component families and is at least partially accounted for by [2]. Designers must choose suitable HW parts depending on the environmental requirements, but there are limits. For example, most passive components, such as ceramic chip capacitors, are limited to 125 °C [3].

The mission profile defines local ambient temperature in time and temperature cycle parameters due to power dissipation. This temperature profile should accurately reflect the local environment of the component rather than that of the system as a whole. IEC TR 62380 [2] uses a predefined mission profiles, e.g. "Motor control" or "Passenger compartment", which can be further adapted for specific environments. Generation 3 of EPS [4] specifies two concepts:

- Belt Drive (BD) EPS with mission profile defined for environment close to the engine control
- Column Drive (CD) EPS with mission profile defined for environment within the passenger compartment

An example for a BD EPS mission profile is shown in [figure Appendix-1](#).

SN 29500 [18] is another industry standard for HW part FIT estimations which includes temperature dependence.

For example capacitor C301 which is ceramic class 2 (no TC coefficient) is estimated with 2.79 FIT for BD EPS mission profile [2]. C301 will be used in the next sections for further evaluation.

For a comparison, the same capacitor is estimated with 1.78 FIT (approx -36% difference) for CD EPS mission profile where the main difference is in a drop of 125 °C max envisaged temperature for BD EPS to 85 °C for CD EPS.

Target- and Confidence-Levels

[1, Table 6] is one of potential sources for defining a quantitative target level for random HW failure evaluation. An example for ASIL D is shown in [Table 1](#).

Table 1. Target values.

ASIL volume	Average probability of failure per hour over the operation lifetime
D	$< 10^{-8} \text{ h}^{-1}$

This target will be compared against estimated FIT rates of HW parts.

FIT rates of HW parts can be scaled depending on the desired confidence level as it is shown in [1, Table F.1 & Example 1 of Annex F]. This is necessary if FIT rates are estimated from different sources with different confidence levels.

Estimated FIT rates of HW part can be also scaled using Arrhenius equation [6] as it shown below on example for new technology. Suppliers often qualify new technology using JEDEC standard [5], using 60-90 % confidence level. Stress-Test-Driven Qualification using several lots of tens of units at the highest allowed temperature. Table 2 shows an example of a reliability report for new semiconductor technology. Accelerated test for 1000 h (approx 1.5 months) with high stress. The idea is to calculate FIT rate at lower temperature than tested using Arrhenius equation [6].

Table 2. Example of Reliability report for new technology.

Test Variable	Value/Units
No of failures f	0 [-]
No of devices D	935 [-]
No of hours H	1000 h
Accelerated temperaure T_{ACC}	175 °C = 448.15 K
Operating temperature T_{OP}	90 °C = 363.15 K
Activation energy E_A	0.7 eV
Boltzman's constant k	$8.617 \times 10^{-5} \text{ eV/K}$

Cumulative Device Hours CDH is equal to:

$$CDH = D \times H = 935 \times 1000 = 935000 \text{ h} \quad (1)$$

Chi-squared χ^2 value which is used to model failure rate depends on upper confidence interval $(1-\alpha)$ and degrees of freedom ν derived from the number of failures f ; $\nu = 2 \times (f+1)$ [7]. For $f=0$ failures, $\nu = 2 \times (0+1)=2$. Chi-squared χ^2 values for confidence level 60% and 99 % are:

- $\chi^2(1-0.6=0.4, 2)=1.83$
- $\chi^2(1-0.99=0.01, 2)=9.21$

Failure rate $\lambda(T_{OP})$ at an operating temperature can be estimated by the Arrhenius equation used to calculate the thermal Acceleration Factor (AF) for semiconductor device time-to-failure distributions [6]:

$$AF = e^{[(E_A/k)(1/T_{OP} - 1/T_{ACC})]} [-] \quad (2)$$

$$\lambda(T_{ACC}) = \chi^2(1 - \alpha, \nu) / 2 \times CDH \text{ [h}^{-1}\text{]} \quad (3)$$

$$\lambda(T_{OP}) = AF \times \lambda(T_{ACC}) / 10^{-9} \text{ [FIT]} \quad (4)$$

Table 3. Example of confidence level impact.

	60 % confidence level	99 % confidence level
AF (175 °C to 90 °C)	69.82	69.82
λ (175 °C)	979 FIT	4925 FIT
λ (90 °C)	14 FIT	71 FIT

Table 3 shows that estimate of FIT rate of upper confidence level can vary significantly depending on selected confidence level and selected operating temperature. This approach can be re-used for different operating temperatures. Overall FIT rate can be derived by considering the time spent at given operating temperatures as defined in mission profile (see Figure Appendix-1).

Authors believe that 70 % confidence level could be sufficient for HW part FIT estimation if evidence is provided to support it (i.e. warranty data).

Transient (Soft) Errors

The main difference between:

- permanent (hard) errors
- and transient (soft) errors

can be explained in ability/inability to heal. Transient errors are those which can be healed (i.e. by reset) where permanent errors persist.

The failure modes that may occur depend on the used technology of the part. Not all parts are affected by soft errors. Simple parts, e.g. wire-wound resistors, typically are not affected by random soft errors - either the wire is broken or not (however there may be relevant intermitting failure modes, e.g. at contacts).

Soft errors apply primarily to memory devices but may occur in logic devices, too, especially integrated circuits that contain internal solid state volatile memory arrays or bi-stable logic elements like flip-flops.

Soft errors are non-destructive faults induced by alpha particle emitted from radioactive impurities for example in packaging and by cosmic-ray-neutron events [8].

Following [1, Table D.1 in Annex D] the soft error model must be analyzed for volatile memory, registers and internal RAM, and for sequential parts of address calculation to claim a medium (90 %) coverage, and in addition to claim high coverage (99 %), the soft error model must be analyzed for sequential parts of the ALU-data path, for sequential parts of on-chip communication including bus-arbitration, for

configuration registers, and for other sub-elements of semiconductor elements that may be affected by soft-errors.

Soft-error-rates (and failure mode distribution like single- or multiple-bit flips) are highly dependent on involved technology and implementation details. Anything from 0.1 FIT to several orders of magnitude higher rates than for hard errors may be credible. As structures of integrated circuits are shrinking, and internal voltage levels decrease, soft error rates have tendency to increase. Unfortunately recognized industry standards for failure rate estimation such as IEC TR 62380 [2] do not provide models to estimate the soft-error-rates. JEDEC defines two methods to determine soft errors FIT, real-time (un-accelerated) and accelerated testing procedures [8]. Soft-errors and failure models of integrated circuits are discussed in more details in [13] & [14]. For all practical purposes accurate soft-error-rate data needs to be determined and should be provided and justified by the HW part supplier.

FAILURE MODE DISTRIBUTION

FIT rate of HW part can be further distributed per Failure Modes (FM) of HW part (FMD Failure Mode Distribution). IEC TR 62380 [2] defines FMD for most components. For example C301 ceramic capacitor class 2 has the following distribution:

- FM1 = 90 % Short-circuits (SC)
- FM2 = 10 % Open-circuits (OC)

For others HW parts such as connectors, failure mode distribution can be derived from MIL-DBK-338B [9]. For failure modes identification also [1] table D.1 should be considered, if applicable.

FMD may depend on the special conditions of use in the field. Therefore, field experience and expert judgment may be needed to select a suitable FMD in particular cases. Especially, when recognized industry sources list differing FMDs. Typically MIL-DBK-338B is more accurate for FMD while IEC TR 62380 may be more accurate on FIT rate. Expert judgment is also needed if the used standards do not list the particular sub-type of the analyzed part, e.g. for specific parts like ICs, or specific connectors designed for failure exclusions.

If there is a need to evaluate a particular HW part in more detail, such as resistive short of ceramic capacitor in a specific ohmic region, the supplier for specific HW part can run accelerated test to define FMD of resistive short.

The analysis can be enhanced by considering all potential failure modes based on parametric requirements of HW parts used, i.e. by considering which parameters of a component have been identified as being relevant to the operation of the circuit and ensuring all are included together with the their potential failure modes.

This ensures that the requirements flow-down to the detailed level of the design is properly reconciled in the metric calculations. Worst Case Circuit Analysis (WCCA) can potentially act as a source for this parameter list, i.e. what

has been analyzed in the design under no fault conditions needs to be considered under fault conditions.

This approach is consistent with [1, Annex E, Note 2] where a ‘use case’ based approach is proposed rather than the component fault model approach currently being employed in the majority of cases known to the authors. However applying it rigorously is likely to lead to significant increase in the extent of analysis needed and require additional support from component suppliers to ensure component failure modes and distributions are available in the desired level of detail.

EVALUATION OF EACH CAUSE OF SAFETY GOAL VIOLATION (THE 2ND METHOD)

The 2nd method for hardware analysis applies specific classification criteria to establish Failure Rate Classes (FRC).

Classification Criteria

FRC are derived from a target for ASIL D (see table 1) assuming 100 relevant cut-sets per safety goal. This conservative assumption can be verified using Fault Tree Analysis (FTA) as per [1, 9.4.3.4] “If a rationale is provided, the failure rate class ranking may be divided by a number lower than 100.” Therefore FTA can be used to define a number of 1st order cut-sets (assuming no safety mechanism is present) per specific safety goal. The threshold for FRC1 can be derived as [1, 9.4.3.3]:

$$FRC1 = 10^{-8} / 100 = 10^{-10} h^{-1} = 0.1 \text{ FIT} \quad (5)$$

Next threshold for FRC2 can be derived as [1, 9.4.3.3]:

$$FRC2 = 10 \times FRC1 = 10 \times 0.1 \text{ FIT} = 1 \text{ FIT} \quad (6)$$

And so on. Table 4 below shows definition of first 5 FRC for any ASIL.

Table 4. FRC definition based on HW Part FIT.

FRC	HW part λ
FRC1	$\lambda < 0.1 \text{ FIT}$
FRC2	$0.1 \text{ FIT} < \lambda \leq 1 \text{ FIT}$
FRC3	$1 \text{ FIT} < \lambda \leq 10 \text{ FIT}$
FRC4	$10 \text{ FIT} < \lambda \leq 100 \text{ FIT}$
FRC5	$100 \text{ FIT} < \lambda \leq 1000 \text{ FIT}$

HW Part Classification

Once the FRC's are defined (see above), each safety related HW part or HW element can be classified. The classification is done for the whole HW part (e.g. resistors, capacitors) or for the HW element (e.g. ALU of IC, SRAM of IC) [10, Annex F]. This is analogous to rating occurrence in