

Automotive Hardware Development According to ISO 26262

Seo-Hyun Jeon*, Jin-Hee Cho*, Yangjae Jung*, Sachoun Park*, Tae-Man Han*

*Automotive Convergence Platform Research Team, ETRI, 161 Gajeong-Dong, Yuseong-Gu, Daejeon, 305-700, KOREA

happyseohyun@etri.re.kr, chojh@etri.re.kr, cornor@etri.re.kr, sachem@etri.re.kr, tmhan@etri.re.kr,

Abstract— This paper briefly explains ISO 26262, the new automotive standard for functional safety. The standard is for electrical/electronic systems mounted on series of passenger cars. In the standard, Automotive Safety Integrity Level (ASIL) is classified into four levels according to the required safety level. Each of the ASIL has its own process and steps for item development. This paper focuses on the item development at hardware level, especially for ASIL C and D. The hardware development procedure includes the calculation of single point metric and latent fault metric. Furthermore, we present overall calculation steps of controlling random hardware failure.

Keywords— ISO 26262, system, hardware, development, single point fault metric, latent fault metric, diagnostic coverage

I. INTRODUCTION

There is an upcoming standard for automotive industry; ISO 26262 Road vehicles – Functional safety, and it is planning to be published in 2011. The automotive industry should be well prepared to adapt this new standard into their product development process since automotive manufacturers will require their suppliers to provide only products whose development processes complies this standard. It is because the company's competitiveness will be measured by their capability of conducting the standardized development process. The scope of ISO 26262 includes all safety related electrical/electronic (E/E) systems for automotive application.

ISO 26262 is derived from IEC 61508, but adapted to automotive industry. The big difference between two standards is that ISO 26262 considers controllability while IEC 61508 does not. Controllability is ability to avoid hazardous event, the action taken by a driver. Considering this, ISO 26262 classifies Automotive Safety Integrity Level (ASIL) into four different levels, depending on its severity, probability of exposure, and controllability. After determining ASIL, the product is developed in the process according to the method and measure of the corresponding ASIL. As a result, the main purpose of implementing this standard is keeping all the records of safety-related activities from the development process to ensure functional safety.

ISO 26262 is composed of 10 parts: 1.Vocabulary, 2.Management of functional safety, 3.Concept phase, 4.Product development: system level, 5.Product development: hardware level, 6.Product development: software level, 7.Production and operation, 8.Supporting processes, 9.ASIL-

oriented and safety-oriented analyses, and 10.Guideline. The development process of item level starts from part 3 to 7, and all the other parts are supporting process. The development process generally follows V-style process model and can be depicted as Figure 1. [1]

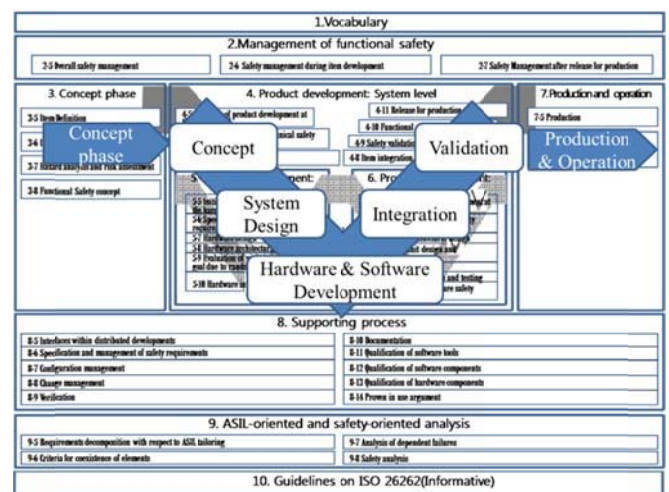


Figure 1. Overview of ISO 26262

As in Figure 1, functional safety concept of the item is derived in the concept phase, and product development at system level will be started. In the product development phase, the system design is specified and each development processes at hardware and software levels are initiated individually.

Although the ISO 26262 standard lists all the requirements to be complied, it is difficult to catch the steps of each activities' what to do and where to start. For this reason, this paper explains how to develop a product to achieve the functional safety according to the standard, especially for the product development at hardware level.

This paper introduces the steps at hardware development by deriving metrics of a hardware element with respect to its failure modes. This analysis is inevitable step when claiming compliance of ASIL C and D. The result of these steps will further perform as an evidence of compliance.

The scope of this analysis is limited to random hardware failure and the parts considered in the analysis are the electrical and electronic parts. For electromechanical parts,

only the electrical failure modes and failure rate are considered.

The derivation steps of hardware architectural metrics will be mainly discussed in Section II. Section II-A explains general process of hardware development. Section II-B describes classification of the failure modes of hardware elements. Section II-C derives hardware architectural metrics according to the classification and gives steps how to calculate. The conclusion is given in III, and a brief example of calculating the metrics and deriving ASIL is given in IV.

II. HARDWARE DEVELOPMENT ACCORDING TO ISO 26262

A. Hardware development process

The hardware development process according to ISO 26262 starts from planning the hardware development. The plan includes specifying the methods and measures to be used during hardware design. Next, hardware safety requirement is specified. This will be derived from several sources such as technical safety concept, software safety requirements and system design specification, from previous activities. (Not mentioned in this paper) Hardware safety requirement specification should be consistent to these documents. And, hardware is designed according to the hardware safety requirements specification. In the hardware design process, hardware architectural metric with respect to random hardware failures needs to be evaluated and verified for ASIL C and D. The steps deriving hardware architectural metrics are explained in the section II-C. Finally, the hardware elements are integrated and tested. Overall steps of hardware development are depicted in Figure 2. [2]

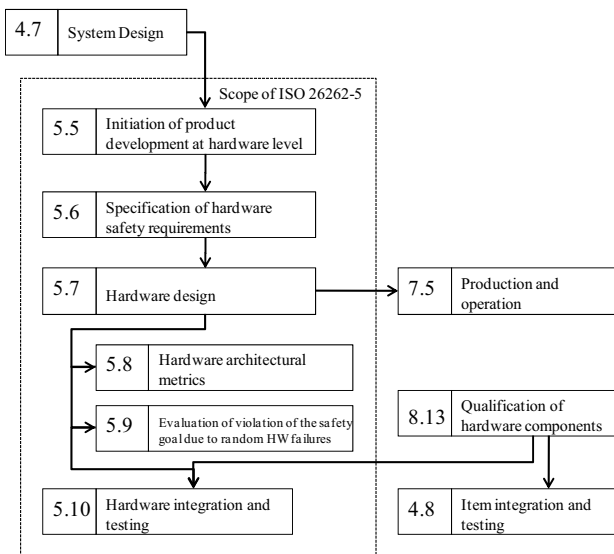


Figure 2. Hardware development procedure

Each of the number appeared in the left box and the name in the right box in the figure 2 shows the corresponding number and the name of clauses in the ISO 26262.

B. Failure mode classification of a hardware element

Random hardware failure normally occurs arbitrarily in a hardware element, however, its failure rate can be predicted with reasonable accuracy. The random hardware failure data can be obtained from several sources. (see list of II-C, 1))

To calculate the hardware architectural metrics, the failure mode needs to be defined. Each faults occurring in a safety-related hardware element can be classified as in figure 3 and are defined in the standard as follows: ([2], [3])

- Safe fault: fault whose occurrence will not significantly increase the probability of violation of a safety goal
- Multiple point fault: one fault of several independent faults that in combination, leads to a multiple point failure (either perceived, detected or latent)
 - Perceived: This fault is deduced by the driver without detection by a safety mechanism within a prescribed time.
 - Detected: This fault is detected by a safety mechanism to prevent the fault from being latent within a prescribed time.
 - Latent: This fault is neither detected by a safety mechanism nor perceived by the driver.
- Single point fault: fault in an element which is not covered by a safety mechanism and where the fault leads directly to the violation of a safety goal
- Residual fault: portion of a fault which by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by existing safety mechanisms

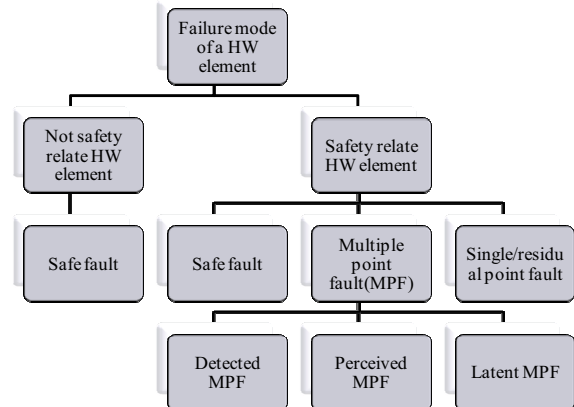


Figure 3. Failure modes classification of a hardware element

C. Hardware architectural metric calculation

To obtain objective evidence for the hardware design that it has achieved the safety goal, the hardware architectural metric needs to be calculated for ASIL C and D according to the following procedure.

- 1) Estimate failure rate of single point fault and latent multiple fault.
- 2) Estimate diagnostic coverage of safety mechanism.
- 3) Calculate "single point faults metric" and "latent faults metrics."
- 4) Compare the metrics with target values.

The detailed explanation for the procedure is given as follows:

1) Estimate failure rate of single point fault and latent multiple fault.

The failure rate of a hardware part can be estimated either from following sources.

- Using a recognised industry sources (i.e., IEC 62380, IEC 61709, MIL HDBK 217 F notice 2, RAC HDBK 217 Plus, NPRD95, EN50129 Annex C, EN 62061 Annex D, RAC FMD97, MIL HDBK 338, etc.);
- Using statistics based on field returns or tests; or
- Using expert judgement based on engineering approach.

2) Estimate diagnostic coverage of safety mechanism.

Diagnostic coverage can be calculated using Annex D of [2] which tables of every element or part used in the hardware architecture are given with their achievable diagnostic coverage.

Table 1 shows an example of the components consisting hardware architecture and their faults or failures that needs to be analysed to derive diagnostic coverage. For relays to achieve 99% of diagnostic coverage, 2 factors need to be detected: i) does not energize or de-energize, ii) individual contacts welded. This table is only part of the quotation of the standard, therefore, for further examples of hardware components, see Annex D of [2],[4],[5].

TABLE 1. EXAMPLE OF REQUIRED FAULTS OR FAILURES TO DERIVE DIAGNOSTIC COVERAGE

Components	Recommendations for diagnostic coverage		
	Low (60 %)	Medium (90 %)	High (99 %)
Relays	Does not energize or de-energize Welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or de-energize Individual contacts welded
Invariable memory range	Stuck-at for data and addresses	d.c. fault model for data and addresses	All faults which affect data in the memory
Variable memory range	Stuck-at for data and addresses	d.c. fault model for data and addresses	d.c. fault model for data and addresses Dynamic cross-over for memory cells No, wrong or multiple addressing

Techniques to derive the diagnostic coverage and the maximum achievable diagnostic coverage for the selected component are given in table 2. This is the example of a variable memory range from table 1. Block replication in table 2, for instance, aims to detect all bit failures of the memory by duplicating the address space in two memories. The mechanism is: the first memory is operated in the normal manner, the second memory stores the same information inversely and it is inverted again when accessed in parallel to

the first, and the outputs difference leads to a failure message. This technique can achieve high diagnostic coverage.

TABLE 2. DIAGNOSTIC TECHNIQUE/MEASURE AND THEIR COVERAGE FOR VARIABLE MEMORY

Diagnostic technique/measure	Maximum diagnostic coverage considered achievable
RAM test "checkerboard" or "march"	Low
One bit redundancy	Low
Detection of RAM data failures with error-detection-correction codes (EDC)	High
Block replication	High

3) Calculate "single point faults metric" and "latent faults metrics."

When all the failure rates estimated, "Single point faults metric" and "latent faults metrics" are calculated as following equations.

Single point faults metric:

$$= 1 - \frac{\sum_{SR}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR} \lambda} = \frac{\sum_{SR}(\lambda_{MPF} + \lambda_S)}{\sum_{SR} \lambda} \quad (1)$$

Latent fault metric:

$$= 1 - \frac{\sum_{SR}(\lambda_{MPFL})}{\sum_{SR}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR}(\lambda_{MPF PD} + \lambda_S)}{\sum_{SR}(\lambda - \lambda_{SPF} - \lambda_{RF})} \quad (2)$$

where,

- Safety related HW elements: $\sum_{SR}$
- Failure rate associated to hardware element single point faults: λ_{SPF}
- Failure rate associated to hardware element residual faults: λ_{RF}
- Failure rate associated to hardware element multiple point faults: λ_{MPF}
- Failure rate associated to hardware element perceived or detected multiple point faults: $\lambda_{MPF PD}$
- Failure rate associated to hardware element latent multiple point faults: λ_{MPFL}
- Failure rate associated to hardware element safe faults: λ_S with $\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S$ and $\lambda_{MPF} = \lambda_{MPF PD} + \lambda_{MPFL}$.

4) Compare the metrics with target values.

Numerical target values for "single point faults metric" and "latent faults metrics" are given in table 3. Appropriate target values wrt. their ASILs are chosen for the hardware architectural metric of the product. Finally, by comparing the result of calculated metrics with the target values, the product can be claimed compliance with the standard.

TABLE 3. TARGET VALUES FOR SINGLE POINT FAULTS METRIC AND LATENT FAULTS METRIC

	ASIL B	ASIL C	ASIL D
Single point faults metric	> 90 %	> 97 %	> 99 %
Latent faults metric	> 60 %	> 80 %	> 90 %

III. CONCLUSION

The hardware development process according to ISO 26262 is explained in this paper. The process consists of planning, hardware safety requirement specification, hardware design, and integration and testing. The calculation of hardware architectural metrics during hardware design process for ASIL C and D is explained in detail by 4 steps. Evaluation of hardware architectural metrics with respect to random hardware failures and final claiming evidence are included in the steps. By obtaining hardware architectural metrics, the architectural detailed design can have ASIL dependent pass/fail criteria and can be objectively assessable.

Developing an item in compliance with ISO 26262 is not a simple task, but automotive companies should implement the standard in advance to their development process because this will show the evidence of organizational capability of performing functional safety in near future.

IV. EXAMPLES

The example of calculation of single point fault metric and latent fault metric are given in table 4 and 5, respectively. [2] Recall the 4 steps.

1) Estimate failure rate of single point fault and latent multiple fault.

The first step is to fill the failure rate (F) of the second column of the table 4 and 5. This failure rate is normally provided with the component (C). And check in the "SR" column, whether the component is safety related or not. This selection is made by the hardware developer.

Also, fill in the failure mode (FM) and failure rate distribution (FD). Failure mode can be derived using FMEA. [6] The summation of failure rate distribution of each component should be 100%.

2) Estimate diagnostic coverage of safety mechanism.

If the failure mode of the component has potential to violate the safety goal in the absence of safety mechanism or due to independent failure of another component, check "V" or "VI" column.

And, describe in the "SM" or "L" column, the safety mechanism that prevents the failure mode from violating the safety goal or being latent. Continuously, fill out the diagnostic coverage of the safety mechanism in "FC" and "FCL" column of table 4 and 5.

Residual or single point fault failure rate (RF/SPF) can be calculated by multiplying $F*FD*(1-FC)$. Latent multiple point fault failure rate (LMPF) can be calculated by multiplying $F*FD*(1-FCL)$.

3) Calculate "single point faults metric" and "latent faults metrics."

- Total failure rate: 118
 - Total safety related failure rate: 108
 - Total not safety relate failure rate: 10
- Total residual or single point fault failure rate : 5.234
- Total latent multiple point faults failure rate: 0.6

Now, applying (1) for single point faults metric, we calculate:

$$= 1 - \frac{\sum_{SR}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR} \lambda} = 1 - \frac{5.234}{108} = 95.2\% \quad (3)$$

Applying (2) for latent fault metric, we calculate:

$$= 1 - \frac{\sum_{SR}(\lambda_{MPFL})}{\sum_{SR}(\lambda - \lambda_{SPF} - \lambda_{RF})} = 1 - \frac{0.6}{(108 - 5.234)} = 99.42\% \quad (4)$$

4) Compare the metrics with target values.

The result of this hardware is complying ASIL B because the single point faults metric satisfies > 90% of ASIL B but not enough for > 97% of ASIL C. Latent faults metric satisfies in all cases but the result of the hardware is conservative and becomes ASIL B.

This example shows that in order to receive higher ASIL the hardware component with lower failure rate or safety mechanism with higher diagnostic coverage is needed. If hardware does not meet the target value, rationale for how will the safety goal be achieved should be stated in the safety case.

TABLE 4. SINGLE POINT FAULTS METRIC EXAMPLE

C	F	SR	FM	FD	V	SM	FC	RF/SPF
R1	2	SR	Open	90%	X	none	90%	0.18
			Closed	10%				
C1	2	SR	Open	20%		SM1		
			Closed	80%	X		99%	0.016
I1	4	SR	Open	70%	X	SM1	99%	0.028
			Closed	20%	X		99%	0.008
			Drift 0.5	5%	X		99%	0.002
			Drift 2	5%				
L1	10	NSR	Open	90%				
			Closed	10%				
μC	100	SR	All	50%	X	SM3	90%	5
			All	50%				
Total	118							5.234

TABLE 5. LATENT FAULTS METRIC EXAMPLE

C	F	SR	FM	FD	VI	L	FCL	LMPF
R1	2	SR	Open	90%	X	SM1	100%	0
			Closed	10%	X		0%	0.2
C1	2	SR	Open	20%	X	SM1	0%	0.4
			Closed	80%	X		100%	0
I1	4	SR	Open	70%	X	SM1	100%	0
			Closed	20%	X		100%	0
			Drift 0.5	5%	X		100%	0
			Drift 2	5%				
L1	10	NSR	Open	90%				
			Closed	10%				
μC	100	SR	All	50%	X	SM3	100%	0
			All	50%				
Total	118							0.6

Table indices:

- **C** (Component name): list of components.
- **F** (Failure rate): input failure rate of the component.
- **SR** (Safety Related): state whether the component is safety-related (SR) or not (SNR).
- **FM** (Failure mode): Describe failure mode of each component.
- **FD** (Failure rate distribution): for each of the failure mode, derive failure rate distribution. The sum of each distribution will be 100%.
- **V** (Potential to violate the safety goal in absence of safety mechanism): check whether the absence of safety mechanism can cause the violation of the safety goal.
- **SM** (Does the safety mechanism prevent the failure mode from violating the safety goal?): if checked (X), write the safety mechanism.
- **FC** (Failure mode coverage): diagnostic coverage of the selected safety mechanism
- **RF/SPF** (Residual or single point fault failure rate): calculate the residual or single point fault failure rate by $RF/SPF = F \times FD(1 - FC)$.
- **VI** (Independent failure): check if the failure mode may lead to violation of safety goal in combination with an independent failure of another component.
- **L** (Does the safety mechanism prevent the failure mode from being latent?): if **VI** is checked, write the safety

mechanism allowing preventing the failure mode from being latent.

- **FCL** (Failure mode coverage wrt. latent failures): diagnostic coverage of the selected safety mechanism
- **LMPF** (Latent multiple point fault failure rate): calculate the latent multiple point fault failure rate by $LMPF = F \times FD(1 - FCL)$.

ACKNOWLEDGMENT

This work was supported by the fund of Development of Integrated Control SW Platform for Automotive Electronics project (MKE).

REFERENCES

- [1] R. Hamann, J. Sauler, S. Kriso, W. Grote and J. Moessinger, "Application of ISO 26262 in Distributed Development ISO 26262 in Reality," *SAE World Congress & Exhibition*, Apr. 2009.
- [2] *ISO 26262 Road vehicles – Functional safety – Part 5: Product development: hardware level*
- [3] *ISO 26262 Road vehicles – Functional safety – Part 10: Guideline*
- [4] *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 1: General requirements*
- [5] *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 7: Overview of techniques and measures*
- [6] *Potential Failure Mode & Effects Analysis*, Chrysler LLC, Ford Motor Company, General Motors Corporation, Jun. 2008