Qualifying Dependent Failure Analysis within ISO26262: Applicability to Semiconductors

Alison Young, Alastair Walker

Functional Safety Consultants

LORIT CONSULTANCY, Scotland

alison.young@lorit-consultancy.com

alastair.walker@lorit-consultancy.com

Abstract

In early 2018, the second edition of ISO 26262:2018[1] functional safety standard for road vehicles, was released.

One of the main challenges in safety analysis is the decision on suitability of dependent failures. Many discussions ensue on the suitability and the potential impact of any common cause or dependent failures. ISO 26262 parts 9 and 11 give guidance of the categories of dependent failures initiators, but how to gauge acceptability is not so easily quantified.

There is a lot of excellent literature on calculating failure rates for common causes, but this information may not easily support design teams in assessing the dependency of the 7 groups of dependent failure initiators listed in ISO 26262-9:2018.

IEC 61508 uses a grading system based on a series of questions, however it relates any score gained to the beta factors used in calculating failure rates. Ultimately it is desirable for dependent failures analysis to produce a quantitative result, but not one that feeds into failure rates, as many decisions based on failure rates involve software or system level considerations and are systematic rather than random.

One other significant factor in the dependent failures analysis is that many products being assessed against ISO 26262 were not originally designed to meet the standard, and are being adapted to comply. In this case an assessment of additional safety mechanisms and the quality of them is key.

This paper proposes a quantitative approach to grade dependent failures analyses such that an acceptability criterion can be defined for different ASILs.

Keywords

Functional safety, dependent failures analysis (DFA), common cause failures

1 Introduction

Many design teams in the automotive industry working to ISO 26262 implement the requirements of parts 4, 5 and 6 of the standard to the letter of the law. The activities defined in part 9 such as DFA however are both trickier to define down to the limited amount of available information. The DFA like the dependent failures initiator (DFI) identification in ISO 26262 is good, but how to actually define what is or is not acceptable is a trickier question.

In ISO 26262 there are two defined goals for the DFA activities

1. Identify single events, single causes & failure modes
2. Identify safety measures to mitigate dependent failures

For point a. above identifying the events is typically a straight forward activity but deciding that the impact is or is not acceptable is more difficult.
By defining a weighting system based on the type of dependence between the components permits a grading system of acceptability to be defined and hence whether the dependency is permissible in the given project.
Equally for point b. a weighting system can be used for any safety measure to define the necessary effectiveness and quality of the mechanism.
Techniques can be equally applicable to discrete or semiconductor components. Dependent failure analysis on a single silicon die looks for interdependencies between hardware elements on the same die, or between hardware and software elements. Typically, analysis focuses on hardware elements performing a safety function and their safety mechanisms.

2 Dependent failure analysis

2.1 Dependent failure initiators

Dependent failure analysis typically begins with identification of pairs – usually a hardware element and its safety mechanism. The scope of the analysis should be defined at the outset, and may include safety mechanisms implemented in hardware, software, or both.
Following the methodology recommended by Faller[2], each of the pairs in this list are then examined to determine if:

- A potential dependent failure would impact the safety function
- No test exists for the potential dependent failure of the hardware element and safety mechanism
- No safety measures exist to control or mitigate the effects of the dependent failure.

If the answer for these three questions is positive then the pair should be included in dependent failure analysis. The next step is to examine potential root causes of a dependent failure, these are termed Dependent Failure Initiators (DFI) in ISO26262-9:2018.
ISO26262-9: Annex C describes 7 groups of dependent failures initiators (DFI), these are represented in Figure 1 below. This annex also lists typical examples of DFI for each of the 7 categories, and maps the categories to the topics in ISO26262-9:2018 clause 7.4.4 and those described along with related mitigation measures in the Guideline on application of ISO26262 to semiconductors in ISO26262-11:2018 clause 4.7.5.

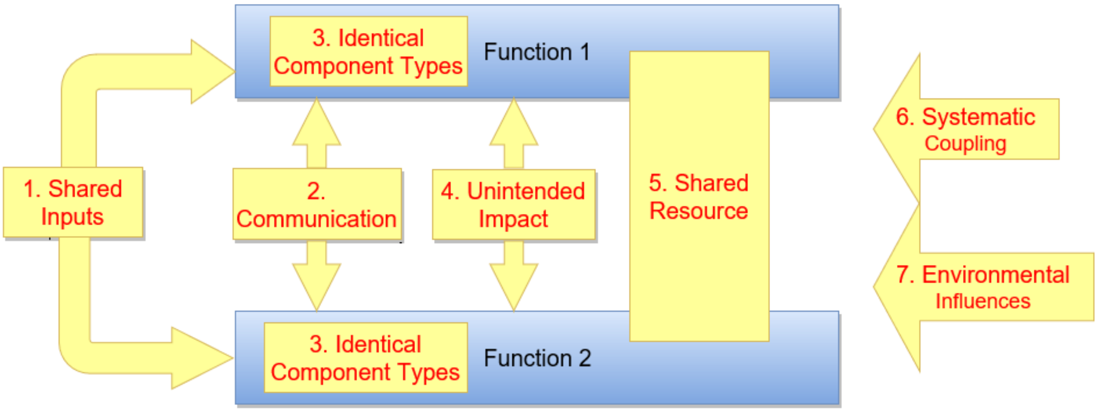

Figure 1 ISO26262-9:2018 Dependent Failure Initiators

When analysing dependent failures within a semiconductor device there will be some dependent failure initiators that can influence a large portion of the device, for example shared resources such as common clocks and shared power supplies. It is often possible to address these dependencies within standard safety analysis. Dependent failure analysis focuses on the dependent failure initiators that cannot be addressed in standard safety analysis.

One particular challenge when performing analysis on semiconductors is choosing pairs of components and initiators that have the greatest potential impact, and having confidence that the breadth of the analysis is sufficient. A weighting system that helps prioritise the key functions and initiators that can influence them is therefore very useful.

2.2 Common Cause Failure Analysis

2.2.1 IEC61508 Strategy for Common Cause Failure Analysis

To enable the calculation of beta factors for common cause analysis in IEC 61508[3] a series of 37 questions are used to estimate the common cause frailties of the system in question. These questions are split into the following categories:

- Separation
- Diversity/Redundancy
- Complexity/Design/Use/experience
- Judgment/analysis of data
- Procedures/usage
- Competence/Training/Safety culture
- Monitoring the surrounding conditions
- Test and environment.

From the results of these 37 questions a weighted value results, this result determines the beta factor used in scaling the failure in time rates.

2.2.2 Controller Strategy

There are many different controller architectures [4] available to support functional safety relevant projects – symmetric, asymmetric and multicore processers. The pros and cons of the different types in relation to common cause failures is also well documented.

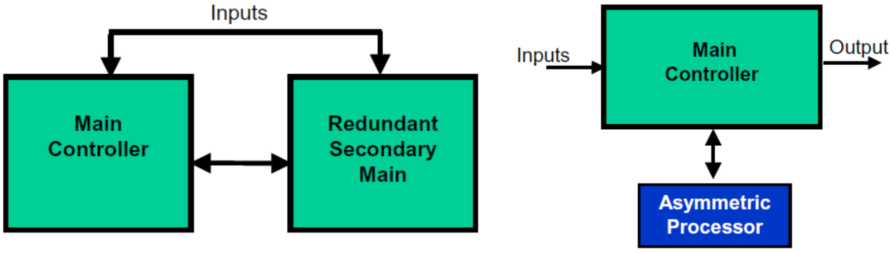

Figure 2 Symmetrical and Asymmetrical Controller Strategies

2.3 Inherent good design against safety mechanism.

In the cases where an existing product is being assessed for suitability to comply with ISO 26262 the architecture may not have been designed in accordance with ISO 26262. In these cases risk control measures may need to be added to the architecture
The risk management standard ISO 14971[5] for medical devices recommends 3 techniques for reducing risk. The first is inherent good design, the second risk control measures and lastly the use of accompanying documents. The last option would not be applicable for the automotive industry, however if we use scaling factors for safety mechanisms these risk control mechanisms can be graded for the reduction they can make to the DFA grading score.

3 *Proposed Strategy*

3.1 Dependent Failure Initiator Grading

A scoring system for acceptance of DFI impacting a new design could be typically defined as below. The categories are those listed in ISO 26262-9:2018 Annex C, but this is not an exhaustive list, there are others that will be applicable for any given project

DFI Group	DFI Type	Detail	Score
Shared Resources	Clock	Same clock source for both channels no checks	10
		Test only for stuck at faults	7
		Test for stuck at, jitter, DC, drift	4
		Full independent clock monitoring	1
	Power Supply	Identical Power Supply	10
		Same technology but different PSU implementation	7
		Different power supply technology	4
		Different power supply technology, with independent monitoring, level, transient and oscillation	1
	Common Software	Identical software component	10
		Different provider same functionality	7

		Different provider similar functionality different hardware	4
		Different SW implementation	1
	Same silicon package	Intended function and safety measure in the same silicon package – no monitoring	10
		Intended function and safety measure in the same silicon package – single level of internal monitoring	7
		Intended function and safety measure in the same silicon package – single level of external monitoring	4
		Intended function and safety measure in the same silicon package – multiple levels of external monitoring	1
Shared Information Inputs	System or HW -external physical signals	Identical data handling of the signals	10
		Diverse handling through the same interface	7
		Diverse handling through different interface	4
		Diverse handling through a different interface with independent monitoring	1
	Software global variables	High number of global variables	10
		Minimal number of global variables	7
		Minimal number of global variables EDC-ECC	4
		Minimal number of global variables EDC-ECC, full static analysis, control and data flow	1

DFI Group	DFI Type	Detail	Score
Environmental Influences	Mechanical shock	Designed to meet the mechanical requirements	10
		Designed and tested to meet all mechanical requirements (one sample)	7
		Designed and tested to meet all mechanical requirements (multiple samples)	4
		Designed and tested to exceed all mechanical requirements (multiple samples)	1
	Water ingress	Not designed to specified IP rating	10
		Designed to meet IP rating requirements	7
		Designed tested to meet IP rating requirements and expected servicing and service life	4
		Designed tested to exceed IP rating requirements and expected servicing and service life	1
	EMC	Designed to meet all emission and immunity levels (not tested in all scenarios)	10
		Designed and tested to meet all emission and immunity levels (one sample)	7
		Designed and tested to meet all emission and immunity levels (multiple samples)	4
		Designed and tested to exceed all emission and immunity levels (multiple samples)	1
	Transient upsets	No testing of transient immunity	10
		Design principles to minimise transient impact	7
		Transient testing of devices e.g. JEDEC 89	4
		Full confirmation of devices to ISO 26262 for transient metrics. ECC for memory	1
Systematic Coupling	Same algorithms	Identical	10
		Same function different processor	7
		Same function different implementation	4

		Different function different implementation	1
	Connection technology	Designed to meet the requirements	10
		Designed and tested to meet all requirements (one sample)	7
		Designed and tested to meet all requirements (multiple samples)	4
		Designed and tested to exceed all requirements (multiple samples)	1
Components of Identical Type	Identical hardware	Identical	10
		Same function different software control	7
		Similar functional different software control	4
		Independent monitoring of results	1
	Identical software libraries	Identical	10
		Same function different hardware platform	7
		Similar functional different hardware platform	4
		Independent monitoring of results	1
Communication	Failure of the physical layer of the communication. SW Exchange of information. Failure of the application or protocol layer of the communications.	Minimal checks on data integrity	10
		Time-outs, message counters, CRC checks	7
		Full end to end ECC	4
		Full end to end ECC with external confirmation	1

DFI Group	DFI Type	Detail	Score
Unintended Impact	HW Crosstalk	No consideration connection impedance	10
		Basic matching of impedances	7
		Full evaluation of impedance and termination	4
		Full evaluation of impedance, termination and physical location	1
	Thermal impact	Basic design analysis	10
		Design analysis and test per requirements	7
		Design and analysis of overstressed levels, thermal analysis (one sample)	4
		Design and analysis of overstressed levels, thermal analysis (multiple samples)	1
	SW Timing and execution e.g. Repetition of information Loss of information Delay of information Insertion of information Masquerade or incorrect addressing of information Incorrect sequence of information Corruption of information Asymmetric information sent to multiple receivers Information from a sender received by only a subset of receivers Blocking access to a communications channel	Minimal checks on data integrity	10
		Time-outs, message counters, CRC checks	7
		Full end to end ECC	4
		Full end to end ECC with external confirmation	1
	SW Memory e.g. Corruption of content Inconsistent data Stack overflow or underflow Read or write access to memory	Basic defensive design	10
		Full static analysis	7
		Full static analysis data & control flow	4

	allocated to another software element	Full static analysis data & control flow. ECC	1
	Training of development and QA personnel	Basic design training	10
		All training by certified bodies	7
		All personnel at least 5 years functional safety experience trained by certified bodies	4
		All personnel at least 5 years functional safety experience trained by certified bodies. All hold functional safety qualifications and similar e.g. AutomotiveSPICE	1
	Training of service personnel	Basic or no training	10
		All personnel trained on the specific project	7
		All personnel trained to certified qualifications and on multiple projects	4
		All personnel trained to certified qualifications and on multiple projects. Servicing inspected by colleagues	1

3.2 Additional Safety Mechanism Grading

If we take the example of a lack of inherent good design or a device developed prior to consideration of ISO 26262 requirements, then the addition of a safety mechanism can also be given a weighting factor to determine quantitively the acceptability of the functionality combined with safety mechanism. The guidelines would follow those of section 3.1 above again comparing the safety mechanism to the intended functionality to determine the independence.

4 Acceptable Outcomes

The acceptable outcomes from the grading system can be applied based on the ASIL of the safety goal.
e.g. for ASIL D the total score must be lower than 40 with the caveat that no single category score can exceed 4. ASIL C should be less than 80 and ASIL B should be lower than 120
Again, the categories in section 3.1 are not exhaustive and if additional categories are added, then the acceptance limits can be scaled up accordingly

5 Conclusions

ISO 26262:2018 provides a good framework for design teams to develop compliant products and those that offer satisfactory levels of functional safety. However, the analysis of dependent failures and that of common cause failures often leaves more questions that it provides answers. The lack of guidance to design teams on what is an acceptable level for DFA is an issue that many organisations find difficult to answer.
Much of the theory on common cause failures focuses on hardware failures, but considering the competence of service personnel is a far harder question to judge.
In this paper we propose a solution based on the ideals of IEC 61508, but not aligning the outcomes with beta factors, in this case giving criterion on how one can accept or reject a given level of dependent failure.

6 Future work

Lorit Consultancy is working to enhance this approach to DFA and further document the strategy in order to support customers in ISO 26262 DFA activities, in both semiconductor devices and discrete component design.

Literature

[1] – ISO DIS 26262:2018 Road vehicles – Functional safety

[2] - Specification of a Software Common Cause Analysis Method", Rainier Faller, pp 162 – 171, SAFECOMP 2007. Springer-Verlag 2007.

[3] – IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

[4] – Controller Integrity in Automotive Failsafe System Architectures – Padma Sundaram and Joseph G. D'Ambrosio, Delphi Corporation. SAE Technical Paper Series 2006-010840.

[5] – ISO 14971 Medical Devices- Application of risk management to Medical Devices

7 Author CVs

Alison Young

Alison has 15 years' automotive industry experience, and for the last 6 years has been responsible for ensuring the functional safety of automotive microcontrollers. She has been involved in the development of microcontrollers for a variety of automotive applications and has extensive experience of delivering the work products required by ISO 26262, including requirements capture, safety plan, safety case, FMEDA and customer facing safety documentation.

Alastair Walker

Alastair Walker is an engineer with over 25 years' development experience in medical, automotive and aviation industries. He is a TÜV Rheinland Functional Safety Engineer he has been working as a functional safety consultant for 5 years and has extensive knowledge of developing embedded systems in safety related industries, such automotive drive train, in-wheel motors and battery management systems.