

Decomposition Scheme in Automotive Hazard Analysis

David D. Ward
MIRA Ltd.

Peter H. Jesty
Peter Jesty Consulting Ltd.

Roger S. Rivett
Jaguar Land Rover

Copyright © 2009 SAE International

ABSTRACT

Safety-related systems in road vehicles are subject to hazard analysis as part of developing their safety requirements. Automotive hazard analysis leads to a requirement for target risk reduction in the system to be developed, usually expressed as a safety integrity level, SIL, or ASIL. During risk analysis, credit can be taken for risk reduction from facilities outside the system of interest, or from architectural decisions to distribute the required risk reduction to sub-elements of the system. Up to now, such concepts have been presented in standards without any justification. The different approaches in the standards are discussed, and a scheme for more rigorously defining the allocation of safety integrity requirements across different elements of a system is proposed.

INTRODUCTION

Safety-related systems in road vehicles, in common with other sectors, are subject to hazard analysis as part of the process of developing their safety requirements. Automotive hazard analysis is based on evaluating the severity of the potential outcome, along with exposure to the hazard¹ and the possibility for the driver to control

the hazardous situation [1, 2]. This leads to a requirement for target risk reduction in the system to be developed, usually expressed as a safety integrity level, SIL ([2, 3, 4]) or ASIL ([5]).

Hazard analysis usually consists of the stages of hazard identification, hazard classification and risk analysis [1]. Some processes combine the last two stages and the resulting hazard classification (such as the ISO CD 26262 ASIL) is also the target measure of risk reduction.

During risk analysis, however, it is permissible to take credit for risk reduction from facilities outside the electronic system of interest. These are usually referred to as “other technology risk reduction measures” and “external risk reduction measures” [3]. Furthermore, architectural decisions can be taken which involve distributing the required risk reduction allocated to an electronic system to sub-elements of that system. An example of this approach is “ASIL decomposition” in ISO CD 26262, which can be used (for example) to develop an ASIL D system from two ASIL B elements, provided adequate independence between the two elements can be shown.

Up to now, such concepts have been presented without any form of justification. In this paper a scheme is proposed that indicates how the allocation of safety integrity requirements across different elements of a

¹ Refer to “Definitions” for the definition of “exposure to the hazard”

system can be defined on a more rigorous basis. The allocation can be to:

One or more sub-elements of an electronic system;
Non-electronic (i.e. “other technology”) elements of the system;
External risk reduction facilities.

THE PROCESS OF SAFETY INTEGRITY ALLOCATION

A typical framework for automotive hazard analysis incorporates the following steps [1]:

Hazard identification;
Hazard classification;
Risk analysis.

The basis of hazard classification is to evaluate the risk associated with each hazard based on the severity of the hazardous event, the probability of exposure in the hazardous situation, and the possibility to avoid the hazardous event.

Risk analysis then relates the hazard classifications to the safety integrity required of the system in order to provide adequate risk reduction to reduce the hazard risk to the “broadly acceptable” level. Standards show how this hazard classification is related to the required risk reduction. In the MISRA Safety Analysis Guidelines [2] the hazards are classified using the parameter R , which is the risk associated with the hazard before any risk-reducing schemes are devised. It is shown how R can be related to both random and systematic safety integrity requirements. The latter are measured using SILs that, unlike those of IEC 61508, do not include a random requirement. The random requirements are expressed separately, and can be either qualitative or quantitative. The quantitative requirements are implicitly assumed to be equivalent to IEC 61508. For example, R4 maps to SIL 3 for systematic requirements; and an example of how a quantitative requirement can be derived is given which gives a target failure rate between 10^{-7} and 10^{-8} per operating hour, i.e. equivalent to the IEC SIL 3 requirement. The mapping shown in the MISRA Safety Analysis Guidelines assumes that all of the risk reduction will be achieved through a single programmable electronic system.

In ISO CD 26262 the ASIL is a measure of both the hazard classification **and** the required risk reduction. The ASIL therefore assumes a one-to-one mapping between these separate quantities.

These mappings assume that all of the required risk reduction will be achieved by a single programmable electronic system and that there are no “external risk

reduction facilities” or “other technology safety-related systems” as envisaged by IEC 61508. However, there are a number of circumstances where the risk analysis may wish to include such credit:

- The existence of an external or other technology risk reduction feature, for example a mechanical device that protects against a dangerous state that could be requested by an electronic system.
- Prototype or developmental use of vehicles, where risk reduction can be claimed from “external” measures such as the use of specially-trained drivers or a closed circuit on a test track. This is a special case of an “external risk reduction” measure.
- Architectural features of the electronic system implementation that mean that the overall risk reduction requirement can be achieved by two or more independent elements.

IEC 61508 acknowledges this step in Part 1 Section 7.6 “Safety requirements allocation”. Essentially this step takes safety integrity requirements, which are expressed in terms of risk reduction, and allocates them to one or more risk-reducing facilities. Where the risk reduction is allocated to one or more electrical, electronic or programmable electronic systems, this is further allocated with the result that a SIL is allocated to each **individual** electronic system. Thus the overall risk reduction can be achieved by:

- One or more electronic safety-related systems **and/or**
- One or more “other technology” safety-related systems **and/or**
- One or more external risk reduction measures.

Thus, for example, a system with an overall requirement for risk reduction of MISRA R4 may allocate these requirements to two independent electronic systems. If the risk reduction were to be achieved through a single electronic system, then the requirements for risk reduction would be expressed as SIL 3. A rigorous scheme is therefore needed to define what SIL should be allocated to the individual independent systems that together achieve the overall risk reduction requirement expressed as SIL 3.

SAFETY INTEGRITY ALLOCATION SCHEMES

In this section the schemes for safety integrity allocation in three identified standards: IEC 61508, Def Stan 00-56 and ISO CD 26262 are presented and discussed.

IEC 61508 – IEC presents a scheme for safety integrity allocation in Part 2, under the requirements for architectural constraints on hardware safety integrity (see clause 7.4.3.1). It is permissible to claim, for

example, a SIL 3 risk reduction from two SIL 2 subsystems provided they are adequately independent. The example in Figure 6 of Part 2 is not particularly well presented, but essentially the argument is based upon the concept of “hardware fault tolerance” i.e. a hardware fault tolerance of N means that $N+1$ faults could cause loss of the safety function.

A brief explanation of this concept is presented as follows. The SIL that can be claimed for an element of a system is comprised of three aspects in IEC 61508:

- The predicted random failure rate for the hardware;
- The level of coverage against dangerous failures achieved by diagnostic features (expressed as the “safe failure fraction”, SFF);
- The level of robustness against systematic faults in both the development process and the product of that process.

Consider an element that implements a certain safety function, and the development has been shown to meet the requirements of SIL 2 for the random and systematic requirements, and the element has an SFF between 90% and 99%. If a single failure in an element can cause loss of the safety function then the hardware fault tolerance is defined to be zero.

Consider now the case that the function is implemented through two completely independent elements for which the following are true:

SIL 2 and the SFF between 90% and 99% can be claimed for both elements;
 There is no common cause failure that could lead to loss of the safety function.

This architecture is deemed to have a hardware fault tolerance of 1, i.e. both of the two elements must fail (without a common cause failure) to cause loss of the safety function.

Taking an extract of Table 3 of Part 2 for this specific safe failure fraction it is found that:

Safe failure fraction	Hardware fault tolerance		
	0	1	2
90% – < 99%	SIL 2	SIL 3	SIL 4

Thus an overall risk reduction of SIL 3 can be claimed based on these architectural constraints.

Figure 1 shows a practical example of this IEC SIL allocation scheme. In this example the safety function is to shut down the flow of a reagent in a process by closing a valve. The overall risk reduction is SIL 3, and

this is achieved through two independent lanes both of which are claimed to provide a risk reduction commensurate with SIL 2.

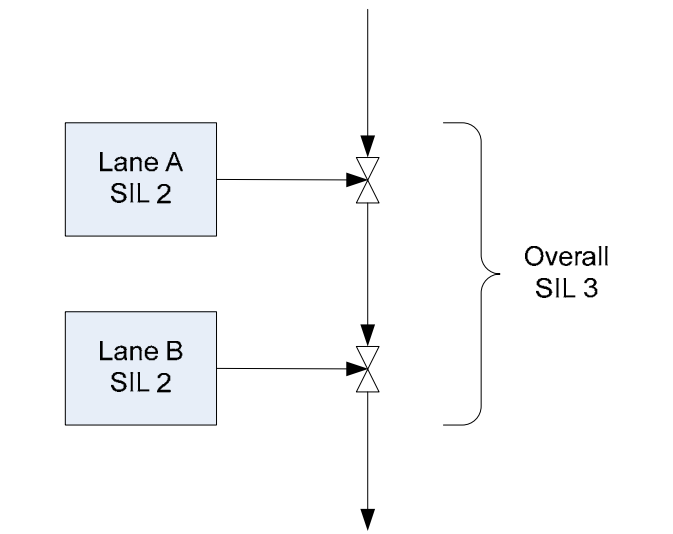


Figure 1: IEC 61508 concept of SIL allocation

The following observations may be made on this scheme:

The standard implies a bottom-up approach to analyzing the architecture. This consists of the following steps:

- For an individual element, the diagnostic coverage, its own hardware fault tolerance and the type of system (A or B — related to factors such as complexity) lead to a SIL claim for the element.
- For elements that are architecturally not redundant, that is, a failure in any one element can lead to loss of the safety function, then the SIL that can be claimed for that branch of the architecture is the **lowest** SIL of the constituent elements.
- For elements that are architecturally redundant, that is, simultaneous failures in all elements have to occur to lead to loss of the safety function, then the SIL that can be claimed for that branch of the architecture is the **highest** SIL of the constituent elements increased by one for each additional independent element. This implies that, for example, the following claims could be made:

$$\begin{aligned} \text{SIL 2} + \text{SIL 1} &\rightarrow \text{SIL 3} \\ \text{SIL 2} + \text{SIL 2} &\rightarrow \text{SIL 3} \\ \text{SIL 2} + \text{SIL 1} + \text{SIL 1} &\rightarrow \text{SIL 4} \end{aligned}$$

However it should be noted that the algebra is not performed on the SILs directly.

Criticality analysis In IEC CD 61508 Edition 2 [6] a further process, called “criticality analysis” is provided. This is aimed at analysis of the systematic aspect of

SILs. If a function is composed of two or more elements, then if a single deviation in an element from a specified function cannot cause an unsafe situation, but in combination with a second failure of another element may cause an unsafe situation then the SIL of the element may be decreased by one level. A SIL 1 element cannot be reduced further. The standard discourages claiming more than one level of SIL reduction since “there is not yet enough experience with the effectiveness of measures to avoid common cause initiators of systematic failures.” Thus from a **systematic** aspect a top-down decomposition of SIL n into two or more SIL ($n-1$) elements is permitted. However the elements need to be functionally diverse. Furthermore, any element such as a voter or comparator has to conform to the requirements of the highest SIL being claimed.

In summary IEC 61508 implies a bottom-up approach to analyzing the aspects of architectures relating to random failures, and a top-down approach to systematic failures.

DEF STAN 00-56 – Edition 2 of this standard [7] incorporated a scheme for SIL partitioning. Essentially one provision of this scheme was that SIL n could be achieved by two SIL ($n-1$) functions provided these functions were strictly independent and that any “combiner” also met the requirements of SIL n . This is very similar in practice to the “criticality analysis” described in IEC 61508-2 Edition 2 [6] although the latter includes more specific requirements for demonstrating the independence.

Thus the following allocations, amongst others, were permitted:

- SIL 4 $\rightarrow$ SIL 3 + SIL 3
- SIL 3 $\rightarrow$ SIL 2 + SIL 2
- SIL 2 $\rightarrow$ SIL 1 + SIL 1

This scheme has since been removed from the latest edition, Def Stan 00-56 (Issue 4), and the authors understand that this is because it was being misused to argue down the SIL allocated to systems without sufficient justification.

ISO CD 26262 – ISO incorporates a scheme called “ASIL decomposition”. As with IEC 61508, this scheme is not presented clearly in the standard, and at present does not have any rationale behind it, but essentially it is claiming that an overall allocation of an ASIL to a system can be decomposed into lower ASIL requirements for the architectural elements that comprise it if those elements are sufficiently independent.

The permitted decompositions are:

ASIL D $\rightarrow$ ASIL C + ASIL A
ASIL D $\rightarrow$ ASIL B + ASIL B
ASIL C $\rightarrow$ ASIL B + ASIL A
ASIL B $\rightarrow$ ASIL A + ASIL A

ISO CD 26262 also permits decomposing (ASIL x) to (ASIL x + QM) but this effectively refers to partitioning safety-related vs. non-safety-related elements and is not considered further for the purposes of this discussion.

“Confirmation measures” and “independence of the elements” have to be shown in accordance with the initial ASIL. This means, for example, that decomposition cannot be used as a way to avoid the full independent safety assessment requirements for an ASIL D system. The notation ASIL $y(x)$ is used to denote a decomposed ASIL, where x is the original ASIL and y the decomposed ASIL. Thus in the case where ASIL D is decomposed into ASIL C and ASIL A elements, these are labeled ASIL C(D) and ASIL A(D) respectively to signify that some requirements remain at the ASIL D level.

ISO CD 26262 also incorporates a scheme for criticality analysis that is very similar to that given in IEC 61508 Edition 2. However this scheme is only intended to be applied to individual functions within an element, e.g. where an electronic control unit contains a mixture of functions with different allocated ASILs.

ISO CD 26262 is silent on the concept of any “comparator”, “voter” or “combiner” acting on the outputs of the individual channels or elements and consequently on any requirements for such an element.

REQUIREMENTS FOR A DECOMPOSITION SCHEME

In this section some requirements for developing a rigorous scheme for automotive decomposition of safety integrity requirements are considered.

SCOPE – the scheme needs to be applicable at several architectural levels. These are:

When taking into account inherent risk reduction due to the circumstances in which the vehicle is to be used.
When allocating the overall required risk reduction to electronic systems and/or “other technology” safety-related systems and/or external risk reducing measures.