

Safety Integrity Level (SIL) allocation and Due Diligence

Richard M Robinson BE BA FIEAust
 Director, Risk & Reliability Associates (R2A) Melbourne

Ing Alain Ducheyne MBC
 Engineer, Risk & Reliability Associates (R2A), Melbourne

SUMMARY: Safety Integrity Level (SIL) ratings are being applied extensively to safety control systems generally, and in power stations and networks particularly, using the concepts embodied in AS (IEC) 61508. This has often proven an expensive and frustrating exercise for asset owners especially since the integration of SIL concepts with other established risk based processes has proven both elusive and expensive. This paper outlines a method of satisfying technical due diligence requirements and the SIL allocation provisions of AS (IEC) 61508 simultaneously with both statutory and common law provisions in Australia.

1.0 INTRODUCTION

The concept of SIL (Safety Integrity Level) appears to come from the IEC 61508 standard, officially introduced in 1998 in Europe. In 2002 it was endorsed as an Australian Standard. The standard consists of 7 parts:

- IEC 61508-1 General requirements.
- IEC 61508-2 Requirements for Electrical/Electronic/Programmable Electronic Safety related systems (E/E/PES).
- IEC 61508-3 Software requirements.
- IEC 61508-4 Definitions and abbreviations.
- IEC 61508-5 Examples of methods for the determination of Safety Integrity Levels (SIL).
- IEC 61508-6 Guidelines of the application of part 2 and 3.
- IEC 61508-7 Overview of measures and techniques.

IEC 61508 is considered by the International Electrotechnical Commission (IEC) to be an enabling standard and is the basis for IEC 61511, the process control standard amongst others. Never the less, IEC 61508 is still commonly used on a stand alone basis. It entails a generic approach for the development, installation, use, modification, maintenance and the decommissioning of E/E/PE systems used for providing safety functions on equipment under control. Its purpose is to provide a protocol to minimise dangerous failures in E/E/PE systems.

The standard defines that the rating of an E/E/PE safety related system should be held in consideration when applying a SIL achievement standard. This is mentioned so that the use of high level SIL ratings are not used for lower level safety systems. Of course this is where SIL allocation comes into play and it is here that asset owners struggle the most with the IEC 61508 standard.

2.0 IEC 61508 AND SIL RATINGS

Safety Integrity Levels (SIL) are four levels of safety performance for safety functions as defined in the IEC

61508 standard, SIL 1 being the lowest and SIL 4 the highest. Usually the higher levels (3 and 4) are used for safety critical systems such as “vital” signalling. The lower levels are reserved for non-vital and communication systems which are safety related.

Each SIL level also has a distinction between continuous control (high demand) and on demand use (low demand). The necessary demands to meet each SIL requirement under the different situations are listed below in Table 1.

		<i>Continuous control</i>	<i>On demand</i>
		Probability of dangerous failure per hour	Average probability of failure to perform its design function on demand
<i>Safety-critical</i>	SIL 4	1E-9 to 1E-8	1E-5 to 1E-4
	SIL 3	1E-8 to 1E-7	1E-4 to 1E-3
<i>Safety-related</i>	SIL 2	1E-7 to 1E-6	1E-3 to 1E-2
	SIL 1	1E-6 to 1E-5	1E-2 to 1E-1

Table 1. SIL Values

By way of illustration, Table 2 shows the years between failures based on the continuous mode of operation. The demand mode of operation table seems to be an alternative way of describing what is usually known as fractional dead-time. No explanation for how any of these numbers were determined appears to be made.

	years between failure	
SIL 4	114,155	to 11,416
SIL 3	11,416	to 1,142
SIL 2	1,142	to 114
SIL 1	114	to 11

Table 2: Years between failure for continuous control

Functional Safety Assessment, the process of investigating and determining the achieved functional safety of E/E/PES, may recognise commercial off-the-shelf systems with 95% availability and best practice as SIL1. SIL2 requires compliance to the process as specified in IEC 61508 and best practice. SIL3 appears to require redundancy (needs to take account of common mode failures) and formal methods, while SIL4 would be expected to require triple redundancy.

3.0 LEGAL CONTEXT

In common law jurisdictions the approach outlined in IEC 61508 may not sit well. This may be why it has sometimes come in for some harsh criticism, for example:

The standard (IEC 61508) is without practical value or merit. The methods described are inconsistent with accepted industry practices, and many of them are known only to specialist academics, presumably including the members of the drafting committee. O’Conner (2002).

Although being referred by regulators, the IEC 61508 standard and its derivatives do not appear to have been implemented in Australian regulation to date. So until they are mandated they remain subordinate to the current OH&S legislation in Australian jurisdictions. This means that the hierarchy of controls must be applied. In Australia the legislated hierarchical order of risk control is typically:

- i) Elimination or removal
- ii) Design or engineering
- iii) Administration
- iv) Training

This makes for an essential observation, that usually civil and mechanical design is logically prior and normally dictates SIL requirements, if any, since if a hazard or problem can be eliminated or engineered out then a SIL rated electronic control system to manage such a hazard ought not to be required. Following the hierarchy of controls, it is actually illegal in Australia to adopt an active control system when a practical elimination option is available.

For example, if grade separation can be achieved then all the complexity associated with a train level crossing is eliminated. This intention is noted in the standard in Section 7.4.2.2:

Although not within the scope of this standard, it is of primary importance that determined hazards of the EUC are eliminated at source, for example by the application of inherent safety principles and the application of good engineering practice.

In common with other recognised standards or codes of practice IEC 61508’s legal status would probably be that of *recognised good practice*, or more particularly,

that many of the ideas in IEC 61508 are regarded as *recognised good practice*. As such its use would not be a definitive defense in the event of an accident where its application may be claimed to have had a beneficial effect. The caveat placed on many UK standards probably applies, namely: *Compliance with a British Standard does not of itself confer immunity from legal obligations.* (BS 5760:1993).

This means that the target levels of safety approach, suggested by the standard and used by many, would not be expected to survive legal scrutiny after a loss event if a added minor barrier could have reduced the level of risk significantly.

4.0 SIL ALLOCATION

As noted in the background, IEC 61508 is comprised of seven parts. The allocation of the appropriate SIL rating (or hazard and risk assessment) is being conducted in the first part of the standard with Part 5 providing some risk based methods of achieving this.

It is here that the greatest difficulties seem to appear for the industry and so it is on this aspect that the paper will focus. Figure 1 below shows a generic “V” model for the R2A method of SIL rating assessment.

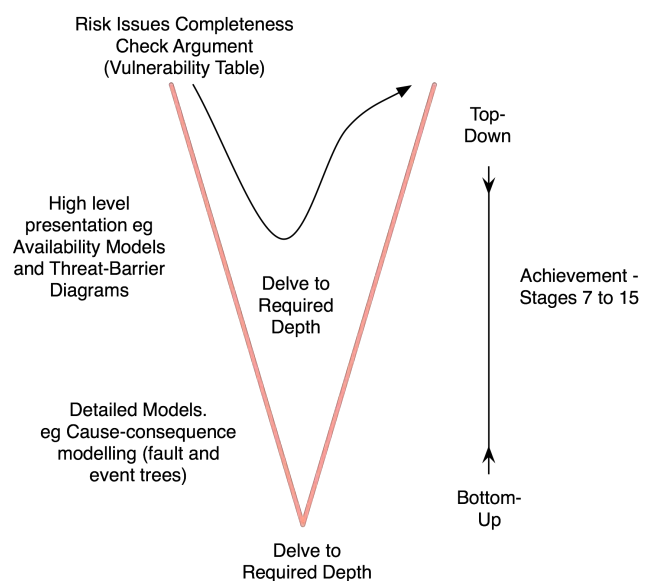


Figure 1: Top Down ‘V’ Model

In summary, the method starts with the identification of all credible threats and hazards of a system under consideration. This is followed by the creation of threat barrier sequences (sometimes known as bow-tie diagrams) to identify which means are or will best prevent these hazardous scenarios being realised. By examining each barrier within its overall context is possible to determine how vital each is and so determine what SIL rating each barrier requires. If there is an E/E/PE SIL component to a barrier, it can then be allocated in context of the overall threat scenario. A

Hazard Control System Failure Analysis (HCSFA) and sign off by the collective participants should then be completed.

R2A believes that such a process will satisfy common law safety case arguments for the allocation of SIL ratings on E/E/PE safety-related systems. The method provides clarity so that senior management can easily understand the allocation process and, if necessary, judges and juries. Each step is considered in more detail in the following sections.

4.1 Complete, Credible, Critical

A vulnerability assessment is used to determine the hazardous situations which might occur.

The strength of this vulnerability technique is that if you have identified all of the critical success factors, assets and exposed groups (the things which you want to protect) and all the credible threats that get exposed to the former, you get a complete check of all the hazardous scenarios that might occur.

A simple example of such a criticality vulnerability assessment is shown below. The intersections of threats and assets are the vulnerabilities of the system in question. This tool also enables to evaluate the gravity of the vulnerabilities which can help to set priorities if need be (for example to re-evaluate design factors).

Assets>>	Travelling Public	Operator Staff	Emergency Services	Local Residents	Habitat/Air quality	Infra-structure
<u>Threat Scenarios</u>						
HCV load fire stationary vehicle in free flowing traffic	xx	xx	xxx	x	x	x
HCV vehicle fire burning vehicle in stationary traffic	xxx	xxx	xxx	x	x	x
Injury/entrapment accident - all lanes blocked	xx	x	x	-	-	-
Fatal accident - all lanes blocked	xx	x	x	-	-	-
Pedestrians in Tunnel on walkway	x	x	x	-	-	-
Cyclist in Tunnel	xx	x	x	-	-	-

Table 3 Sample Vulnerability Table for a Tunnel

4.2 Threat-barrier sequences (bow-tie diagrams)

Once all threat scenarios have been identified, a time sequenced threat barrier diagram can be created for each. This should be used to represent all expected hazard control barriers consistent with the hierarchy of controls under OH&S legislation.

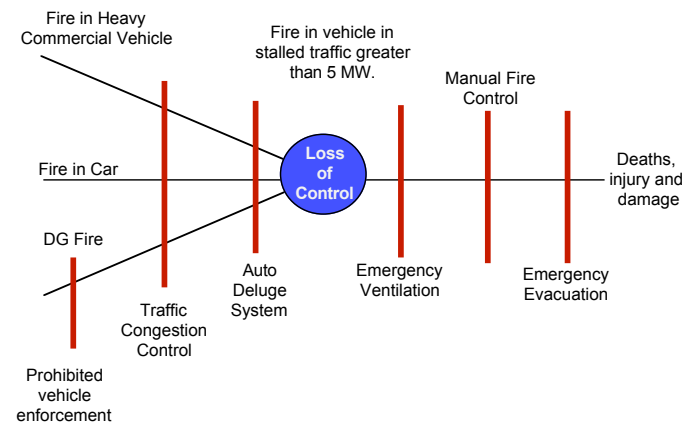


Figure 2. Threat-Barrier Diagram

This legislation requires that hazard elimination and passive engineering options are logically prior to active controls. If these passive options cannot adequately resolve the hazard, active engineering options using E/E/PE can then be considered.

4.3 Barrier SIL

To accurately determine the SIL rating for a barrier, the decision group must have knowledge of the full context in which this barrier is situated. If there are many other reliable barriers in place (preferably passive ones) then active barriers using E/E/PE should be irrelevant.

For example, if the sighting distance in Figure 3 (above) is excellent, then the variable message signalling will be of little importance. However if in that same diagram the sighting distance is reduced in effectiveness (for example an upcoming turn) then the relevance of the variable message signalling will be higher. In the latter case a safety allocation of the variable message signalling system will have more value.

In practice this means that the SIL rating for the E/E/PE is a subset of the SIL rating of the barrier as a whole. Thus a further term, barrier safety integrity level or Barrier SIL will be used to describe the probability of success of an independent safety barrier. This can be a function of the E/E/PE SIL, failure modes of the Equipment Under Control (EUC), operator errors, internal and external common mode failures of the barrier under consideration.

E/E/PE SIL is a thus a function of software safety integrity level (Software SIL), hardware safety integrity level (Hardware SIL) and systematic safety integrity level (Systematic SIL) for the described E/E/PE system.

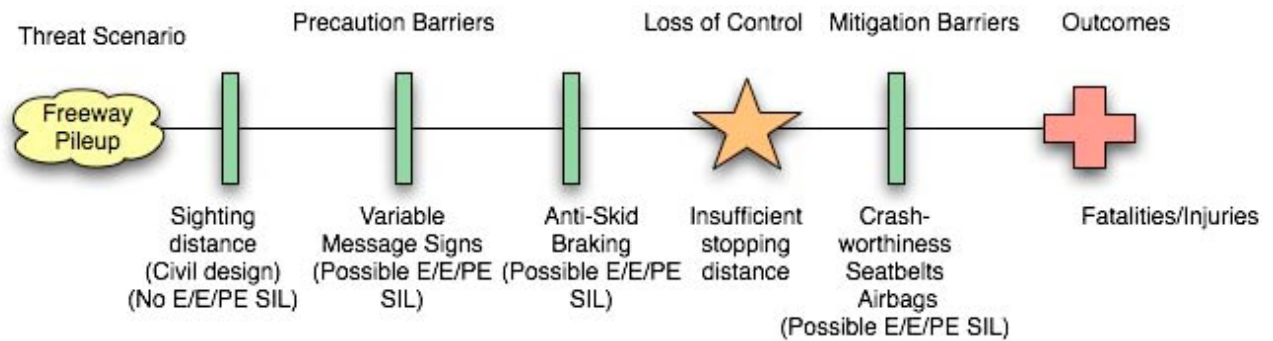


Figure 3. Threat-Barrier diagram for Freeway Collision

4.4 E/E/PE SIL

In many cases, the primary hazard control barriers will be of an exclusively mechanical or civil design, thus the E/E/PE aspect will not be present at all. If there is an E/E/PE contribution, it will still be subject to two constraints.

Firstly, it is generally pointless in having an E/E/PE SIL which is more reliable than the individual barrier it is constrained to (for example the reliability of a mechanical barrier).

Secondly, an E/E/PE SIL with an elevated contribution may very well be pointless in the overall context of the existing barriers since the safety outcomes of a particular scenario are determined by the collective independent barriers in place. If there are multiple barriers present, the high E/E/PE SIL rated aspect might be negligible or it could be more efficiently addressed by another barrier.

As a general observation on risk design philosophy, it is almost always better (risk and/or financial wise) to have a large number of independent, low reliability barriers in place than to have relatively few highly reliable (gold plated?) barriers.

4.4 Hazard control system failure analysis

If an E/E/PE SIL has been allocated, the consequences and implications of the malfunction of the E/E/PE controls system need to be examined. If the findings of these examinations reveal any potentially dangerous failures of control systems, acquiring further E/E/PE SIL allocations should be contemplated.

4.5 Review sign-off

A final test of any risk process should be a question of the participants as to whether there are any outstanding issues or good ideas that have not been raised to date but which ought to have been considered.

5.0 CONCLUSION

Paramount to allocating a SIL rating to a barrier, or part of it, is having a sound overview of the context in which the barrier is (to be) placed. To achieve such an overview all credible threat scenarios must be identified and the impact of the barrier on them assessed.

If this is not done, it seems difficult to see how Australian legislative (OH&S) and common law provisions can be met.

6.0 REFERENCES

- O'Conner Patrick D T (2002). Practical Reliability Engineering. John Wiley & Sons. Fourth Edition.
- Robinson, Richard M, Gaye E Francis et al 2007. *Risk & Reliability - An Introductory Text* (7th ed.) R2A Pty Ltd Melbourne.
- Standards Australia 2002. AS 61508: 2002 (IEC 61508:1998).