

TECHNICAL DUE DILIGENCE AND SAFETY INTEGRITY LEVEL (SIL) ALLOCATION

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

Tim Procter BE GradIEAust
Engineer, Risk & Reliability Associates (R2A), Melbourne

Summary: The adoption of IEC 61508 as an Australian Standard has seen an increased use of Safety Integrity Level (SIL) ratings in many industries. However, when applying such a standard it is imperative that it is done in its proper context. This paper outlines a safety assessment process which considers both statutory and common law duty of care during the SIL allocation process.

Keywords: Technical due diligence, Safety Integrity Levels (SIL), IEC (AS) 61508.

1.0 INTRODUCTION

The rising popularity of IEC (AS) 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-related Systems*, and the associated application of Safety Integrity Level (SIL) ratings, has proved surprising complex in some industries.

In Victoria for example, following Maxwell QC's 2004 review of the Victorian Occupational Health and Safety (OHS) Regulations, the use of risk assessments in general and target levels of risk in particular are no longer necessary to ensure *due diligence* is achieved during safety assessments. This type of thinking has profound implications on traditional SIL allocation processes.

2.0 IEC (AS) 61508: FUNCTIONAL SAFETY OF E/E/PE SAFETY-RELATED SYSTEMS

The International Electrotechnical Commission first published IEC 61508 in 1998 as a seven part document. The various sections were adopted by Standards Australia as AS 61508 between 1999 and 2001.

IEC 61508 is a European derived standard which addresses the functional safety of safety related systems by ... *setting out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components ... that are used to perform safety functions.*

Safety in this context is defined as ... *freedom from unacceptable risk.* Functional safety is defined as the ... *part of the overall safety relating to the EUC (equipment under control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities (IEC 61508 Pt 4 §3.1.8-9).*

The standard also aims to enable the development of other international standards dealing with E/E/PE safety-related systems that are used to perform safety functions on equipment under control (EUC). Application sector international standards have since been developed for a variety of industry sectors, such as IEC 61513 for the nuclear sector and IEC 61511 for the process sector.

The standard consists of seven parts:

- IEC 61508-1 General requirements.
- IEC 61508-2 Requirements for electrical/electronic/programmable electronic safety-related systems.
- IEC 61508-3 Software requirements.
- IEC 61508-4 Definitions and abbreviations.
- IEC 61508-5 Examples of methods for the determination of safety integrity levels.
- IEC 61508-6 Guidelines on the application of IEC 61508- 2 and IEC 61508-3.
- IEC 61508-7 Overview of measures and techniques.

Parts 1, 2, 3 and 4 of IEC 61508 are basic IEC safety publications that are referenced by other IEC standards.

In general, IEC 61508 addresses the safety aspects of E/E/PE systems by specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety related systems. Safety integrity is defined as the ... *probability of a safety related system performing the required safety functions under all the stated conditions within a stated period of time (IEC 61508 Pt 4 §3.5.2).*

The Safety Integrity Level (SIL) specifications and ratings are given in the table below:

		<i>Continuous control</i>	<i>Low 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 (Highest)	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 (Lowest)	1E-6 to 1E-5	1E-2 to 1E-1

Table of SIL values

The authors note that the standard does not appear to give any explanation for how these numbers were determined.

	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

Years between failure for continuous control

The standard requires that an investigation, known as a functional safety assessment, use evidence to judge the functional safety achieved by the combination of any E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

Based on R2A experience, a functional safety assessment may recognise commercial off-the-shelf (COTS) systems with 95% availability and best practice as SIL 1. SIL 2 requires compliance to the process as specified in IEC 61508 and best practice. SIL 3 appears to require redundancy (taking into account common mode failures) and formal methods, while SIL 4 would be expected to require triple redundancy.

3.0 AUSTRALIAN LEGAL CONTEXT

IEC 61508 appears to have been derived in the context of the European Roman law/inquisitorial system, in the most part due to the requirement that *...one or more persons shall be appointed to carry out a functional safety assessment in order to arrive at a judgement of the functional safety achieved by the E/E/PE safety-related systems* (IEC 61508 Pt 1 §8.2.1).

However, when using this as a basis for safety assessments in Australian adversarial-based legal jurisdictions, care must be taken to ensure that statutory, regulatory and common law requirements are satisfied. To this end, a number of other safety assessment paradigms and considerations must be taken into account.

3.1 Statutory and Regulatory Requirements

IEC (AS) 61508 has not to the authors' knowledge been called up by statute or regulation in Australia to date. This means that it probably represents recognised good practice under Australian OH&S legislation and common law.

OH&S legislation is generally recognised as a statutory statement of the common law duty of care. While the OH&S legislation varies slightly between states, the basic premise is that options for hazard control should encompass, in order of priority:

- i) Elimination or removal
- ii) Design or engineering
- iii) Administration
- iv) Training and personal protective equipment

Civil and mechanical measures often precede E/E/PE control systems in the control of a hazard. If a reasonable method of eliminating the hazard is cost effectively available, it is actually illegal in Australia to allow the hazard to remain and provide an active control.

This is addressed (somewhat briefly) in IEC 61508 Pt 1 §7.4.2.2 and its associated note:

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 general, it appears that Australian jurisdictions may be moving away from mandating risk

assessments as part of safety assessments, as discussed in more detail in the following section.

3.2 Common Law Requirements

Common law requirements are determined through the concept of the 'duty of care'. The duty of care is essentially a legal test of the reasonableness of any attempts to reduce or eliminate a foreseeable risk.

A duty of care exists where there is reasonable foreseeability of injury to anyone, allowing for a proximity of plaintiff and defendant. The duty is breached if the required standard of care is not met.

The standard of care is the degree of care expected of a reasonable person for the particular circumstances in question. In general, the actions of a reasonable person demonstrating a degree of care will comprise both the identification of a hazard and the determination of a control to address it.

The generic methods of assessing hazards and determining controls are provided in the table from the Engineers Australia Safety Case Guideline 2007, below. In general, combinations of some or all of the techniques highlighted in the will be required.

Technique>> Risk Management Paradigm		Expert reviews	Facilitated workshops	Selective interviews
1.	The rule of law	Yes (Legal opinions)	Yes (Arbitration, moot courts)	Yes (Royal Commissions)
2.	Insurance approaches	Yes (Risk surveys, actuarial studies)	Yes (Risk profiling sessions)	Yes (especially moral risk)
3.	Asset based, 'bottom-up' approaches	Yes (QRA, availability & reliability audits)	Yes (HazOps, FMECAs etc)	Difficult
4.	Threat based 'top-down' approaches	Difficult in isolation	Yes (SWOT & vulnerability)	Yes (Interviews)
5.	Solution based 'good practice' approaches	Difficult to be comprehensive	Difficult to be comprehensive	Yes (Fact finding tours)
6.	Simulation	Yes (Computer simulations)	Yes (Crisis simulations)	Difficult
7.	Risk culture concepts	Yes (Quality audits)	Difficult	Yes (Interviews)

Risk Management Paradigm - Technique Matrix
(Engineers Australia Safety Case Guideline 2007)

3.3 Good Practice vs Risk Assessment

The good practice concept suggests that if there is a recognised accepted precaution being used in a similar situation or situations, then this should be the initial basis for any control adopted for the specific hazard.

This is reflected in Victoria's OHS Regulations as of 1 July 2007, with the revised regulations having a:

...new emphasis on enabling employers and workers to focus their efforts on controlling rather than assessing risk.

(Streamlining Victoria's OHS Regulations – information sheet January 2007).

This is further expanded in the Regulatory Impact Statement, Occupational Health and Safety Regulations 2007, Equipment (Public Safety) Regulations 2007:

Further, mandating risk assessments may be a barrier to the implementation of risk controls. For example, where hazards and risks are well known and there are universally accepted control measures, a duty holder may identify the hazard and implement the appropriate control without doing a risk assessment. In these cases, a risk assessment would yield no new knowledge and would be likely to delay the implementation of controls.

This view is also advocated by the UK Health and Safety Executive (*Reducing Risks, Protecting People* (2001) Appendix 3):

... the starting point should be an option which is known to be reasonably practicable (such as one which represents existing good practice). Any other options should be considered against that starting point, to determine whether further risk reduction measures are reasonably practicable.

Taking the good practice concept into account, a SIL allocation should only be considered in the context of controls that others in the industry are using.

Note too that it is the ideas in standards that are recognised as good practice, and, as such, IEC 61508 could be considered a reasonable starting point for control measures. However, compliance with a standard does not ensure compliance with legal obligations. Australian and British Standards sometimes provide disclaimers, for example:

Compliance with this Standard may not necessarily meet your OHS legal obligations.

(AS/NZS 4801:2001 Occupational health and safety management systems)

TECHNICAL REQUIREMENTS		OTHER REQUIREMENTS
<p>PART 1 Development of the overall safety requirements (concept, scope definition, hazard and risk analysis)(E/E/EP safety-related systems, other technology safety-related systems and external risk reduction facilities) Stages 1 to.5</p> <p>PART 1 Allocation of the safety requirements to the E/E/PE safety-related systems. Stage 6</p> <p>PART 2 Realisation phase for E/E/PE safety-related systems (mutual feedback with Part 3)</p> <p>PART 3 Realisation phase for safety-related software</p> <p>PART 1 Installation and commissioning and safety validation of E/E/PE safety related systems. Stages 13 and 14</p> <p>PART 1 Operation and maintenance, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems. Stages 15 to 17</p>	<p>PART 5 <i>Risk based approaches to the development of the safety integrity requirements</i></p> <p>PART 7 <i>Overview of techniques and measures</i></p> <p>PART 6 <i>Guidelines for the application of parts 2 and 3</i></p>	

Overall framework for IEC 61508 (adapted from IEC 61508-1:1998)

Further, as discussed below, the use of target levels of risk raises some significant points regarding the common law duty of care.

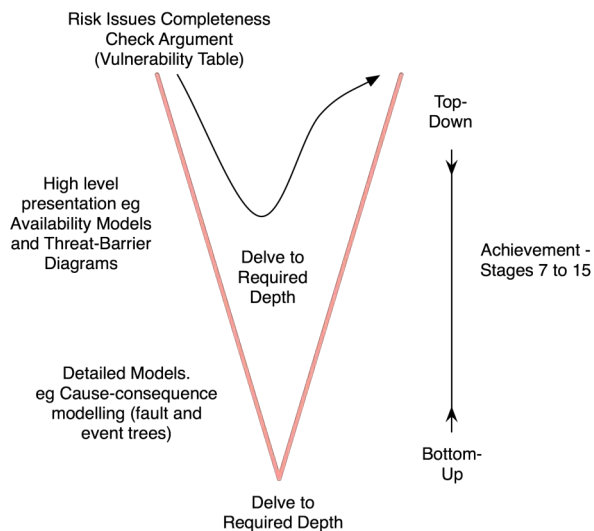
3.4 'Acceptable' to 'Not Intolerable'

If determined that a risk assessment is required to address a particular hazard, IEC 61508 may prove useful. However, it is important to note that, in order to meet the common law duty of care, it would appear that risk management is moving away from the concept of 'acceptable' risk to 'not intolerable' risk. This appears to be supported by

the cessation of the use of the term 'acceptable risk' in the 2004 revision of AS/NZS 4360:2004 *Risk Management*.

Provided a risk is not intolerable, that is, prohibitively dangerous, in which case the activity involving the hazard must immediately stop, implementation of controls is subject to the balance of the significance of the risk reduction versus the effort required to reduce it. Effort, in this case, may encompass time, expense, difficulty and inconvenience.

This implies that there is no lower limit to risk when deciding on control measures. If, for very little effort or cost, a small risk can be further reduced, then in the event that it occurred, given a duty of care existed and was breached and material damages resulted, the failure to have further reduced the risk will give rise to negligence.



Top Down 'V' Model

This concept is summarised by Chief Justice Gibbs of the High Court of Australia:

Where it is possible to guard against a foreseeable risk which, though perhaps not great, nevertheless cannot be called remote or fanciful, by adopting a means which involves little difficulty or expense, the failure to adopt such means will, in general, be negligent.

Turner v. The State of South Australia (1982) (High Court of Australia before Gibbs CJ, Murphy, Brennan, Deane and Dawson JJ).

In practice, risk tends to 'pixelate' as it is reduced lower and lower, with the determination of any benefits of further controls becoming difficult to establish.

4.0 IDEALISED E/E/PE SIL ALLOCATION

In view of the complexities discussed above, the application of IEC 61508 has led to a significant amount of intellectual confusion in industry especially in the hazard and risk assessment aspects of the safety allocation elements.

In order to address the requirements of stages 1 to 6 of Part 1 of the standard (shown in the diagram opposite), the hazard and risk assessment aspects

and safety allocation elements, R2A typically use the following process:

- i) Establish All Credible, Critical Threat/Hazard Scenarios
- ii) Develop Threat-Barrier Sequences
- iii) Determine Barrier SIL
- iv) E/E/PE SIL Allocation (if required)
- v) E/E/PE SIL Hazard Control System Failure Analysis
- vi) Review Sign-off

This process takes into account the requirements of a common law duty of care.

This process can also be represented by a 'V' model shown adjacent.

The experience of the authors is that such a process would satisfy common law arguments for E/E/PE SIL allocation since, inter alia, it should be comprehensible to judges and juries as well as senior management.

4.1 Credible critical threat/hazard scenarios

Using a criticality vulnerability assessment (hazard identification) determine the hazardous situations which might occur. This is a high level completeness check to construct an argument as to why there is confidence that no credible hazardous scenario has been overlooked. A simple sample vulnerability matrix for a freeway is shown below.

<u>Assets>></u>	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	-	-	-

Sample Vulnerability Table for a Tunnel

Note that the threat scenarios can be expanded into different mechanisms.

4.2 Develop threat barrier sequences

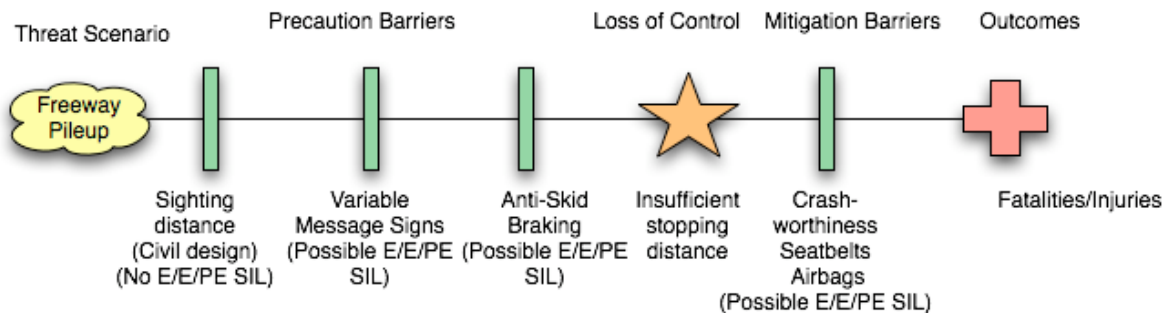
For each of the hazardous scenarios identified a time sequenced threat barrier diagram (called ‘bow-tie’ diagrams in some industries) is created showing all the expected hazard control barriers consistent with the hierarchy of controls under OH&S legislation. That is, elimination and passive engineering options are considered first and active engineering controls second. The

following diagram shows a concept event sequence for a multi-car freeway pile-up.

4.3 Barrier SIL Determination

The effectiveness of each of the identified barriers is determined. To determine the E/E/PE SIL allocation it is absolutely necessary to understand the overall context in which the E/E/PE system finds itself.

If there are many other reliable (usually passive) barriers then the E/E/PE SIL allocation will be irrelevant.



Threat barrier diagram for a freeway pile-up

For example, on a freeway, sighting distance is a primary control. If the road is clear and straight (civil design) without any blind corners then the relative importance of variable message signs (VMS) will be small. Conversely, if there are many blind corners, the effectiveness of the sighting distance will be reduced and the variable message signs become significantly more important in risk control terms.

Reliance on post loss of control point measures under the hierarchy of controls is really a last resort and would not normally be considered in the initial SIL allocation. In practice this means that the SIL rating of the electronic, electrical or programmable equipment is a sub-set of the SIL rating of the precautionary barrier. Practically, this requires that a further definition for SIL is required in addition to the one in IEC 61508 Pt 4, §3.5.6:

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety and safety integrity level 1 has the lowest.

The authors hereafter describe the definition in IEC 61508 as *E/E/PE SIL*. *E/E/PE SIL* is 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.

A further term, Barrier Safety Integrity Level or *Barrier SIL* will be used to describe the probability (generally on demand) of success of an independent safety barrier. This can be a function of the *E/E/PE SIL*, failure modes of the EUC, operator error and any external and internal common cause or common mode failures of the barrier under consideration.

4.4 E/E/PE SIL Determination and Allocation

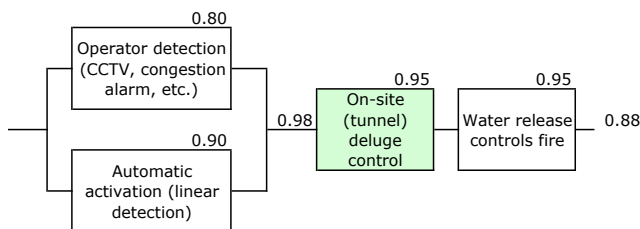
In very many cases barriers will be no E/E/PE aspect. That is, these barriers will be exclusively of civil or mechanical design. However, if required, the potential contribution of the individual E/E/PE SIL to each barrier is then determined. If there is an E/E/PE contribution then it is subject to two further constraints:

- a) There is no point in having an E/E/PE SIL more reliable than the individual barrier is constrained to by, for example, the reliability of the mechanical aspects of the barrier.

- b) The safety outcomes of a particular threat scenario are determined by the collective independent barriers, especially those prior to the loss of control point. If there are multiple barriers, there may be little point in having a barrier with an elevated E/E/EP SIL contribution or alternatively another barrier (external risk reduction facility or ERRF) may be best.

As an observation on risk design philosophy, it is almost always better (and cheaper) to have a larger number of low reliability, independent barriers than to have one or two highly reliable (gold plated) barriers.

For full traceability, reliability block diagrams (RBDs) can be used to describe the barriers and their components. A simple sample is shown below:



Sample Reliability Block Diagram

4.5 E/E/PE SIL Hazard Control System Failure Analysis

If an E/E/PE SIL has been determined and allocated then an analysis to consider the implications of the failure of the E/E/PE control system will be required. Potential dangerous failures of various active controls may determine if such possibilities require a further E/E/PE SIL allocation.

4.6 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 which had not been raised to date but which ought to have been considered.

5.0 CONCLUSIONS

When applying standards such as IEC 61508 to a safety assessment of any sort it is imperative to ensure that a context of the study is established.

Focusing exclusively on an isolated aspect of a safety system (such as individual E/E/PE equipment) may lead to excessive effort and SIL allocation that may be more appropriately addressed through other measures.

6.0 REFERENCES

Engineers Australia, Risk Engineering Chapter, Victoria Division (2007). *Safety Case Guideline*. Published via Engineers Media, Sydney.

International Electrotechnical Commission 1998. IEC 61508. *Functional safety of electrical/ electronic/ programmable electronic safety-related systems*.

Also known as AS 61508:1999.

Robinson, Richard M, Gaye E Francis et al 2007. *Risk & Reliability - An Introductory Text* (7th edition). R2A Pty Ltd Melbourne.