heroengineering
valued solutions

HERO ENGINEERING

AS/IEC 61508 Application to Guidelines in the Australian Mining Sector – Part 1 Fundamental Issues

For

Safe Work Australia – Public Discussion

Code of Practice
Underground Winding Systems

Technical Publication Number: HE-TP-2011-001-1

heroengineering
valued solutions

Contents

Tables

1 Introduction

1.1 Hero Engineering and its personnel have been involved in control and safety system design, deployment and maintenance since before the company's inception in 2006. This involvement has included projects outside of the mining sector in both the manufacturing sectors and oil and gas sectors. The involvement includes safety system design and implementation within the AS/IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" framework. AS/IEC 61508 is a standard in which several Hero Engineering staff have gained certification under the Internationally recognised German TUV Rhineland FSEng (Functional Safety Engineer) system.

1.2 Most recently this experience and skill set has been utilised in several underground mine shaft sinking projects. These projects have required compliance with the AS/IEC 61508 standards. Hero Engineering does not claim an extensive history with winding systems and as such has approached the subject from fundamental aspects. We have reviewed the history of winders, the existing legislation, the existing guidelines and the proposed guidelines.

1.3 Fundamental to this is a number of general issues with the basic use of these standards. This document is part 1 of 2 and is intended to highlight some of the ongoing issues with the standards. The second document is intended to be more specific the current discussion of the proposed winder guidelines.

1.4 Although this document was prepared for discussion for the draft guidelines for underground winding systems, this document is not restricted in use for discussion in the development of other guidelines including sectors other than mining. In particular are the "lifecycle" management issues with AS/IEC 61508, which if to be solved, must include not only other engineering disciplines but also non-engineering services and personnel as well.

2 What is AS/IEC 61508

2.1 AS 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" is a general standard developed by the International Electrotechnical Commission (IEC) as a means of standardising the classification of, design of, maintenance of and components used in electrical/ electronic/programmable electronic safety-related systems.

2.2 Unlike previous systems it included concepts such as:

- The way components and systems fail; and,
- That not all components of the same type have the same reliability; and,
- The management of safety systems; and,
- The safety required by different industries would need additional and specific standards.

2.3 This standard was intended as a general standard covering any general application. The intention was that for specific industries other standards based on IEC 61508 would be developed, which has happened in for the process industry, machinery and other areas (see Table 1 below). The standard is sometimes referred to as an umbrella standard with the other

standards underneath the 61508 standard. As such in this and other documents when refereeing to AS/IEC 61508 the reader may imply this as a reference to other standards.

2.4 Table 1 is not all inclusive and only includes those current standards produced by the IEC. There are other functional safety standards not listed, readers are encouraged and advised to look for and search for standards as may be applicable to their needs.

Table 1. IEC 61508 Related Standards

AS/IEC Number	Title	Industry or Application
61511	Functional safety – Safety Instrumented systems for the process industry sector (note: 3 parts)	Process Industry
62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems	Machinery
61513	Nuclear Power plants – Instrumentation and control systems important to safety – General requirements for systems	Nuclear Instrumentation
62304	Medical device software - Software life cycle processes	Medical Software
61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (note: is part of a larger standard)	Variable Speed Drives

Note: AS/IEC 62061 has an equivalent ISO Standard 13849 Safety of machinery – Safety-related parts of control systems.

3 AS/IEC 61508 Fundamental Issues

3.1 AS/IEC 61508 has a number of current issues that make general application of the standard problematic. This does not make the standard unusable or irrelevant or too difficult to apply.

3.2 The cornerstones of the “functional safety” issues are essentially time and education. AS/IEC 61508 is little more than a decade old. Compared to other engineering disciplines such as civil engineering mining which is thousands of years old and compared to hazardous area engineering which has foundations going back over a century in coal mining functional safety is still in its infancy.

3.2.1 Significantly, apart from a few commercial training and certification courses there are no equivalent education and certification courses for technicians as there are for hazardous areas and high voltages.

3.3 A secondary effect of this is that as engineers outside of control and safety system engineering in general have little understanding of these standards. Tertiary to that is those outside engineering effectively have no knowledge at all of these standards. The consequence of this is that the non-engineering safety personnel who control the safety regimes on mine sites have no knowledge if the plant and machinery actually meet any safety standards. There exists a separation of safety control, which is not uncommon in many industries.

A key aspect for all industries will be for the safety engineering personnel to include other disciplines in the AS/IEC61508 process. In particular this will apply to non-engineering personnel in the management of functional safety.

3.4 These issues will be discussed in more detail in later sections of this document.

4 IEC 61508 Guidelines from other Sources

Prior to discussing the AS/IEC 61508 issues Hero Engineering will bring to note 2 Norwegian guidelines which have proven useful.

4.1 In other areas outside the mining sector where Hero Engineering operates and there are IEC 61508 guidelines with significant history and are further developed than exist for the mining sector. This is not detraction on the mining industry or other sectors. As a simple consequence of what incidents other sectors have faced, those sectors or industries are simply further ahead in the development of guidelines. As such it is prudent to learn from and use the experience available.

4.2 The Piper Alpha accident in the North Sea resulted in may recommendations amongst which the Norwegian authorities produced the OLF 070 “Application of IEC 61508 and 61511 in the Norwegian Petroleum Industry“.

4.3 Where this guideline fundamentally differs from other guidelines is in its approach and justification. OLF 070 does not simply list the fundamental safety functions as occur in the petroleum industry and provide minimum SIL ratings for such functions.

4.4 It first explains the standards and the management and system validation requirements. Then it explains the system development requirements. The actual minimum function requirements are a subsection of this (section 7.6). Rather than provide an inflexible system it then provides a mechanism (section 7.7) for the re-assessment of safety functions, such that where it can be engineered functions do not need to meet the minimum requirements as described.

4.5 Hero Engineering has recently seen this exercised where an FPSO low pressure flare knock out drum high fluid level safety function was through assessment re-evaluated from the OLF 070 table 7.1 requirement of SIL 3 down to SIL 2. No safety was compromised, sound engineering principles were exercised and the guidelines were met. There was full disclosure in a report justifying the lower SIL requirement.

4.6 OLF 070 goes on to cover design, installation, mechanical completion, system validation and then operational management. This includes guidelines for the management of change (MOC).

4.7 Most importantly OLF 070 dedicates a significant amount (two-thirds) of its time in justifying its requirements and providing practical guidance on each of the functions types its deals with. This includes practical examples of the use of reliability data in determining the characteristics of a deployed system.

4.8 Further to OLF 070, the Norwegian SINTEF organisation produced a report on the post deployment management of IEC 61508 systems. This report “SINTEF A8788 Guidelines for follow-up of Safety Instrumented Systems (SI) in the operating phase” is to date one of the few guidelines of its type that addresses the ongoing management of functional safety. This is irrespective of industry type or nationality.

4.9 The value of this document cannot be underestimated by both engineers and non-engineers as in particular it highlights the level of organised management required. The list of participants in the development of this guideline gives enormous credence to the guideline. This guideline

includes advice on documentation control, procedural control and competence management. There are some significant technical aspects to this guideline, which non-engineering personnel will generally avoid, but the structures it advises are something they should be involved with.

5 Discussions of AS/IEC 61508 Issues

The following sections are primarily based the experiences related to and experienced by the authors with respect to the issues they have faced with the application of functional safety standards not only in mining, but also in manufacturing and the petroleum industries.

5.1 61508 Infancy issues

5.1.1 In engineering terms, Functional Safety, as a specific engineering discipline may well be regarded as still in its infancy. Compared to other engineering disciplines it is very young. Civil Engineering with road works, plumbing, bridge building etc. has been practiced for several thousand years. Metallurgy and alloying has been practiced for centuries. Hazardous Area techniques have been in practice for over a hundred years and standardised for many decades.

5.1.2 In terms of hazardous area component certification there is an international system the IECEx system, which is established and accepted, as are the standards that system is based on. In Australia there is a nationally accredited system administered through the TAFE system of education of both engineers and technicians.

5.1.3 In terms of some engineering disciplines there are legal requirements for the persons involved such as structural engineering and electrical installation.

- Functional safety has no International system for component certification.
- Apart from short courses offered by various companies and organisations there appears to no basic education at the university degree level for engineers in functional safety.
- There are no equivalent training courses and qualifications for technicians for safety related installation, testing or maintenance as there are for hazardous areas and high voltage.
- There are no legal requirements yet for the qualifications for those who design or modify safety systems.
- Excepting specific applications, such as winders, there are few (as mostly vague) legal requirements for safety related systems on industrial plant and machinery.
- Accepting the efforts some industries there is a general lack of reliable safety related data.

The future success of functional safety as an engineering discipline will depend on numerous factors all happening in a cohesive planned structure that includes education, legislation and guidelines. For that to occur, cooperation of government, industry management (non-engineering), the tertiary education system and engineers will have to work together.

5.2 AS/IEC 61508 Management Issues

5.2.1 AS/IEC 61508 as an engineering concept is holistic in nature; terms such as “life cycle” and “periodic proof testing” and similar are often discussed. Less discussed are the management issues and combined with the separation between engineering and non-engineering there is a significant support issue. If engineering personnel do not garner the

support of non-engineering resources in assisting in the management of the safety systems there maintain they can only expect to fail in that maintenance.

5.2.2 The non-engineering personnel generally include those with general “slip, trip and fall”, personnel protection equipment (PPE) and safety induction interests. As these personnel often have a significant effect on any industrial site’s safety environment, systems and practice, having such people remain ignorant of engineering safety standards like AS/IEC 61508 can leave any mine site with serious unknown issues.

5.2.3 This in fact should not be the case, AS/IEC 61508 contains within its management structure some basic requirements where the inclusion of non-engineering safety personnel can play a significant and vital role.

5.2.4 Engineers by their nature and work regimes can be very organised in technical activities and extremely unorganised in non-technical activities. This cannot happen in the AS/IEC 61508 framework where record keeping, document control, management of change, and other aspects are vital to the maintenance of these safety systems.

5.2.5 Section 4 of A8788 details many of the activities that require organisation in the operation of AS/IEC 61508 systems. It is the organisational support where non-engineering personnel are required. The technical aspects of these activities do not need to be understood, but getting these activities done on time and as per procedure and by people with the right training and competencies is vital, and engineers will benefit from the right support.

As such the future inclusion of non-engineering personnel into the AS/IEC 61508 management structure should not be seen by engineers as an intrusion into their operations. It should be seen as a vital, if not essential support service. The task facing safety engineers is the education they must provide to other engineers and non-engineering personnel such that those services are provided successfully.

5.3 AS/IEC 61508 Security Issues

5.3.1 Along with (and possibly part of) the management support required is the future security issue for AS/IEC 61508. Not only are there backup version control issues there are the cyber issues. The STRUXNET virus (described as the world’s first cyber-weapon) proved beyond doubt that software based control systems can be attacked and safety breached. As safety systems move more towards programmable safety control, there is an ever increasing reliability on portable and fixed computers (engineering stations) to support those systems. STRUXNET attacked via the engineering support software located on standard personal computers as used by engineers.

5.3.2 Protecting the support and engineering systems for AS/IEC 61508 is a vital part of maintaining plant and machinery safety. Information technology (IT) in most industries is not seen by engineers as part of engineering it is seen as something external to their operations. In AS/IEC 61508 the separation of safety control from basic control is often carried into the engineering support. In many cases the computers from which safety systems are supported are design and planned to operate in isolation from other systems. There is no intent to have such computers linked in any way to local or plant wide networks.

5.3.3 IT personnel have a tendency to treat all computers on any site in any industry as their territory and their responsibility. Safety engineers express this vulnerability with phrases such as

"the greatest threat to safety is an IT person with a spare patch lead". Amongst the safety engineering community there are often discussions about experiences of engineering stations and laptops being "updated" or linked into local networks without their knowledge.

This is an area of vulnerability where safety engineers will best be served by a management system based on inclusion (see 5.2 above).

5.4 AS/IEC 61508 Failure Concepts

5.4.1 This is a key area where safety engineers can often be at cross or opposite purposes with all other engineering and non-engineering disciplines.

> ***A key concept in functional safety is that "given time any and all components and systems shall fail".***

5.4.2 In general everyone else (management, engineering, maintenance) are concerned with making something work or keeping it working, an AS/IEC 61508 safety engineer is primarily concerned when things don't' work. In general, with the exception of maintenance, when a plant or machine is commissioned an engineer's job is over. An AS/IEC 61508 engineer's job is over when the plant or machine is decommissioned. This is often referred to as the "61508 lifecycle".

5.4.3 As such, an AS/IEC 61508 engineer is in general involved in the design of opposite or reverses logic systems. For example - a regular engineer would monitor the normally open contact on motor contactor to see if the motor gets switched on and consider it a failure if it doesn't switch on. A safety engineer is concerned with the normally closed contact and considers it a failure if the motor does not switch off. A safety engineer is only concerned with bring equipment to a safe state. Making equipment work is either another task, sometimes an interlinked task and sometimes irrelevant.

5.4.4 Added to this is that AS/IEC 61508 considers that any component or system can fail either dangerously or safely and that failures are either detectable or not. In AS/IEC61508 this is expressed by the safety parameter - Safe Failure Fraction (SFF), and is a percentage of the failures of a component or system that are either safe or detectable. There is also a second parameter called Diagnostic Coverage (DC) which is the percentage dangerous failures that are detectable.

Engineering is about making plant and machinery work. Safety engineering is about making plant and machinery safe. These are not the same thing.

5.5 AS/IEC 61508 Common Misunderstandings

5.5.1 Prior to the acceptance of AS/IEC 61508 the dominant concepts in both machinery and process safety were based on physical architecture and usually in terms of redundancy. Parts of AS 4204 "Safety of Machinery" were and still are based on the European standard EN 954 "Safety- related parts of control systems".

5.5.2 The EN 954 system categorised safety primarily on architecture the lower categories are single channel the upper categories are redundant. In the process industry safety systems became dominated by the TMR concept. TMR triple mode redundancy basically performed critical safety functions with 3 of everything. 3 sensors, 3 processors and 3 output devices. Some of the early programmable safety controllers for machinery also followed the TMR concept.

5.5.3 From this there have been basic misunderstanding that in the AS/IEC 61508 frame work:

- SIL 1 means 1 of; and,
- SIL 2 means 2 of; and,
- SIL 3 means 3 of.

5.5.4 The acronym SIL stands for Safety Integrity Level it is a measure of probability that a safety function will do as expected. There are in actuality 4 SIL levels defined in 2 sets for 2 types of demand (see Table 2 below). The standard safety integrity as the "probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. Demand in this context is a measure of how often the safety system or function is called upon.

Table 2. AS/IEC 61508 SIL Levels

SIL Level	Low Demand Mode Average probability to fail on demand (PFD_{AVG})	High Demand Mode Probability of a dangerous failure per hour (PDF_{HR})
1	>= 10^{-2} to < 10^{-1}	>= 10^{-6} to < 10^{-5}
2	>= 10^{-3} to < 10^{-2}	>= 10^{-7} to < 10^{-6}
3	>= 10^{-4} to < 10^{-3}	>= 10^{-8} to < 10^{-7}
4	>= 10^{-4} to < 10^{-5}	>= 10^{-9} to < 10^{-8}

Note: Table 2is taken from tables 2 and 3 AS 61508.1-1999 (IEC61508.1-1998)

5.5.5 The SIL level required by a system is not equal to the number of independent or backup channels or a description of redundancy. In AS/IEC 61508 systems redundancy is referred to as Hardware Fault Tolerance (HFT) and ranges from 0 to 2. HFT is the number of faults the function or system can tolerate before the function may not be able to operate.

5.5.6 Table 3 below shows the HFT for type A and B subsystems, which are distinguished by what can be determined about a sub-system's failure modes and fault behaviour under fault conditions. Type A are well defined and Type B less defined. For winders an example of a type A device would be the emergency stop button on the winder drivers control console, when all parts of the button and contacts are suited to use in AS/IEC 61508 applications. Things like a Lilly controller would be Type B systems for several reasons as described in the standard.

Table 3. AS/IEC 61508 Hardware Fault Tolerances

Safe Failure Fraction	Type A Safety-related Subsystems			Type B Safety-related Subsystems		
	Hardware Fault Tolerance			Hardware Fault Tolerance		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	Not Allowed	SIL 1	SIL 2
60% - <90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Note: Table 3 is taken from tables 2 and 3 AS 61508.2-2001 (IEC61508.1-2000)

5.5.7 What Table 3 shows is that unlike previous standards where the design architecture and redundancy requirements were set by the function classification alone in AS/IEC 61508 these requirements are a combination of the function classification and the capabilities of the components used. This is because previous systems did not consider the reliability of components. A weakness of previous systems was that the quality and reliability of components

was not considered. As such systems with identical architecture would have the same ratings irrespective of whether the components used were of equal quality. Previous systems relied on fault detection and did not include allowances for differences in undetectable dangerous failures.

5.5.8 In particular the AS/IEC 61508 system considers how components behave when they fail. It accepts that not all failures are detectable and that there exists for any system failures that can be both dangerous and undetectable.

5.6 AS/IEC 61508 Safety Related Data

5.6.1 Of all the issues facing the application of AS/IEC 61508 systems safety related data is the not only the most significant it is at times the most misunderstood and misused.

5.6.2 Prior to AS/IEC 61508 systems such as that described in EN 954 and sued in AS 4024 were based on the weakest link principle. The rating of the weakest link was the rating of the system or function. It did not matter what the rating of the input device(s) or logic solver or output device(s) were, which ever had the lowest category rating dictated the system rating.

5.6.3 This made rating such systems relative easy but has however caused issues in the application of AS/IEC 61508. For example, previously the combination of a category 2 input a category 2 logic solver and category 2 output made for a category 2 system. In AS/IEC 61508 systems the combination of a SIL 2 input a SIL 2 logic solver and SIL 2 output ***does not necessarily make a SIL 2 safety function or SIL 2 system***.

This is because AS/IEC 61508 takes into account the functional behaviour of the components and system in combination. Hence the term functional safety.

5.6.4 A particular misconception is the certification of AS/IEC 61508 components. Aside from there being no single system or a system such as the IECEx system that exists for hazardous area applications, there exist misconceptions over what is a certified safety product. ***In real terms there is in fact no such thing as a SIL rated device. There are devices rated for use in SIL rated applications***. This is because, as mentioned previously, SIL rating is a holistic rating of either a function or a system. This may appear as a slight play on terminology but is an important concept. AS/IEC 61508 is holistic in nature and this is carried through in use of safety related data.

A device suitable for use in an AS/IEC 61508 system is one where the data for determining the SIL rating of the system or function is available.

Devices with certification are those which have been tested or assessed by a certification authority or organisation and the safety related data determined and described for use, which may include limits on use.

5.6.5 One serious issue with the use of basic data is its relevance to the actual field experience. As previously discussed management is important and an aspect of this is the collection of data. The aforementioned A8788 guideline provides guidance on the re-evaluation of safety related data. The highly regarded text by David J Smith “Functional Safety – A Straightforward Guide to applying IEC 61508 and related standards” separates data into site specific, industry specific and generic data. In section 7.3 of this text the concept of confidence levels in these data types is discussed. In previous searches by hero Engineering only 1 other such study in the relevance of safety related data was found and that was only in reference to a study in the British Nuclear industry – the actual report was unavailable.

5.6.6 What the Smith text highlights is actually part of the previously discussed management of functional safety. Functional safety management includes the collection of and use of failure data.

Without the assistance of others such as maintenance personnel accurate data cannot happen successfully.

Without the assistance of other non-engineering management personnel the security and retention of the data cannot be guaranteed.

Without senior management realising the importance of safety related data collection and keeping and ongoing re-assessment processes. The safety of personnel they are responsible for may not be what they expect or believe it to be.

5.6.7 A difficult aspect of applying standards such as AS/IEC 61508 to winders is that the variety of winders is immense and varied. In recent projects Hero Engineering has dealt with winders ranging in power from 15kW to over 2000kW and design speeds from below 0.5m/s to over 10m/s. The configurations include synchronised winders, electro-mechanical-clutched drivetrains and electro-hydraulic transmissions.

5.6.8 When compared to other AS/IEC 61508 guidelines in other industries what is missing is a fundamental system where given basic winder engineering parameters are used to classify the requirements. This is not unprecedented as AS 4343 Pressure Equipment – Hazard Levels uses simple engineering values such as volume, pressure and fluid type to classify pressure vessels, vacuum vessels, boilers and pressure piping – (see AS 4343 Table 1). The basic set of winder safety functions are well established, what is not as clear is what any given winder might or might not require.

6 Conclusions and Recommendations

6.1 Although complex and still in its infancy AS/IEC 61508 and its related standards are the way forward for not only the Australian Mining Sectors but for other sectors as well.

- The tested and certified components for use in safety systems worldwide are following this system. Any other system would or could lead to engineers being unable to use components with any degree of certainty.
- There exist well developed guidelines from other industries and nations which have been developed that can provide the basis for all Australian Industries developing similar and consistent guidelines.

6.2 There must be further development of education not only for engineers practicing standards such as AS/IEC 61508 but other engineers whose work runs alongside these systems. One or more of the internationally recognised certification programs for engineers must become formally recognised in legislation to bring safety systems implementation in line with similar engineering practice such as exists for structural engineering.

6.3 There must be further education development and qualifications for non-engineering management support of engineers practising AS/IEC 61508 and related standards.

6.4 There must be training and qualifications developed for technical support staff to bring safety related systems into line with other practices such as hazardous areas and high voltages.