NOPSA

Technical Safety Bulletin:

FUNCTIONAL SAFETY IN THE AUSTRALIAN OFFSHORE PETROLEUM INDUSTRY

National Offshore Petroleum Safety Authority

Independent and professional regulators of Australian offshore petroleum health and safety

nopsa.gov.au

March 2011

FUNCTIONAL SAFETY IN THE AUSTRALIAN OFFSHORE PETROLEUM INDUSTRY

Following a number of issues where the use of control systems containing programmable devices or software was identified as a possible cause of a dangerous event, NOPSA published **Safety Alert 45** outlining the issue and giving preliminary advice to Operators on a way forward.

This technical bulletin is intended as a more detailed supplement to Safety Alert 45, offering more in-depth analysis of the issues and legal duties imposed by the *Offshore Petroleum and Greenhouse Gas Storage Act 2006*. This document provides duty holders with guidance on possible methods for reducing risks from functional safety issues to as low as is reasonably practicable (ALARP).

INTRODUCTION

This section introduces some key concepts that support understanding of how functional safety relates to the occupational health and safety regulations in the Australian offshore petroleum industry.

What is functional safety?

While some hazards are created by the physical implementation of control systems, such as noise and high-pressure fluid in hydraulic systems, or electric shocks from relay logic, instances of harm from these sources are comparatively rare.

Control systems implemented in software are 'virtual' in that they usually consist of a series of magnetic signals, and cannot directly cause physical harm.

Control systems can cause harm when they fail to carry out their function correctly, such as:

- an unsolicited movement of a crane hook could cause a dogman to be crushed by a heavy load;
- the failure of a dynamic positioning system could lead to a diving support vessel dragging a diver into a hazardous situation; or
- the failure of a pressure sensor or logic solver could cause a hydrocarbon leak due to an overpressure in a pipe, leading to a burst.

Functional safety is sometimes described as relating to the failure of a control system to operate reliably. There have, however, been incidents where a system component has operated correctly, and in accordance with its design intent, but with unintended consequences. The failure in such cases is in the design and implementation process rather than being a matter of unreliability in the control system itself, which could theoretically produce hazardous outputs with high degrees of reliability.

The IEC standard 61508-0[(1)] avoids this issue by defining functional safety as, "part of the overall safety that depends on a system or equipment operating correctly in response to its inputs."

This leads to a further definition of a safety-related control system as one which is able to cause a hazard if it does not respond to its inputs correctly.

These two definitions highlight why it is so important to identify all hazards associated with the control system: without doing a thorough job of hazard analysis, it is impossible to correctly specify the correct system response.

Programmable systems

Software is increasingly being used in safety-related applications ranging from smart instrumentation to programmable logic controllers. Active, computer-based safety management systems are being employed for such significant applications as electronic permit-to-work packages.

Software's unique inherent properties require approaches and treatments quite different from traditional engineering activities such as mechanical or structural engineering.

The UK's Health and Safety Commission 1998 report, *The use of computers in safety-critical applications*, describes the issue as "the essentially discontinuous behaviour of discrete logic, and in particular of software." [2]

Control systems process inputs to produce desired outputs. The nature of software is such that, if a system gives a correct output for a given input, it cannot be assumed that even a slightly different input will also give a satisfactory result.

Since testing every possible combination of inputs to ensure none will produce a hazardous set of outputs is unviable, steps need to be taken to mitigate the risks involved.

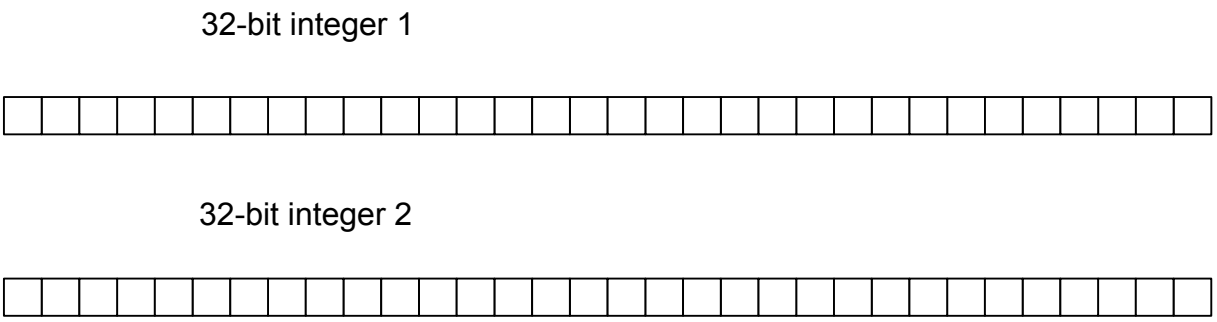

Figure 1 – a simple software operation

Consider Figure 1, which shows a simple example based on a 32-bit microprocessor programmed to add two numbers represented as strings of 32-bit binary digits. The total possible number of input combinations is 2^{64}.

If one million combinations were tested every second, it would take over five hundred thousand years to test them all. For very complex systems involving a typical processor running an operating system and several programme packages, the inherent complexity renders exhaustive software testing effectively impossible.

Software, therefore, cannot be tested in the same way as, say, a mechanical or structural system. If a bridge can safely take a ten-tonne load, then it can usually be assumed that a lighter load will be acceptable. In software, the concept of a 'lighter load' does not exist.

Similarly, if a mechanical component in a machine fails, replacing it with a stronger, but otherwise identical component allows a claim to be made that the machine will be at least as reliable as it was beforehand. The same cannot be said of software, and there are numerous cases of additional bugs being introduced as a result of attempts to correct previously identified programming errors.

If the corruption by means of computer virus, voltage spike, or powerful radiation, is ignored, software, unlike mechanical components, does not suffer from degradation due to wear or stress. For this reason, all errors in software can reasonably be assumed to be design faults.

It is also for this reason that management of risks caused by software focus on the rigorous methodologies required to limit the number and consequence of design faults. This is discussed further in the section on standards.

Goal-setting regulation

The philosophy behind the safety regulation of the offshore petroleum industry in Australia highlights that those creating hazards are responsible for making sure the risk of harm from that hazard is as low as reasonably practicable (ALARP)[3]. This means that safety legislation does not set out a list of prescriptive measures for managing risk, but puts the onus on Operators to identify the best way of approaching risk reduction.

Following the July 1988 Piper Alpha disaster in the UK, the subsequent Cullen Public Inquiry report was clear that prescription stifled continuous improvement in safety and diverted responsibility from those who were creating the risk. It was also clear that those creating the risk were in the best position to fully understand it and therefore best placed to identify appropriate control measures.

Although there are no explicit regulations that point Operators towards designing, installing, testing, operating and maintaining control systems, they are significant issues and Australian law requires them to be properly managed in a goal-setting framework that reduces any residual risk to ALARP.

LEGAL DUTIES

This section looks at the relevant portions of the legislation that apply to functional safety in the offshore Australian petroleum industry.

In general terms, the law requires that any safety-related control system is designed, installed, tested, maintained and operated in such a way as to reduce risks to ALARP. As is often the case with goal-setting regulations most of these duties are general in nature; they do not have to specifically mention control systems for the law to apply, nor do they specify exactly what must be done to comply.

For this reason, the discussion is based on the duties of various parties specified in the regulations, and what this implies in terms of functional safety.

The word ‘plant’ in the regulations refers to any machinery, equipment tool or component, including software.

Operators

The overriding duty of Operators of offshore petroleum and greenhouse gas facilities is covered in Clause 9 of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006*.

Clause 9(1) is a general duty to take all reasonably practicable steps to ensure that the facility is safe, and that all work and other activities are carried out in a safe manner.

These general duties are supplemented by a number of specific duties including: Clause 9(2) (c), “to take all reasonably practicable steps to ensure that any plant, equipment… are safe”; 9(2) (e) “to take all reasonably practicable steps to implement and maintain appropriate procedures and equipment for the control of, and response to, emergencies at the facility.”

These duties imply that if control systems are used, then they must be designed in a way that will reduce risks to ALARP.

The duties apply to all safety-related control systems, the implication being that Operators should be aware which, if any, of their control systems are safety related and take all reasonably practicable steps to make them safe, including adequate testing and maintenance.

Persons in control of parts of a facility or particular work, and employers

As outlined in relevant sections of Clauses 10 and 11 of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006*, it is not only employers of people working on a facility who have very similar duties to Operators. Anyone given responsibility or control of a part of a facility, or of any particular work carried out at a facility, is subject to the same duties.

This extends the duty of care to include, among others, diving supervisors, contract labour, operators of remotely controlled vehicles, and those in control of mobile drill rigs located temporarily on fixed platforms.

Manufacturers

Clause 12(1) of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* is relevant to anyone who manufactures plant that they ought reasonably to expect will be used by members of the workforce of a facility. It would be applicable, for example, to developers of electronic permit-to-work systems as well as to manufacturers of automated pipe handling systems, gas detection and shutdown systems, and dynamic positioning systems.

The manufacturers' duties differ from those placed on Operators, employers and persons in control of parts of the facility or particular work in that it includes a requirement to carry out all reasonably practicable research and testing necessary to discover and eliminate or minimise any risk, and make the plant safe.

It also includes the duty to ensure that the plant is so designed and constructed as to be safe when properly used so far as is reasonably practicable. For manufacturers of plant, the functional safety aspects of this duty could relate to identifying possible methods of preventing the defeating of safety devices, such as interlocks, and that manufacturers should be clear as to what comprises the intended use of the plant they have manufactured.

Finally, the legal duty includes making available adequate written information about the use for which the plant has been designed and tested, details of its design and construction, and any conditions necessary to ensure that it will be safe when employed for its intended purpose (the use for which it was designed and tested).
This implies that manufacturers of plant should provide information on inspection, testing and maintenance and any other information necessary to meet the required legal duty.

Suppliers

Suppliers of plant are covered by Clause 13 of the *Offshore Petroleum and Greenhouse Gas Storage Act 20*06. This requires suppliers to ensure that, so far as is reasonably practicable, at the time of supply, the plant is in such condition as to be safe when properly used.

It also requires suppliers to ensure that research, testing and examination are done to discover, eliminate or minimise any risk to health or safety that may arise from the condition of the plant.

As for other duty holders, suppliers are obliged to make available adequate written or recorded information in connection with the use of the plant. This information includes:

- the condition of the plant at the time of supply;
- any risk posed to the health and safety of personnel at the facility from the condition of the plant and its usage; and
- the steps required in order to eliminate such risk.

Persons

Clause 15 of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* requires a worker at a facility to take all reasonably practicable steps to ensure that no act or omission creates a risk or increases an existing risk. Personnel are also duty-bound to cooperate with the facility Operator to meet obligations imposed on them. The requirement specifically directs anyone on a facility to use equipment "in accordance with any instructions given by the equipment supplier, consistent with the safe and proper use of the equipment."

These obligations would be relevant in cases where users of control systems deliberately defeat safety systems such a guard interlocks.

Functional safety in Safety Cases

As discussed in the introductory remarks about goal-setting legislation, it is open to Operators of facilities to specify the standards they use when reducing risks to ALARP.

Regulation 2.7 of *the Offshore Petroleum (Safety) Regulations 2009* requires Operators to specify in their Safety Case "all Australian and international standards that have been applied or will be applied in relation to the facility or plant used on the facility".

This implies that the standards used in the design, testing, operation and maintenance of control systems must be included in the Safety Case for any facility that has safety-related control systems.

Control systems are specifically mentioned in Regulation 2.19 of *the Offshore Petroleum (Safety) Regulations 2009*.

This regulation sets out a requirement on Operators to ensure that the Safety Case contains "adequate provision for the facility, in the event of an emergency, in respect of: back-up power supply, lighting, alarm systems, ballast control and emergency shut-down systems."

Before an Operator can submit a Safety Case, a scope of validation may be agreed upon with NOPSA. Validation activities may include functional safety aspects.

AS LOW AS REASONABLY PRACTICABLE (ALARP)

The preceding sections contain references to the phrases ‘so far as is reasonably practicable’ and ‘as low as reasonably practicable’. This is legal recognition that it is not always possible to completely eliminate risk. A balanced decision needs to be made to determine the amount of sacrifice needed in terms of time, resources and funding that it is reasonable to commit to achieve a given amount of risk reduction.

If risks have been reduced so far as is reasonably practicable, then the residual risk is said to be as low as reasonably practicable, usually referred to by the acronym ALARP.

This section attempts to tie up the various themes covered in previous paragraphs by giving guidance on how to approach the concept of functional safety in control systems to ensure that all risks associated with their use are ALARP.

The need for demonstration

As has been noted above, Operators are expected to detail in their Safety Cases that adequate provision has been made with respect to shut-down systems. Operators should also be in a position to demonstrate that they have done everything required to reduce risks from all hazards to ALARP.

It is possible that NOSPA inspectors will also ask for adequate demonstration that control system and functional safety have been addressed on facilities, either during an inspection, or as a part of the validation process relating to Safety Case submissions.

The role of standards

The introductory text in most Australian standards describes them as ‘living documents which reflect progress in science, technology and systems’. Standards therefore form a useful reference source when identifying benchmarks for good practice, and in determining what is reasonably practicable.

Historically, there has been a slight difference in approach between standards aimed at machinery safety, which tend to use qualitative, risk-graph approaches, and those originating in the process industries that have traditionally favoured the use of quantitative approaches and Safety Integrity Levels (SILs).

It is generally recognised that the risk-graph approach, while fine for simple components, does not deal adequately with programmable systems and components. ISO 13849-2:2003 states, for example, “this…standard does not give complete validation requirements for programmable electronic systems and therefore can require the use of other standards.”

The gap between these two approaches is narrowing with the publication of standards that deal with the inclusion of software-based systems. This convergence is illustrated in Figure 2, taken from AS 62061, which shows the interrelationships between various international standards relating to the functional safety of machinery.

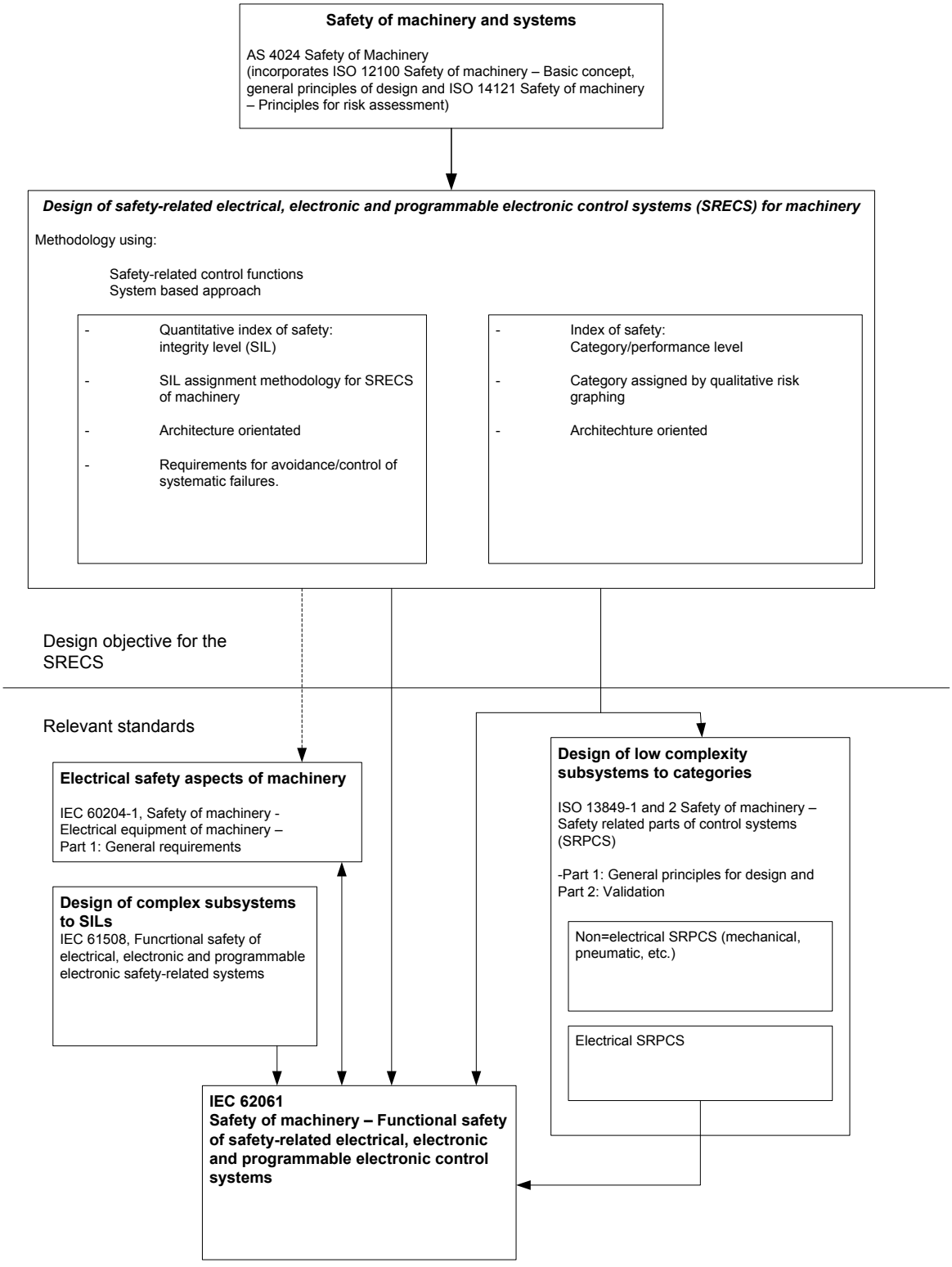

Figure 2 – Interrelationship between AS4024, AS 62061 & ISO 13849

It is up to the Operator to select appropriate standards, and make an assessment as to whether or not following a particular standard will result in a particular control measure being ALARP.

Current international standards on functional safety are based on the hazard identification and risk assessment approach to designing for safety, and are clear in their requirements for a methodical approach that limits to ALARP the possibility for systemic failures.

These standards clearly define the types of documentation required to assist in the design process, thus facilitating the legal obligations of duty holders to provide adequate information and enabling them to make valuable demonstrations when developing Safety Cases.

These standards incorporate guidance on validation, verification and ongoing testing requirements of control systems that all contribute to meeting various legal requirements.

There are, of course, other sources of guidance than standards, such as *The Engineering Equipment and Materials Users' Association's (EEMUA) Publication* 222[(4)].

	Duty holder			
	Operator	Person in control	Supplier	Manufacturer
Process Safety				
AS 61508 series #	X		X	X
EEMUA Publication 222	X		X	
Machinery Safety				
AS62061 Safety of machinery * #	X	X	X	X
ISO 13849 *	X	X	X	X
AS 4024.1-2006 Series : Safety of machinery^	X	X	X	X
Bespoke systems (such as custom-coded software systems)				
AS 61508 series #			X	X

Notes

These standards including, AS IEC 61511-2004 : Functional safety - Safety instrumented systems for the process industry sector, are derived from AS 61508, and share a common methodology.

***** see diagram 1 for inter-relationship.

^ A useful reference for 'traditional' machinery type standards.

Table 2 – Typical functional safety standards and their relevance to duty holders under the regulations.

Any other equally effective means

Although the standards and approaches described in this document are acknowledged as authoritative sources of good practice by industry practitioners, they are recommendations only, and are not to be considered mandatory.

One of the greatest strengths of goal-setting legislation is that it allows innovation in risk reduction. It is open to all duty holders to investigate different approaches to managing functional safety from those outlined in this paper, provided they can demonstrate that the alternative solution is at least equally as effective.

REFERENCES

(1) – Available in Australia as AS 61508.0-2006: Functional safety of electrical/electronic/programmable electronic safety-related systems - Functional safety and AS 61508. Online overview can be found at: **http://www.iec.ch/functionalsafety/**

(2) – The use of computers in safety-critical applications, the final report of the study group on the safety of operational computer systems. HSE Books.
ISBN 9780717616206.
http://books.hse.gov.uk/hse/public/saleproduct.jsf?catalogueCode=9780717616206

(3) – **http://www.nopsa.gov.au/document/Leaflet%20-%20Prescriptions%20and%20Standards.pdf%20%20**

(4) – The Engineering Equipment and Materials Users' Association (EEMUA) Publication 222 - Guide to the Application of IEC 61511 to safety instrumented systems in the UK process industries. ISBN 0 85931 168 6. **www.eemua.org.**