CONSIDERATIONS FOR FUNCTIONAL SAFETY WHEN A MACHINE IS LINKED TO A PROCESS

There is frequently a need to fit machinery into a process environment (e.g. an agitator in a tank). The machine should have been constructed in accordance with IEC 62061 or ISO 13849 but it may have to interface with and have an impact on a safety system designed to IEC 61511 & IEC 61508. The process in which the machine is installed may also have an impact on the safety requirements for the machine that could not have been anticipated by the machine builder.

In the UK operating sites and machine manufacturers are subject to the ***Management of Health and Safety at Work Act 1999***. In principle this requires the site operator or duty holder to reduce the risk to ***As Low As Reasonably Practical (ALARP)***. To meet this objective the site operator (End User), must ensure that any machine to be utilised within a process has been fully specified in terms of its operating environment and the functionality of the machine within the process.

Examples of machinery: Gas Turbine, Screw Conveyor, Elevator, Agitator.

What are the problems?

What should the Functional Safety Engineer be aware of?

What are the solutions?

DISCLAIMER

[1] *The Association would welcome any comments on this publication, see http://www.61508.org/contact.htm. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.*

[2] These guidelines have been produced by The 61508 Association to assist its members and others to consider how to deal with combined BPSC and SIS systems. *The Association would welcome any comments on this publication, sent to legacy@61508.org. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.*

Contents

Revision History

Version	Date	Author	Comments
V1.0	xx/03/2015	PB	Draft release for review by 61508 Association
V1.1	10/06/2015	CJH/RS/PB	CJH peer review and update
V1.2	11/12/2015	PB	Update for ISO 13849-1 amendment
V1.3	19.05.2016	JT	New T6A Logo added and WG references deleted

1 Introduction

The UK operating sites and the machine manufacturer are subject to the ***Health and Safety at Work etc Act 1974*** which places a duty on '*...any person who designs, manufactures, imports or supplies any article for use at work...to ensure, so far as is reasonably practicable, that the article is so designed and constructed that it will be safe and without risks to health...*'.

The UK operating sites and the machine manufacturer are subject to the ***Management of Health and Safety at Work Act 1999*** which requires a suitable and sufficient risk assessment of

(a) *the risks to health and safety of his employees to which they are exposed whilst they are at work; and*
(b) *the risks to the health and safety of persons not in his employment arising out of or in connection with the conduct by him of his undertaking.*

As well as complying with section 6 of the Health and Safety at Work etc Act 1974, the machine builder is legally obliged to follow the requirements of the ***Machinery Directive*** (and other directives) or, in the UK, ***The Supply of Machinery (Safety) Regulations*** namely:

- the machinery must meet all relevant ***Essential Health and Safety Requirements*** (EHSRs);
- the machine builder must draw up a ***Technical File***;
- the machinery is issued with a ***Declaration of Conformity*** (DoC);
- the machine builder affixes a ***CE mark*** to the machine.

Before placing the machinery/process system assembly into beneficial use, the end user must carry out an assessment for worker protection, in the UK this is implemented by the ***Provision and Use of Work Equipment Regulations*** (PUWER) and implemented in the EU by the ***Use of Work Equipment Directive*** (2009/104/EC).

The ***Official Journal of the European Union*** lists the harmonised standards for the European product safety directives (e.g. the Machinery Directive). Although there use remains voluntary if a harmonised standard is followed fully by the product designer it can confer a presumption of conformity for one or more Essential Health and Safety Requirements (EHSRs).

The use of harmonised standards therefore can save designers much time in assessing risks and adopting strategies for safety particularly where the harmonised standard covers all the essential requirements for a particular product. IEC 62061 and ISO 13849 are harmonised in the Official Journal of the European Union. Machine type specific or type 'C' harmonized standards considering multiple aspects of machine safety, referencing IEC 62061 and/or ISO 13849, also exist to support the machine builder.

IEC 61511 is recognised and adopted across the process industry for functional safety and has been identified as good practice by the UK Health and Safety Executive (HSE). *The Dangerous Substances and Explosives Atmospheres Regulations* (DSEAR) Approved Code of Practice (ACoP) suggests the use of IEC 61508 / IEC 61511 for the process industry.

It is not unusual for the engineering team of the process plant to be inexperienced in the subject of machine safety and functional safety for machinery. Conversely it is also not unusual for the machine builders engineering team to be inexperienced in the matters of process safety and functional safety for the process industry. Functional Safety for all sectors is reliant on some form of hazard analysis and risk assessment which drives the functional safety requirements. There are however significant

differences in risk assessment and how they define the safety integrity of a system for machinery in relation to the process industry. This report aims to improve the understanding of functional safety on both sides of this intersection.

2 Scope

This document is an introduction to the issues of Functional Safety for when machinery interacts with a process plant. The aim of the document is to introduce the world of functional safety for process to the machine builder and to introduce the world of functional safety for machinery to the site operator and therefore is not a detailed analysis or comparison of IEC 61511, IEC 62061 and ISO 13849. The suitable Functional Safety standard must be followed in full to provide a functionally safe system for the equipment under control which is a topic outside the scope of this document. This document has three main objectives:

- To help engineers understand the issues for both machine and process related functional safety when machines are used as part of a process plant.
- To generate a guidance document that summarises the likely challenges and issues and offers practical advice, with supporting evidence, to find a solution.
- To consider some examples of when a machine interacts with a process to aid in the creation of this report, namely; If I fit an agitator within a tank in the middle of a process plant, that impacts the risk of the process what are the problems and solutions?; If I have a Dive Support Vessel (DSV) that has a Hyperbaric Monitoring and Control Systems to support the diving chamber complex (process) and launch and recovery systems to move the dive bells (machine), that impacts the risk of the process what are the problems and solutions?; If I have a energy from waste plant that must process the waste with machines before a process converts the processed material to energy, what is the impact on the risk from one part to the other and what are the challenges that must be faced when implementing the different functional safety standards.

The final outcome for any hazard is to show that the risk is ALARP. As the equipment under control could be from many different applications it is not possible to define ALARP that is common for all examples. It is however possible to discuss what would not be ALARP where possible.

3 Comparison of Functional Safety Standards

Why and how are IEC 61508, IEC 61511, IEC 62061 and ISO 13849 different?

The basic approach for tackling the hazards at hand is generally similar for all the functional safety standards discussed here. The idea is to identify the hazards / hazardous situations, then assess the risks they represent. The target is to remove, replace, or reduce and control the risk they represent by ‘good engineering design’ through either ‘layers of protection’ or a hierarchy of control. Some form of Hazard Analysis and Risk Assessment must be performed e.g. PHA, HAZID, HAZOP, ISO 12100.

IEC 62061 and ISO 13849 do not define the tolerable risk and these standards reference ISO 12100 which also references protective measures implemented by the end user. Type ‘C’, or machine type specific, harmonized standards support in the definition of tolerable risk but often the machine builder must produce more evidence that ALARP has been achieved.

IEC 61511 / IEC 61508 do not define tolerable risk. Tolerable risk for harm to people must be defined by the corporate body, it is up to the Duty Holder/End User/Operator to meet, AND the Duty Holder/End User/Operator must show that ALARP has been achieved.

The IEC standards have definitions for the terms 'Verification' and 'Validation' where as the ISO standard does not. ISO 13849 uses the term 'Verification' on a few occasions but mainly uses the term 'Validation' even where, in relation to the IEC standards, the term 'Verification' might seem to be more appropriate. ISO 13849-2 covers Validation in detail, for ISO 13849-1, which is a very important aspect of all functional safety standards. Even though the IEC and ISO standards define Verification and Validation slightly differently it is recommended to follow the IEC definitions, and the intent of all the standards discussed here, even when using the ISO machinery standard. After all one person's Verification activity is another person's part Validation. When the equipment under control contains both machinery and process plant then the functional safety will need Verification and Validation activities covering at least two of the standards e.g. IEC 62061 and IEC61511. These activities may need to be combined under the same planning and FSM systems.

The IEC standards cover 'Management of Functional Safety' (FSM) however the ISO standard does not use the term at all. The ISO standard is more prescriptive in its approach however Functional Safety Management (FSM) with planning is also recommended for meeting the requirements of the ISO standard. At the same time the ISO standard has numerous features, e.g. basic safety principles & well-tried safety principles, which should be inserted in any FSM system and safety plan. A combination of approaches then, especially for machinery, is recommended.

The ISO standard only refers to the term 'lifecycle' in relation to safety-related software and both the machinery standards, IEC 62061 and ISO 13849, have a limit in the lifecycle coverage up to the completion of Validation. Therefore, once a machine enters the operation phase, the coverage of IEC 62061 and ISO 13849 has ended. *The Supply of Machinery (Safety) Regulations* and *The Provision and Use of Work Equipment Regulations* (PUWER) cover safety of machinery from this point forward. As this legislation is in place it is recommended to apply the full lifecycle management approach to all functional safety aspects where possible.

The IEC 62061 approach to Management of Functional Safety is Safety Planning (ISO 13849 uses the term Validation Planning). It assumes that a machine is built by a single machine builder who is in control of the full picture. Often, with modern complex machinery / production lines, this is not the case and here an approach to Management of Functional Safety more similar to that of IEC 61508 & IEC 61511 would probably be more appropriate. For example, if a new production line is being installed that contains multiple machines from different suppliers and the integration/commissioning is to be done by a 3rd party system integrator (machine manufacturer). In this type of situation it is very important that someone takes overall responsibility for the FSM system and other safety aspects.

The option to use components or technology that is 'proven in use' is not available for the machinery standard IEC 62061 as all applications are deemed to be high demand or continuous mode of operation. IEC 62061 therefore states that equipment must conform to the relevant requirements of Route 1_H of IEC 61508-2:2010 section 7.4.4.2. ISO 13849 does not specifically exclude components or technology that is 'proven in use' however the requirements driven by the $MTTF_d$, DC, etc do typically exclude 'proven in use' as an option.

The architectures available for the machinery functional safety standards are limited and defined to a total of 4 architectures around the themes 1oo1 and 1oo2 where as the process industry functional safety standard, IEC 61511, does not have this type of limitation.

The IEC standards (IEC 61508, IEC 61511 and IEC 62061) use a similar definition '*failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel (redundant architecture) sub-system, leading to a failure of a SRCF/system failure*' for common cause failure (CCF) where as the ISO standard uses the definition '*failures of different items,*

resulting from a single event, where these failures are not consequences of each other'. Regardless of this difference in definition CCF is typically considered to be the same across all the standards considered here and it is recommended it is treated the same for machinery and process.

The various functional safety standards considered here have slight differences in the definition of diagnostic coverage (DC) however DC should be treated the same across all the functional safety standards. The ISO standard for machinery does however fail to make reference to automatic on-line testing or to exclude faults detected by proof testing.

The IEC standards (IEC 61508, IEC 61511 and IEC 62061) have a similar definition for safe failure fraction (SFF) however the ISO standard (ISO 13849) has no definition for SFF and SFF is not used within ISO 13849. ISO 13849 mainly relies on DC in this area. SFF is the fraction of the overall failure rate that does not result in a dangerous failure (i.e. safe failures & dangerous detected failures) where as the DC is the ratio of dangerous failures that can be detected.

The safety requirement specification (SRS) is similar for all the functional safety standards discussed within this document.

All the functional safety standards discussed in this document highly recommend separation of safety functions from non-safety functions. Many types of safety-related controller are available in the market place, some of which offer levels of physical separation and others which offer technical or logical methods of separation. The use of safety-related controls with technical or logical separation is readily accepted within the machinery sector. The process industry has other requirements, e.g. 24/7 operation and BPCS online changes, that must be considered when deciding on the separation methodology used. The 61508 Association has written a separate paper on this issue.

3.1 IEC 61508 has just been revised what is happening with IEC 62061?

IEC 62061 was amended in 2012 (as IEC 62061:2005+A1:2012) which has then been harmonized under the machinery directive at the end of 2013.

The amendment is more to bring the standard in line with other machinery safety standards than to bring the standard in line with IEC 61508 edition 2 however the updated definitions for low demand mode, high demand or continuous mode, probability of dangerous failure per hour, proof test, and diagnostic coverage have been included from IEC 61508-4 / ISO 12100.

A note supporting the estimation of Safe Failure Fraction (SFF) has also been added referencing sources of information.

Notes reinforcing the approach for machinery in relation to IEC 61508:2010 and Route 1_H and Route 2_H have been added in numerous areas. ISO 13849-1 is due an amendment that could result in changes than possibly impact the quality of the safety-related parts of the control system (SRP/CS). We recommend that current good functional safety practice is still followed even if the amendment to ISO 13849-1 lessens some requirements.

3.2 IEC 61508 has just been revised what is happening with IEC 61511?

IEC 61511 is due to be updated in late 2015 or early 2016. IEC 61511 is being updated to bring it in line with IEC 61508 edition 2 which was released in 2010 for example adding Systematic Capability (SC) and SIS Security. More emphasis has been placed in Functional Safety Audits (FSA) and more clarity has been added for Safety Requirement Specification (SRS). Information on the changes in edition 2 is relatively available so we feel no need to comment further in this document.

3.3 Comparison of Functional Safety Management (FSM)

The FSM requirements for standalone machinery are simple and based around safety planning. A full IEC 61508 FSM system would fit and work for machinery; however it is typically too onerous for standalone machinery and would never be used by small machine builders.

If the situation occurs where a machine presents risks for a process the machine builder must be part of the process FSM system. If the machine is just standalone the simple IEC 62061 / ISO 13849 FSM system can be used.

If machinery is to be combined into large complex assemblies of machinery a full IEC 61508 FSM system, or at least a FSM taking into account multiple organisations being involved, can be a better solution. If the machinery safety-related control system contains Safety Instrumented Functions (SIFs) as well as machinery Safety Functions then the machinery and machine builder will need to come under an IEC 61508 / IEC 61511 FSM system.

Assemblies of machinery is where multiple machines have been combined together to produce a common element, functionally linked so that each unit effects the operation of other units or the whole assembly (separate combined risk assessment required), using the same control system.

Application Type	Apply IEC 61508/IEC 61511 FSM	Apply IEC 62061 FSM	Apply ISO 13849 FSM
Process with machinery that can impact the risk	Yes	Yes [Note 1]	Yes [Note 1]
Process with no machinery or machinery that cannot impact the risk	Yes	No [Note 2]	No [Note 2]
Standalone machinery	No	Yes	Yes
Machinery in a complex assembly	Recommended	Yes [Note 1]	Yes [Note 1]

Note 1 – Either IEC 62061 or ISO 13849 can be applied for machinery
Note 2 – Treat machinery that does not impact the risk of the process as standalone machinery

4 What are the issues for the Functional Safety (FS) Engineer?

The machinery functional safety standards do not mention or use the term ‘competence’ in relation to the FS Engineer other than in the possible requirement to have knowledge for FMEA of the machinery under control. IEC 61508 and IEC 61511 do list competence as a requirement for the FS Engineer in their more comprehensive functional safety management requirements. Competence must be seen as a requirement for the FS Engineers in all industries.

The UK Health and Safety Executive (HSE) website contains guidance on competence for functional safety. The guidance has been issued by the HSE, the Institute of Engineering Technology (IET) and the British Computer Society. This guidance applies to ALL sectors including machinery and the process industry:
http://www.hse.gov.uk/humanfactors/topics/mancomppt1.pdf
http://www.hse.gov.uk/humanfactors/topics/mancomppt2.pdf

It is not unusual for a machine to be built up from sections of ‘partly completed machinery’ from various suppliers that is then completed by the ‘machine manufacturer’. These sub-suppliers must fulfil all their functional safety responsibilities and pass on appropriate information, the status of the EHSRs, to the ‘machine manufacturer’ so the machine manufacturer can then fulfil their remaining

functional safety requirements and EHSRs. Both the sub-suppliers and the 'machine manufacturer' should use competent FS Engineers where appropriate and ensure good communication between all parties involved in the building of the machinery. A functional safety management system similar to that required by IEC 61508 maybe more suitable in such circumstances.

The role of FS Engineer in the process industry is most frequently a specialised role within a 'Control and Automation' or 'Instrumentation and Control' engineering group that has multiple competent resource. The role of FS Engineer with general industrial machinery is often a hybrid role combined with that of general control and automation which means it is unusual to find a team of machinery FS Engineers outside of a specialised consultancy group/business. Some of the specialised machinery suppliers and some industries (e.g. nuclear) do however maintain dedicated machinery FS Engineers. This can result in situations where functional safety competence is weak in the machinery sector if good competence/training/update programmes are not a priority especially as the engineers are expected to be multi skilled and conversant with many national/international standards. The machinery sector is however catching up and many large manufacturing companies are requesting functional safety competence as standard. Functional safety competence is required for all sectors of industry and must be a priority for all organisations involved in functional safety.

The actual activities that need to be undertaken by a FS Engineer in the process industry are similar to the activities of a FS Engineer for a machine builder. The functional safety aims for both sectors are the same, but the specific tasks undertaken are different from machine to process and from site to site. The differences are driven by the differences in the functional safety standards and the equipment under control e.g. the machine builders (IEC 62061) functional safety management is in the form of a safety plan for that machine which is typically not a full 'system' and less onerous than the requirements of IEC 61508 / IEC 61511.

The site operator (end user) must supply, to the machine builder and his Functional Safety Engineer, a detailed requirements specification including process parameters and DSEAR information and this must be considered for the risk assessment and design of the machine. The information must be detailed sufficiently to not only enable the Essential Health and Safety Requirements of *The Supply of Machinery (Safety) Regulations* to be met but also the process safety requirements. It is a good idea to start this information exchange prior to order placement on the machine manufacturer.

The machine builder must provide their hazards list (e.g. EHSRs) or preferably details of their machine risk assessment (and SRCF details) to the site operator and their Functional Safety Team so that the machine hazards and risks can be considered in relation to the process. A machine risk assessment can be easily updated if required following the process risk assessment. The site operator may need to include a representative from the machine builder in the HAZID / HAZOP process.

Due to the differences in the 'lifecycle' of the machinery functional safety standards compared to the process industry functional safety standard the machine operator very rarely has a FS Engineer on hand after validation is complete. Normally this is not the case for the process industry as the site operator must maintain the safety-related aspects of the lifecycle through operation, maintenance, decommissioning, etc. This situation can cause issues if machinery is required to be modified (controlled by either *The Supply of Machinery (Safety) Regulations* or PUWER) as the machine operator is normally reliant on external FS competence. It is recommended that a full lifecycle management approach is taken for all sectors including machinery and it is also recommended that the machine operator has some level of functional safety competence available through the lifecycle of the machine.

5 Key Considerations

Machinery that is totally standalone and installed on a process plant, i.e. has no possible impact on the safety of the process, can simply be treated like any other machine. The functional safety shall be handled using either IEC 62061 or ISO 13849. IEC 62061 and ISO 13849 specify the requirements for the design and implementation of safety-related controls systems of machinery. The use of either of these standards, in accordance with their scopes, can be presumed to fulfil the relevant safety requirements. IEC/TR 62061-1 (alternatively ISO/TR 23849) provides guidance on the application of IEC 62061 and ISO 13849 in the design of safety-related control systems for machinery.

Machinery installed on a process plant that does have a possible impact of the safety of the process must use IEC 62061 (or ISO 13849) as well as IEC 61511. The functional safety mechanisms for the machinery standards only consider hazards in the vicinity of the machinery and therefore hazards across the process plant will not be covered.

Hazard Analysis and Risk Assessment for machinery is very different from that for a process plant. *The Supply of Machinery (Safety) Regulations* requires that a defined list of 'hazards', the Essential Health and Safety Requirements (EHSRs), are considered and tackled. A harmonized standard, ISO 12100, is available to support this requirement by considering safety in the design of machinery including hazard identification and risk assessment. This mechanism is significantly different from that used in the process industry e.g. PHA, HAZID, HAZOP. Conversely the ISO 12100 mechanism is not suitable for analysing the hazards of a process plant. It is important therefore, to show ALARP, that both a process and a machinery risk assessment is completed and maintained. Some overlap will exist, for example a HAZOP for a dive support vessel will identify some of the machinery safety hazards and issues, but this will do no harm and will only support the aim of achieving a safe system. It is very important to not consider the machinery hazards in a LOPA. As per the requirements of *The Supply of Machinery (Safety) Regulations* any 'technical protective measures' that require some form of control system must show that the risk reduction is equal to or better than the harmonized standards.

Scenario: Let us consider an access hatch interlock that protects access into a tank with an agitator inside. Access is required on a frequent basis and the hazard concerned is related to the agitator movement. In this case this IEC 62061 or ISO 13849 would both automatically define this interlock as a Safety Function (SF) with a safety-related control system. A LOPA, for this example, may take credit for a Basic Process Control System (BPCS) handling an interlock which could reduce the risk reduction requirement to less than SIL 1. This LOPA approach would probably not meet ALARP (grossly disproportionate) in comparison to the harmonized standards IEC 62061 and ISO 13849.

Which Hazard Analysis and Risk Assessment should be performed first?
In most cases it is better to ensure the machinery risk assessment is completed first and an outline machine design is available prior to the process risk assessment especially for a more detailed type e.g. HAZOP. *The Supply of Machinery (Safety) Regulations* require in law that the risk assessment takes place and is available for use in the machine lifecycle.

5.1 Considerations from within the Process Industry

When is it suitable, if ever, to use IEC 61511 as a mechanism for my machinery functional safety?

It is not suitable to use IEC 61511 for machine functional safety. It is a requirement to use IEC 62061 (or ISO 13849) to ensure that the full requirements of *The Supply of Machinery (Safety) Regulations* are considered.

Can I put my machinery SF's into my SIS?

Yes. Machinery safety functions (SF's) can reside within a SIS as long as the SIS supports the requirements of *The Supply of Machinery (Safety) Regulations* (Machinery Directive). The requirements for both functional safety standards must be considered for the safety-related system. *The Supply of Machinery (Safety) Regulations* (Machinery Directive) covers 'safety components' as well as machinery and a indicative list of safety components is contained in Annex V.

Can I have SF's and SIF's in the same Safety-Related Controller?

Yes. See above. The requirements for both functional safety standards must be considered for the safety-related system so that it can support both high demand and low demand SFs.

How does this fit with a Layer of Protection Analysis (LOPA)?

If the LOPA for the process in question identifies that the machinery or its control system is a layer of protection then the SF's and SIF's must be in separate independent safety-related systems. Any LOPA should not consider the machinery hazards as if a safety-related control system is required they must be SF's to achieve ALARP.

How does 'Proof testing' impact this?

The requirements for 'Proof Testing' are similar across all the IEC functional safety standards and IEC 61508 drives this. It is important to remember that the scope of the machinery functional safety standards ends when the machinery enters the operation phase. The machinery functional safety standards are for high demand applications where the SF demand is often frequent reducing the emphasis on proof testing. It is not unusual for the proof test requirement for a machinery SF to be less frequent than the actual SF demand. This may result in the proof test simply being a visual confirmation that the SF has not been damaged or tampered with. Some more complex machinery SF's do however require extensive proof testing e.g. light curtains and stop tests. Proof testing for a SIF is an essential tool for functional safety due to the fact most SIF's are low demand resulting in elements that may only activate very infrequently.

What should be considered for 'Verification' and 'Validation'?

The concepts for verification and validation are similar for all the IEC functional safety standards however actual details for verification and validation will vary from machine to machine and process to process. Typically however machinery safety functions are much simpler in design and engineering than there process counter parts. It is therefore normal to have a more significant verification and validation task and plan for a process plant in comparison to the verification and validation task and plan for a machine. It is therefore generally easy to add machinery verification and validation tasks into a functional safety management structure for a process plant. The site operator must keep in mind that just a machine builder acceptance test plan does not validate the machinery.

Does new machinery have to be made to any particular standard?

No. The machine builder is not required to build the machine to any particular standard unless this is contractually agreed with the site operator / end user. If the machine in question is listed in Annex IV of the Machinery Directive a Notified Body may insist a particular harmonized standard or standard(s) is used. If non-harmonized standards are chosen the machine builder is obliged to prove in detail that the requirements of the *The Supply of Machinery (Safety) Regulations* (Machinery Directive) have been met (i.e. the EHSRs). The machine builder is not legally required to provide details on how they have achieved compliance they simply need to list the used standards on the Declaration of Conformity (DoC) or Declaration of Incorporation (DoI).

Can the site operator take the CE mark and Declaration of Conformity at face value?
No. As a minimum the site operator should do some due diligence on the machinery and its impact on safety including a risk assessment in relation to PUWER. The impact of the machine on the safety of the process must be considered by the site operator which may require the completion of requirements defined by IEC 61511.

5.2 Considerations from within the Machinery Sector

When is it suitable, if ever, to use IEC 62061 as a mechanism for my process functional safety?
It is not suitable to use IEC 62061 for process functional safety. It is essential to use IEC 61511 as the machine functional safety standards only consider hazards in the immediate vicinity of the machine. Also the machine functional safety standards take a much simpler approach to architectures and functional safety management. The machine functional safety standards also do not consider a 'full' safety lifecycle as their scope ends once the equipment under control enters the operational phase.

Can I put my SIF's into my SRECS?
Yes. The requirements for both functional safety standards must be considered for the safety-related system.

Can I have SF's and SIF's in the same Safety-Related Controller?
Yes. The requirements for both functional safety standards must be considered for the safety-related system so that it can support both high demand and low demand SFs.

How does this fit with LOPA?
If the site operator's LOPA for the process in question identifies that the machinery or its control system as a layer of protection then the SF's and SIF's must be in separate independent safety-related systems.

How does 'Proof testing' impact this?
The requirements for 'Proof Testing' are similar across all the IEC functional safety standards and IEC 61508 drives this. It is important to remember that the scope of the machinery functional safety standards ends when the machinery enters the operation phase. The machinery functional safety standards are for high demand applications where the SF demand is often frequent reducing the emphasis on proof testing. It is not unusual for the proof test requirement for a machinery SF to be less frequent than the actual SF demand. This may result in the proof test simply being a visual confirmation that the SF has not been damaged or tampered with. Some more complex machinery SF's do however require extensive proof testing e.g. light curtains and stop tests. Proof testing for a SIF is an essential tool for functional safety due to the fact most SIF's are low demand resulting in elements that may only activate very infrequently.

What should be considered for 'Verification' and 'Validation'?
The concepts for verification and validation are similar for all the IEC functional safety standards however actual details for verification and validation will vary from machine to machine and process to process. Typically however machinery safety functions are much simpler in design and engineering than there process counter parts. It is therefore normal to have a more significant verification and validation task and plan for a process plant in comparison to the verification and validation task and plan for a machine. It is therefore generally very hard to try and use machinery 'safety planning' to tackle the verification and validation elements for safety instrumented functions of a process plant. We cannot, however, see why anyone would want to even try.

Can the site operator get a copy of the machinery technical file?

The machinery technical file must include drawings of the machinery and its control circuits, the specifications and standards used in the design, and other relevant test results and data. Technical reports and certifications from other organisations may be included as well along with the declaration of conformity (DoC) or declaration of incorporation (DoI). The machine builder, however, is not obliged to make the content of the technical file available to the site operator / end user. If however the 'machinery' has an impact on the process safety of the plant the machine builder must support the site operator by providing appropriate information. This does not normally impinge on the intellectual property rights of the machine builder.

What information should the machine builder supply?

The site operator should have enough information from the machine builder to operate and maintain the machine safely e.g. operation and maintenance manual. This must include information on the residual risk and for the safety functions especially the mission times and proof testing requirements. If however the 'machinery' has an impact on the process safety of the plant the machine builder must support the site operator by providing appropriate information. This does not normally impinge on the intellectual property rights of the machine builder.

6 Existing and Emerging Standards (Suggested item to be included)

IEC 61508:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
IEC 61511-1:2003 – Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements
IEC 62061:2005+A1:2012 – Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic systems
ISO 13849-1:2006 – Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
ISO 13849-2:2012 – Safety of machinery – Safety-related parts of control systems – Part 2: Validation
IEC/TR 62061-1:2010 – Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
ISO/TR 23849: 2010 – Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

Are the two machinery functional safety standards ever likely to come together so that a single functional safety standard exists for machinery?

It has always been the aim to merge the two machinery functional safety standards, IEC 62061 and ISO 13849-1/-2, together however this has taken a long time.

The new merged standard has been allocated a number from both bodies namely IEC 17305 and ISO 17305 which we are expecting sometime around 2017/2018. The aim of this new standard is to aid understanding of machinery functional safety but also to keep backward compatibility with IEC 62061 and ISO 13849 for safety systems that have already been installed.

It is too early to tell which elements of the standards will be kept or lost or even what new aspects will be added. Committee work is still ongoing. However we can speculate, due to the requirement for backward compatibility, that most aspects will be very similar to the existing standards.

7 61508 Association Recommended Practices

This document sets out to overview the current best practices in functional safety systems for machinery and the process industry, but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the equipment and installation.

- Suitable hazard analysis and risk assessments must be completed for both the machinery and the process.
- IEC 62061 and / or ISO 13849 must be used for functional safety of machinery, i.e. equipment that meets the definition of *The Supply of Machinery (Safety) Regulations*, even when the machinery is installed on a process plant.
- IEC 61511 must be used for functional safety of the process with or without interaction to machinery (equipment that meets the definition of *The Supply of Machinery (Safety) Regulations*).
- Functional Safety Management (FSM), considering a full lifecycle approach, must be used for the delivery of functional safety in every industry.
- Competence is essential in the delivery of functional safety in every industry.
- Evidence must be produced in all industries that ALARP / SFAIRP have been achieved.

Important Note: The information within in this report was correct on the date of publication. Legislation and international standards can change therefore we recommend that the information within this report is validated with reference to legislation and the listed international standards before use.

Further Information:
http://www.hse.gov.uk/
http://www.hse.gov.uk/risk/theory/r2p2.htm
http://ec.europa.eu/growth/single-market/ce-marking/manufacturers/directives/index_en.htm
http://www.hse.gov.uk/work-equipment-machinery/machinery-directive-essential-requirements.htm
http://www.hse.gov.uk/work-equipment-machinery/new-machinery.htm