THE 61508 ASSOCIATION
Guidance in Compliance

Where Process Safety meets Machine Safety

A document to aid understanding between the end-user and machine builder for functional safety issues.

by The 61508 Association

Overriding key principle....it must be safe!

THE 61508 ASSOCIATION
Guidance in Compliance

Legislation

In the UK operating sites and the machine builder are subject to the ***Management of Health & Safety at Work Act 1999***.

In principle this requires the site operator to reduce 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.

THE 61508 ASSOCIATION
Guidance in Compliance

Legislation

The UK operating sites and the machine builder are subject to the ***Health & Safety at Work Act etc. 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 builder 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

THE 61508 ASSOCIATION
Guidance in Compliance

Legislation

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***" or, in the UK, the "***Supply of Machinery (Safety) Regulations***" namely (other directives and regulations do apply):

The machinery must meet all relevant **essential health & 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.

THE 61508 ASSOCIATION
Guidance in Compliance

Legislation

The **Official Journal of the European Union** lists the harmonised standards for the European product safety directives (e.g. The Machinery Directive). Although their 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 (EHSR).

The use of a harmonised standard 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.

THE 61508 ASSOCIATION
Guidance in Compliance

What is Machinery

Quote:

An assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application……

Directive 2006/42/EC (Machinery)

The Directive does have exclusions e.g. certain modes of transportation, seagoing vessels, machinery specially designed and constructed for police or military purposes.

THE 61508 ASSOCIATION
Guidance in Compliance

Legislation

What defines the minimum we should do?:

- Harmonized Standards
- Approved Code of Practice
- HSE Guidance
- International Standards

THE 61508 ASSOCIATION
Guidance in Compliance

EHSR's

Materials and products / Lighting / Design of machinery to facilitate handling / Ergonomics / Operating positions / Seating.

Safety and reliability of control systems / Control devices / Starting / Stopping / Selection of control or operator modes / Failure of the power supply.

Risk of loss of stability / Risk of break-up during operation / Risk due to falling or ejected objects / Risk due to surfaces, edges or angles / Risks related to combined machinery / Risks related to variations in operating conditions / Risks related to moving parts / Choice of protection against risk arising from moving parts / Risk of uncontrolled movements.

General requirements (robust, secure, etc.) / Special requirements (fixed, interlocking movable, adjustable, etc.) / Special requirements for protective devices.

Electricity supply / Static electricity / Energy supply other than electricity / Errors of fitting / Extreme temperatures / Fire / Explosion / Noise / Vibrations / Radiation / External Radiation / Laser Radiation / Emissions of hazardous materials and substances / Risk of being trapped in a machine / Risk of slipping, tripping or falling / Lightning.

Machinery maintenance / Access to operating positions and service points / Isolation of energy sources / Operator intervention / Cleaning of internal parts.

Information and warnings on the machine / Warnings of residual risk / Marking of machinery / Instructions.

THE 61508 ASSOCIATION
Guidance in Compliance

Risk

IEC 62061 / 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 / 61508 does not define **tolerable risk**. Tolerable risk for harm to people must be defined by the corporate body and it is up to the Duty Holder to meet **AND** the Duty Holder must show that **ALARP** has been achieved.

Some form of **Hazard Analysis and Risk Assessment** must be performed. (PHA / HAZID / HAZOP / ISO12100)

THE 61508 ASSOCIATION
Guidance in Compliance

Risk Assessment

The "***Supply of Machinery (Safety) Regulations***" require the machine builder to ('shall') perform a risk assessment (e.g. ISO 12100);

The machine builder should eliminate significant risks (by designing them out) or, if that is not possible;

The machine builder should provide safeguards (e.g. guarding) or, if that is not possible;

The machine builder must provide information about any residual risks and affix warning signs.

- The machine builder generally has **little knowledge of the process**
- The end user has **little knowledge of the machine**.
- It is usually best to perform the machine risk assessment first followed by the process risk assessment.

THE 61508 ASSOCIATION
Guidance in Compliance

Risk Assessment

‘End User ➔ ‘Machine Builder’ – **Detailed requirements specification** including process parameters and DSEAR information and this must be considered for the risk assessment of the machine.

The information must be detailed sufficiently to meet the:

- **essential health & safety requirements** of the *Supply of Machinery (Safety) Regulations*
- **process safety requirements**.

‘Machine Builder’ ➔ ‘End User’ – risk assessment (e.g. ISO 12100) / EHSRs, as the hazards and risks of the machine **must be considered in relation to the process**.

THE 61508 ASSOCIATION
Guidance in Compliance

Process Hazard Analysis (PHA)

Identifying hazards

HAZOP (Hazards and Operability Study)

Checklist / What If Analysis

FMEA (Failure Modes and Effects Analysis)

Fault Tree Analysis

Etc.

Causes	Consequences	Safeguards	Recommendations
Column Steam Reboiler pressure control fails, causing excessive heat input	**Column overpressure and potential mechanical failure of the vessel and release of its contents**	**1) Pressure relief valve** **2) Operator intervention on high pressure alarm** **3) Mechanical Design**	**Install SIS to stop reboiler steam flow upon high column pressure**
Low flow through pump causes pump failure and subsequent seal failure	**Pump seal fails and releases flammable materials**	**1) Low output flow pump** **2) Shutdown SIS**	**Existing safeguards are adequate**

THE 61508 ASSOCIATION
Guidance in Compliance

Functional Safety

Functional Safety with the process industry is achieved using **IEC 61511** (and normally in low demand mode of operation) where as functional safety of machinery is achieved using either **IEC 62061 or ISO 13849** as either high demand mode or continuous mode of operation.

IEC 62061 or ISO13849 are **concerned only** with the risk and functional safety requirements in the **immediate vicinity of the machine**. Requirements to mitigate risk arising from other hazards must be considered by the site operator (End User).

THE 61508 ASSOCIATION
Guidance in Compliance

Comparison / Differences

Management of Functional Safety / Safety Planning / Validation Planning

‘Proven in Use’ / high demand or continuous mode of operation / Route 1_H of IEC 61508-2:2010

‘Basic Safety Principles’ / ‘Well-Tried Safety Principles’

The Supply of Machinery (Safety) Regulations

The Provision and Use of Work Equipment Regulations (PUWER)

‘Significant Modification’

Architectures 1oo1 and 1oo2 based

Separation of safety-related controls

‘Mission Time’

Safety-related software

THE 61508 ASSOCIATION
Guidance in Compliance

Comparison / Differences

CCF:

'*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*'

'*failures of different items, resulting from a single event, where these failures are not consequences of each other*'.

SFF:

the fraction of the overall failure rate that does not result in a dangerous failure (i.e. safe failures & dangerous detected failures) .

DC:

the ratio of dangerous failures that can be detected.

SRS:

Safety Requirement Specification

THE 61508 ASSOCIATION
Guidance in Compliance

Functional Safety Management

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 Note 1	Yes Note 1
Machinery in a complex assembly	Recommended	Yes Note 1	Yes Note 1

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

THE 61508 ASSOCIATION
Guidance in Compliance

Functional Safety Engineer

IEC 62061 / ISO 13849 – what competence? / knowledge for FMEA .

IEC 61508 / IEC 61511 – competence as a requirement for the FS Engineer / FSM.

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

THE 61508 ASSOCIATION
Guidance in Compliance

Machinery Sector View

When is it suitable, if ever, to use IEC 62061 as a mechanism for my process functional safety?

Can I put my SIF's into my SRECS?

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

How does this fit with LOPA?

How does 'Proof testing' impact this?

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

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

What information should the machine builder supply?

THE 61508 ASSOCIATION
Guidance in Compliance

Process Industry View

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

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

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

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

How does 'Proof testing' impact this?

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

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

Can the site operator take the CE mark and Declaration of Conformity at face value?

THE 61508 ASSOCIATION
Guidance in Compliance

Key Points

Treat machinery that does not impact the process as **standalone machinery** and apply IEC 62061 / ISO 13849.

Apply IEC 61511, IEC 62061 and ISO 13849 for machinery that does impact the safety of the process.

Must have enough information from the machine builder to **operate the machine safely**.

The machine builder is not required to build the machine to **any particular standard** unless this is contractually agreed with the end user.

If the non-harmonized standards are chosen the machine builder is obliged to prove in detail that the requirements of the *Machinery Directive* have been met (i.e. the EHSR's).

The CE mark is **not a quality mark** and is only one of several requirements that the machine builder has to meet. Reasonable steps must still be taken to ensure the machine is safe.

The **machine builder is not obliged** to make the content of the technical files available to the end user.

THE 61508 ASSOCIATION
Guidance in Compliance

Key Points

IEC 62061 and ISO 13849 specify the requirements for the design and implementation of safety-related control 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

In short, for machinery applications in hazardous process industry applications, the application of **both IEC 61511 and IEC 62061** (or ISO 13849) should be considered.

THE 61508 ASSOCIATION
Guidance in Compliance

The Future

By 2017 / 2018 IEC 62061 and ISO 13849-1 will be merged into a single standard for machinery IEC / ISO 17305.

The aim of this update is to clarify understanding and use of IEC 62061 and ISO 13849 while still keeping backward compatibility to safety systems that have already been installed.

An amendment is expected for ISO 13849-1 that may lessen some requirements for functional safety. We recommend current functional safety good practice is followed.

IEC 61511 will 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).

THE 61508 ASSOCIATION
Guidance in Compliance

Useful Links

http://www.hse.gov.uk/risk/theory/r2p2.htm

http://www.hse.gov.uk/work-equipment-machinery/new-machinery.htm

http://www.hse.gov.uk/work-equipment-machinery/machinery-directive-essential-requirements.htm

THE 61508 ASSOCIATION
Guidance in Compliance

How to contact the 61508 Association?

Web: www.61508.org

Contact: John Todd, Coordinator for the 61508 Association

Email: jtodd@61508.org

Post: The 61508 Association, 15 Hillside Road, Knutsford, Cheshire, UK.