TEN YEARS OF IEC 61508; HAS IT MADE ANY DIFFERENCE?

A. G. Foord and W. G. Gulland, 4-Sight Consulting, UK
C. R. Howard, Istech Consulting Ltd, UK

Since 1998 and 2000, when the first edition of IEC 61508 was published, there have been significant improvements in both the awareness and the use of functional safety. The need for "trip testing" was already very well established, but now there is a realisation that much more is needed, particularly the need for:

- Competence;
- Effective Risk Assessment;
- Verification; and
- Validation.

IEC 61508 has also created some problems, many of which have been addressed by changes in the 2010 revision published last July. All the significant revisions are included and explained in this paper.

KEYWORDS: Functional Safety, Risk Assessment, IEC 61508, IEC 61511

INTRODUCTION

The first three of seven parts of the Basic Safety Standard IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" were first published in 1998 and the remaining four parts in 2000 [IEC 61508, 1998 & 2000]. There have been several positive results and the first revision of all seven parts of IEC 61508 was published in July 2010 [IEC 61508, 2010].

SECTOR SPECIFIC STANDARDS

IEC 61508 is a generic standard and sector specific standards have now been written, for example, [IEC 61511, 2003] for the process, oil production and non-nuclear power plants and [IEC 61513, 2001] for nuclear power plants.

AWARENESS OF FUNCTIONAL SAFETY

There is now a wider understanding that functional safety relies on active systems. Thus, this part of process safety depends on a system or equipment operating correctly in response to input measurements and requires special checking. Increased awareness has come from a number of areas:

PROMOTION BY HSE

The process sector standard, IEC 61511, "Safety Instrumented Systems" and the nuclear power station standard IEC 61513 "I&C systems important to safety" have been promoted by HSE as their expectation for the design, installation, operation and maintenance of automatic protection systems in these sectors of industry. This has encouraged many companies to either adopt these standards or to update their own internal guidance to comply with IEC 61511 or IEC 61513.

MAJOR INCIDENTS

Significant accidents receive massive publicity and failures of prevention and/or mitigation systems have been a contributory factor in some of these incidents even though human factors may have been more important. For example:

1. The explosions at Buncefield in 2005 in the UK [Buncefield, 2008] where both the high level alarm and the high high level trip failed on a petrol storage tank.
2. The major accident at the Sayano–Shushenskaya Dam in Russia [Sayano–Shushenskaya, 2009] where the protection failed because of loss of power (the protection was not designed as "de-energise to trip" [Foord, 2008]) and tragically 75 people were killed.

INCLUSION IN EDUCATION AND TRAINING COURSES

The importance of prevention and mitigation systems, including alarm and trip systems, is now included in many engineering degree courses. Numerous commercial training courses on functional safety are now available. A search on Google for the term "functional safety" generates 115,000 results and the term is defined on Wikipedia.

MANAGEMENT OF FUNCTIONAL SAFETY

Unlike some other countries, the UK Health & Safety at Work Act [HASAWA, 1974] does not require the reduction of risk to zero. Most organisations recognise this and the management of functional safety is now included within the safety management systems of many companies. Safety Integrity Level (SIL) assessment is a form of risk assessment and requires risk targets for safety; these may be implied in a risk matrix or risk graph, or quoted as explicit numerical risk targets. Some companies have now specified realistic numerical risk targets (not zero) for individual hazards. Without non-zero risk targets, the SIL assessment is not possible.

PROOF/TRIP TESTING

Many companies used to have a fixed policy of trip testing, for example once a year. Many now use a more rational

choice of proof test intervals: once a year is not enough for some trips and annual testing is unnecessarily frequent for some other trips.

SAFETY LIFECYCLE

In order to comply with IEC 61508 or any of the sector specific standards, a safety lifecycle must be used for design, installation, operation and maintenance of control, monitoring and protection (prevention and mitigation) systems for safety. Some companies have now integrated a safety lifecycle into their project lifecycle to ensure it is used routinely and not forgotten.

VERIFICATION

Most companies appreciate the value of independent checking at each phase of a project and many can now demonstrate significant savings from earlier detection of inconsistencies and the application of Functional Safety Assessment. For example, the pressure rating of an offshore riser was not consistent with the setting of the high pressure trip. Investigation revealed that the trip setting was correct and the piping specification was incorrect. This error was detected before the riser was installed.

There is still no general appreciation of the degree of independence needed (should checking be done by "peer review" or verification be done by a separate company), but at least there is the understanding that checking is essential and not simply an option.

PROVEN IN USE

It is always difficult to know when to apply a new standard to old systems, particularly when modifications are made to old systems. Methods of dealing with "legacy" systems have been developed and components may continue to be used where they have a proven track record.

PRACTICAL IMPROVEMENTS ARISING FROM THE USE OF IEC 61508

SUBSEA ISOLATION VALVES

Many older subsea isolation valves were installed so that they were activated by a single solenoid valve. Now it is common practice to provide two solenoid valves and avoid the single point of failure. This may be due to a combination of implementing IEC 61508 and evolving best practice.

REDUCED USE OF RELIEF VALVES

High Integrity Pressure Protection Systems (HIPPS) are now often used to isolate the process source of high pressure. As well as being more reliable than relief valves, this avoids the environmental impact of venting or flaring from a relief valve. Relief valves suffer from two problems in particular, they do not always "re-seat" that is they do not reset to be fully closed when the high pressure is removed, and it is difficult to achieve more that SIL 2 with a relief valve. There are now many examples of SIL 3 HIPPS that have been installed which shut-down or bypass pumps and compressors to remove the source of pressure.

LESS RELIANCE ON ALARMS AND OPERATOR RESPONSES

The improved understanding of layers of protection has resulted in an increased provision of suitable trips and less reliance on the operator responding to alarms. This is at least partly due to the HSE insisting on more consideration of Human Factors.

EXAMPLES OF ISSUES WHERE IEC 61508 HAS BEEN UNSUCCESSFUL

INHERENT SAFETY

A common attitude is to "add-on" protection rather than focus on inherent safety and eliminate or reduce the hazards at an early stage in the project. Some companies are still waiting for HAZOP to identify hazards, when this could be done at a much earlier stage in the project lifecycle. Recent project examples include proposing complex leak detection on pipelines rather than focusing on the causes of leaks; identifying the fire pumps as a source of ignition too late in the project to change their location; and providing elaborate mitigation for toxic gas releases because the fuel gas contained 1000ppm H2S rather than removing the H2S.

HIGH SIL = MORE SAFE

Correspondingly there is not enough recognition that a requirement for SIL 3 or SIL 4 systems may be a result of the lack of inherent safety. One company has significant leaks on each of their oil pipelines every year. When the authors pointed out that the solution was not to improve the leak detection, surprise was expressed! Thankfully most companies realise that the solution is to identify the causes of leaks and remove them at the design stage.

THE PERILS OF COMPLEXITY

There is still not enough awareness of the perils of complex systems. Modern computers permit the design of systems so complex that there is almost no chance that the operators will understand them. When these are working and the operation remains within the envelope expected by the original designers, all is well. When modes of operation change or faults appear, the lack of understanding is exposed and, all too often, the operator is blamed.

TECHNOLOGY

There is still an illusion that the use of technology can eliminate human errors. As people who are fallible are involved in every stage of the project lifecycle this is obviously unrealistic [Foord, 2006] yet still widely assumed. The 1998 and 2000 versions of IEC 61508 were weak on

human factors and this might have contributed to the illusion that what was needed was more technology. Both IEC 61511 and IEC 61513 include substantial requirements to both recognise and to take proper account of human factors.

QRA = MORE SAFE

"It must be safe, we did a QRA!" Sometimes it is implied that merely doing the quantitative analysis actually makes it safer. Wisely [HSE, 2001, on page 31] states that "The use of numerical estimates of risk by themselves can, for several reasons ... be misleading and lead to decisions which do not meet adequate levels of safety."

COMMUNICATION NETWORKS

IEC 61508 did not really address industrial communication networks. There is not much more in Edition 2, but a useful new standard [IEC 61784-3:2010] is now available. It has a general requirements section then a number of extensive sections each describing a specific, commercial safety protocol; ProfiSafe is one example.

RISK ASSESSMENT

IEC 61508 and IEC 61511 include parts that are "informative" and suggest possible methods and techniques for risk assessment. Some companies have treated these "informative" parts of the standards as "normative", and insisted on the use of a particular technique for risk assessment even when the guidance is not applicable.

UPDATES TO IEC 61508

The long awaited and eagerly anticipated 2nd Edition of IEC 61508 was published in June 2010 – was it worth it? Overall yes, there are useful updates, welcome clarifications and improvements, changes reflecting technology changes since the first edition was published, but also some additional complexities that may provide opportunities for extensive further discussion. At first sight the changes appear to be more extensive than they are in practice; the real changes are concentrated in particular areas of the documents. Many of the changes have been previously trailed [Bell, 2005 & 2009] and are summarised on the IEC website [Edition 2, 2010]. The following represents a view on some of the more important changes that have been noted thus far in working through the 2nd Edition.

TERMINOLOGY

There have been several important changes to terminology and definitions in the 2nd Edition of IEC 61508. These may affect the interpretation gained from use of the first edition of the standard. In total the list of definitions has been increased by 27 items (although in the new index there are at least two duplications and two omissions and a number of incorrect references). These include new terms and specific definitions for terms used in the text of the first edition but not included in the original IEC 61508-4. Particular examples of new definitions are for "element" and "sub system" that have resulted in changed definitions for "dangerous failure" and "safe failure"; new definitions for "compliant item safety manual", "failure rate", "no effect failure" and "no part failure"; "mean time to repair" and "mean repair time" and "probability of failure on demand" and "average probability of failure on demand". There have also been some removals e.g. "mistake", "module" and "logic system".

THE SAFETY LIFECYCLE

Perhaps the most significant single improvement is the addition to Part 1 of a new phase 9 in the lifecycle specific to definition of the "E/E/PE system safety requirements" as in Figure 1, inserted between the old phase 5 "Safety requirements allocation" and the old phase 9 "Safety related system PES realisation". This has transferred the preparation or the "safety requirements specification" from Part 2 to Part 1 of the standard. This new phase also has the effect of making it clear that preparation of the "safety requirements specification" is the responsibility of those who have developed the risk assessment and overall safety requirements in phases 1 through 5 of the lifecycle; and that they are to provide the necessary information in a suitable format for the organisation who will develop the E/E/PE safety related system into an appropriate physical entity.

With the preparation of the "safety requirements specification" now included in Part 1 (clause 2.10); this has led to a change in Part 2 where a "safety design requirements specification" has replaced the requirement for a "safety requirements specification" in clause 7.2. The "safety design requirements specification" will be used to translate the information provided in the "safety requirements specification" from (Edition 2) Part 1 phase 9 into the specific hardware and software requirements necessary to deliver a suitable physical safety related system. The "software safety requirements specification" section of part 3 remains broadly similar to the original and retains the original term, now fitting within the overall "safety design requirements specification" of part 2.

MANAGEMENT OF FUNCTIONAL SAFETY

The requirements have been made more comprehensive and upgraded to be fully normative rather than partly informative. Particular changes have been made to the requirements for appointing staff with responsibility for identified lifecycle phases and the identification of all the staff who will carry out defined activities for the safety related system; together with the need for all these staff to be appropriately competent for the work they are to do, and for this competence to be documented.

SYSTEMATIC SAFETY INTEGRITY

The requirements for systematic safety integrity have been reinforced in the second edition of IEC 61508, but with

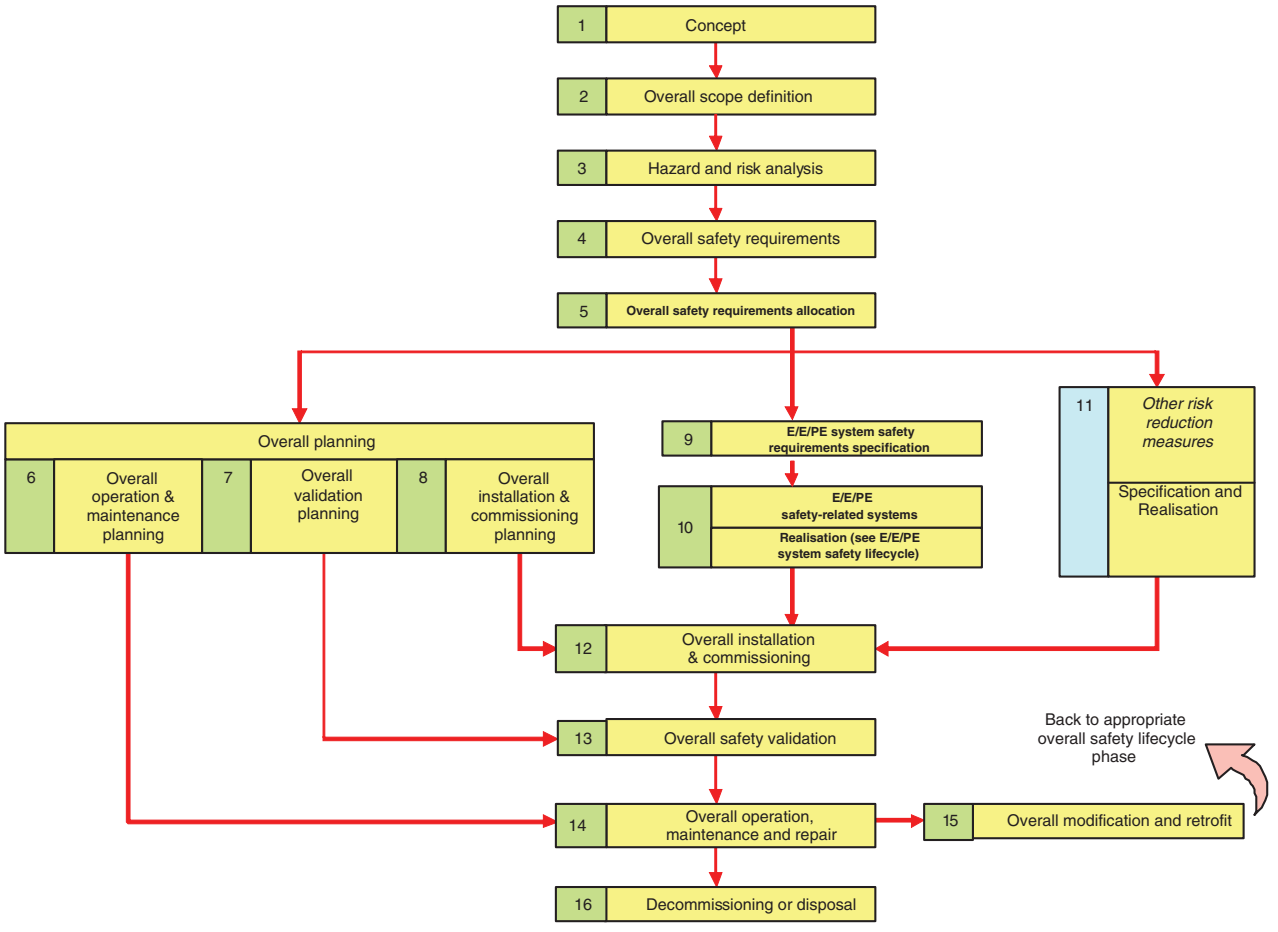

Figure 1. Revised IEC 61508-1:2010 "Overall safety lifecycle"

three possible route options, including the application of proven in use it remains to be seen how easy the requirements will be to apply and also how effective the revised options will be in practice at ensuring systematic safety integrity.

SYSTEMATIC CAPABILITY

This concept, applied to an element of a safety related system, has been introduced as a measure of the confidence that the systematic safety integrity meets the requirements of the specified safety integrity level. It is scaled SC1 to SC4, and apparently will align with the relevant contribution to the overall SIL assessment. This is a welcome clarification to avoid manufacturers' claiming SIL3 capability for individual components/elements.

Within part 3 the original V model figure 5 entitled "software safety integrity . . . ." Has been re-titled "software systematic capability" as in Figure 2, reinforcing the requirements for systematic capability, where safety integrity has often been inappropriately used. This is an example of a small but very significant change to the detail of the text that could easily be overlooked.

ARCHITECTURAL CONSTRAINTS

During the development of the 2nd Edition there were suggestions that the validity of the concept of the safe failure fraction in determining the redundancy needed for particular SILs was being questioned and might be dropped. In the event there are now two alternative routes for achieving the architectural constraint assessment. Apparently these have come about through different national committee approaches and the need for consensus in the final publication. This is potentially confusing and provides opportunities for issues when components assessed by the different approaches are assembled into a system. How it will work in practice remains to be seen for components sourced in the global market and then assembled into systems for export into another market where a different approach may be required to that used in the supply country.

COMPLIANT ITEM SAFETY MANUAL

A normative annex now included in part 2 requires that a safety manual is provided for all items that are claimed to be compliant with IEC 61508, with a clear list for contents, in particular information about failure modes, diagnostics,

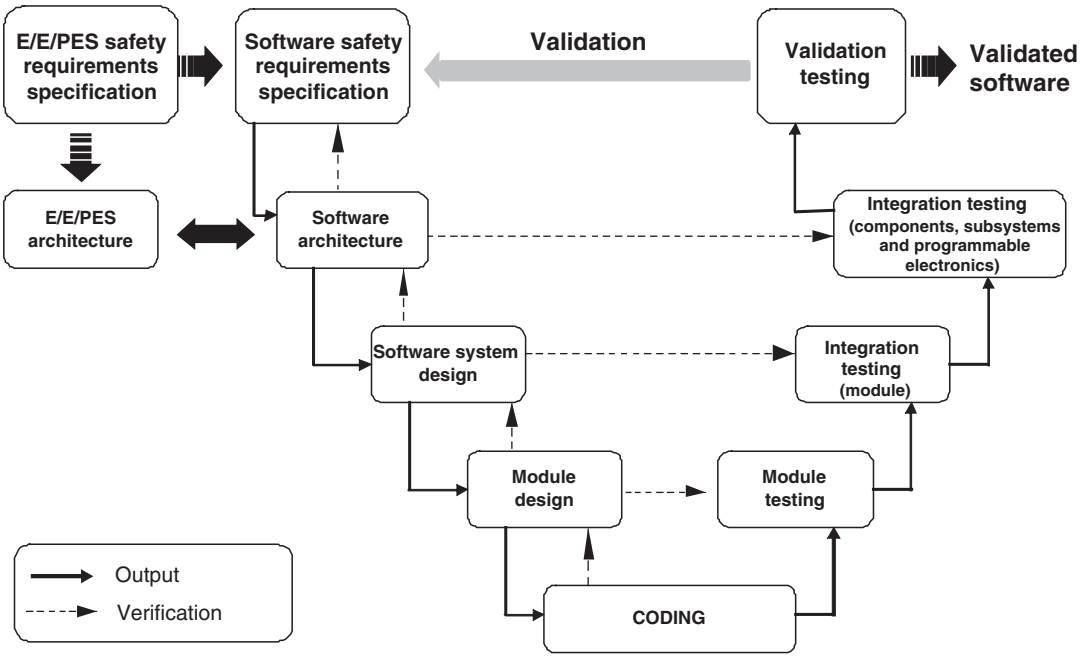

Figure 2. Revised IEC 61508-3:2010 "Software systematic capability and the development lifecycle (the V-model)"

failure rate data, procedures for proof testing and maintenance requirements, systematic capability and measures necessary to prevent systematic failure of the item when in service.

NEW TECHNOLOGIES

The standard has been specifically extended to reflect the new technologies that have become readily available for safety systems since the publication of the first edition in 1997 and in particular the use that can now be made of Application Specific Integrated Circuits (ASICs) and Data Communication.

NORMATIVE REFERENCES

The normative (mandatory) references can easily be overlooked. There have been a number of changes to the specific documents referenced, but also to the versions of the documents listed in the first edition. Part 2 is a particular case in point where a normative reference is a document that is not even a definitive standard, IEC/TS 61000-1-2.

THE INFORMATIVE PARTS

Both the main informative parts providing guidance on the application of the standard, parts 5 and 6 have been significantly extended or revised and provide the user with more comprehensive guidance than before.

In Part 5 significant additions have been made to Annex A, raising the profile of legal requirements to the top of the list, including sections describing individual and societal risk and the concept of risk profiling across the life of an asset, modes of operation and SIL determination, common cause and dependency failures and the role of mitigation systems. A new Annex B summarises the different methods for determining SIL requirements that are covered in more detail in the following annexes. A new Annex F provides information on Layer of Protection Analysis, with much of the text apparently drawn from IEC 61511-3, with additional text on the role of the basic process control system (BPCS) and alarms. Unfortunately the tables with data have not been included in IEC 61508-5. Annex E replaces the previous Annex D addressing the use of risk graphs. This specifically includes a section on the need for calibration of a risk graph (Annex E.3) and makes the vital point that "It is important that this process of calibration is agreed at a senior level within the organisation taking responsibility for safety". Table E2 purports to be an example of calibration, but in practice it is an example of a risk graph (taken form IEC 61511-3) that has already been calibrated elsewhere using the data defined in the table. Unfortunately it does not provide an example of the complete calibration methodology. The annex also continues to use the general scheme examples of risk graphs from the first edition, without including a strong health warning that these are examples and should be used with caution.

In Part 6 annexes B and D in particular have additional or redrafted material that significantly helps in understanding key concepts, in particular information on the use of probabilistic calculations (Annex B2); the Boolean approach (annex B4), that also includes helpful diagrams illustrating the impact of different proof testing regimes; the state/transition approaches (Annex B5) and handling uncertainties (Annex B6). Annex D includes a

section on Binomial failure rate (Shock model) to address the issue of triple or quadruple failures (should they be relevant) where the conventional application of the beta factor approach to common cause failure may result in over conservative results.

CONCLUSIONS

IEC 61508 (and the associated sector specific standards) have significantly influenced the way in which functional safety is perceived and used. There is undoubtedly greater awareness of functional safety issues, but still much confusion about what should be and what is best practise. While most of the changes in the 2nd edition of IEC 61508 are definitely improvements, whether or not it will have the same influence over the next 10 years remains to be seen.

REFERENCES AND BIBLIOGRAPHY

[Bell, 2009], Ron Bell, July 2009, Introduction and Revision of IEC 61508, Ron Bell Consulting Ltd, UK. Measurement + Control, pp. 174–179.

[Bell, 2005], Ron Bell, 2005, Introduction to IEC 61508, HSE, Bootle, UK. Paper UK Crown Copyright, first appeared at the ACS Workshop on Tools and Standards Sydney. Conferences in Research and Practice in Information Technology, Vol. No, 55, Tony Cant Ed.

[Buncefield, 2008], The final report of the Major Incident Investigation Board – Volumes 1, 2a & 2b, December 2008. http://www.buncefieldinvestigation.gov.uk/reports/

[Edition 2, 2010], Major changes in IEC 61508 ed 2.0. http://www.iec.ch/functionalsafety/explained/page2.htm

[Foord, 2006], A G Foord & W G Gulland, May 2006, Can Technology Eliminate Human Error? Trans IChemE, Part B, Process Safety and Environmental Protection, 84(B3): 171–173.

[Foord, 2008], A G Foord & C R Howard, November 2008, Energise or De-energise to trip? Measurement + Control, Vol 41/9.

[HASAWA, 1974], Health & Safety at Work Act, 1974.

[HSE, 2001], Reducing risks, protecting people, HSE's decision making process., ISBN 0-7176-2151-0 (often called R2P2).

[IEC 61508:1998 & 2000], Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1 – 7.

[IEC 61508:2010], Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1–7.

[IEC 61511:2003], Functional Safety: Safety Instrumented Systems for the process industry sector – Parts 1 – 3.

[IEC 61513:2001], Nuclear power plants. Instrumentation and control important to safety. General requirements for systems.

[IEC 61784-3:2010], Industrial communication networks. Profiles. Functional safety fieldbuses. General rules and profile definitions.

[Sayano-Shushenskaya, 2009], Sayano-Shushenskaya hydro accident, 2009. http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_hydro_accident