Session Fifteen

Improving allocation of client and contractor responsibilities for AS 61508 safety lifecycle activities

Mike Dean
Principal Engineer/Director, EUC Engineering Pty. Ltd.

Abstract

Correct allocation of activities and deliverables related to the safety lifecycle of AS 61508 between a client (end-user) and contractor is crucial to achieving success for a project targeting AS 61508 compliance.

Too often end-users establish specifications and scopes of work with the stated intention for the contractor to carry out all of the activities and providing all of the deliverables of overall safety lifecycle phases 1 to 13, without appreciation of their own key role.

End-users need to understand their own legal obligations and the intent of AS 61508 for establishing overall safety requirements. The paper proposes an allocation of responsibilities which achieves legal and AS 61508 compliance.

Introduction

This paper is based upon the use of AS 61508 for applications having a uniquely customised functional safety solution to a single location for a known and identified end-user. The focus of this paper is upon projects implemented under an Engineer-Procure-Construct (EPC) contract model between a client and an engineering contractor.

The Australian Standard AS 61508.1-2011 [1] describes a lifecycle approach to the safety of a facility or process from concept through the decommissioning and disposal. The lifecycle is shown in a diagrammatic form, comprising 16 discrete lifecycle phases, in Figure 2 of that standard [2]. A version of the diagram is shown below.

When considering a plan to initially deliver or to modify an existing E/E/PE safety related system(s) the overall safety lifecycle can be considered as being divided into two stages: Phases 1 to 13 represents the “project” stage and Phases 14 to 16 represents the “operational” stage.

It is reasonable when structuring contractual obligations in an EPC model of project implementation, for an end-user to transfer as much work and associated responsibilities to an engineering contractor as can legally and sensibly be assigned to them. However, when applied to the AS 61508 safety lifecycle, there are limits to what an end-user can assign to another party. These limits include: (a) legal obligations for health and safety at a facility operated by the end-user and (b) the intent of the standard.

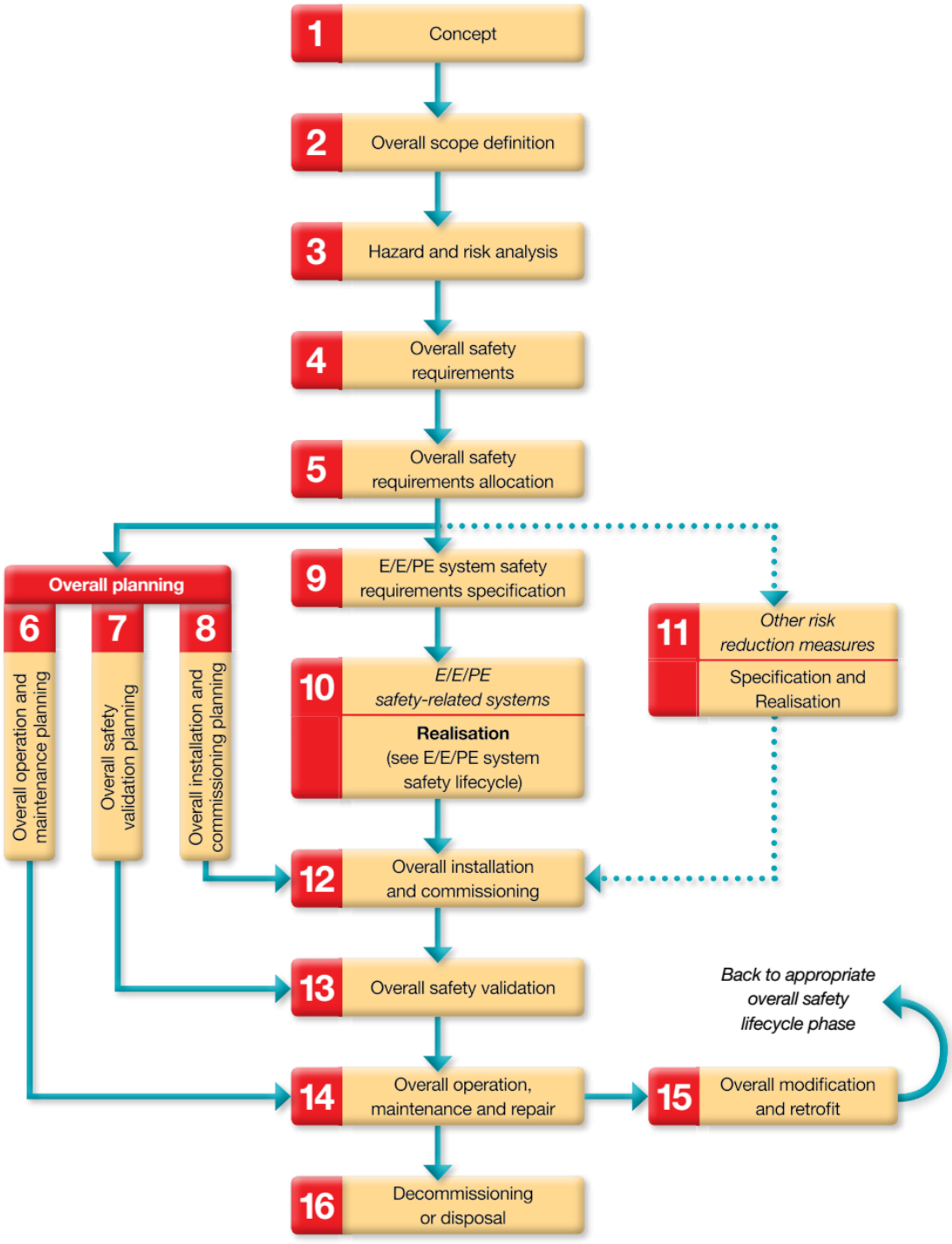

Figure 2 – Overall Safety Lifecycle from AS 61508.1-2011. Sector specific applications (such as the process industries or machinery) may have their own specific flowchart.

The author is familiar with contracts for functional safety projects that attempt to assign "all functional safety activities" and/or "sole responsibility for all functional safety management" in Phases 1 to 13 to a contractor. Attempts to transfer all responsibility to a contractor are: (a) probably not legally enforceable and (b) undermine the intent of the standard. They create a poorly structured basis for a project with a risk that appropriate levels of functional safety will not be delivered or maintained at the facility.

This paper explains some of the limits to transfer of responsibilities in functional safety projects and proposes a model for assignment of responsibilities between an end-user and contractor.

Legal Limits on Transfer of Responsibility for Safety

For the purposes of this paper a useful generalised legislative reference is the Model Workplace Health and Safety (WHS) Act [4] which has been adopted in a mostly verbatim form by various Australian jurisdictions to govern workplace health and safety. It should be noted that other legislation applicable to matters other than workplace health and safety may apply to functional safety solutions.

The subject of functional safety is about achievement of safety of equipment or a process "that depends on the correct functioning of an E/E/PE safety-related system and other risk reduction measures" [3]. Thus the implementation or modification of a functional safety solution in a workplace has to align to the obligations contained within the applicable legislation for safety of personnel at the workplace.

The key section of the Model WHS Act in regards to the primary responsibilities for ensuring the health and safety of persons in a workplace are found in section 19 (Primary duty of care) which states in sub-section 1 (part only): "*A person conducting a business or undertaking (or PCBU) must ensure, so far as is reasonably practicable, the health and safety of: (a) workers engaged, or caused to be engaged by the person …*"[10].

The section relevant to the transference of this and any of the duties found in the Act, is section 14 (Duties not transferrable): *A duty cannot be transferred to another person*" [11]. The Model WHS Act is unequivocal in regards to the non-transferability of this and other duties. This non-transferability is a widely accepted view across a range of Australian jurisdictions (some exceptions from case law have been analysed in [5]).

In the context of functional safety, this prohibition on the transfer of primary duties of a PCBU means that the ultimate responsibility for the safety of a facility or process rests with the end-user (the party or person conducting the business or undertaking). Hence a functional safety solution designed to achieve a safe facility or process shall, in terms of all aspects of its lifecycle (concept to disposal), ultimately be the responsibility of the end-user.

It is reasonable and appropriate that the end-user delegates certain aspects of the implementation (and/or the operations and maintenance) lifecycle phases, inclusive of the applicable functional safety management activities, to third parties under a contract. These third parties may for example have specific products and competencies not possessed by the end-user. But it is important to understand that this does not imply a transference of the end-user's primary duty for health and safety in the workplace and in the context of this paper, the achievement of functional safety in accordance with the standard. Any contract wording that attempts to create such a transference may be legally unenforceable.

The primary duty of the end-user means that: (a) certain aspects of the safety lifecycle should not be delegated and (b) only those that can be delegated in full shall be so delegated. These aspects are embedded in the requirements of the standard. The details of these are discussed later in this paper.

It is worth to mention, in any discussion of legal obligations, that the Model WHS Act also establishes specific duties for workplace health and safety on designers (section 22), manufacturers (section 23), importers (section 24), suppliers (section 25) and installers, constructors and those commissioning (section 26) plant and structures [12]. These aren't elaborated here since they are not central to the focus of the paper.

AS 61508 Requirements for Management of Functional Safety

AS 61508.1-2011 clause 6 describes the objectives and requirements for management of functional safety. It is important to understand that alongside the lifecycle phase activities for the implementation and operation of a functional safety solution, is a parallel and continuous requirement for "management of functional safety".

The standard defines a long list of requirements (AS 61508.1-2011 clause 6.2.1 to 6.2.18) comprising "management of functional safety", however it is clause 6.2.1 which is most relevant in relation to a discussion over the responsibilities of an end-user of a functional safety solution.

Clause 6.2.1 is about the appointment of one or more persons to take responsibility for management of functional safety. It states: "*An organisation with responsibility for an E/E/PE safety-related system, or for one or more phases of the overall, E/E/PE system or software safety lifecycle, shall appoint one or more persons to take overall responsibility for:*"…(the following are paraphrased for brevity):

- The system and for its lifecycle phases.
- Coordinating the safety-related activities in those phases.
- The interfaces between the phases and other phases carried out by other organisations.
- Conducting the other activities defined as management of functional safety.
- Coordinating functional safety assessments.
- Ensuring functional safety is achieved and demonstrated as per the standard.

Since the end-user has "*responsibility for an E/E/PE safety-related system"* and also responsibility for one or more phases of the overall safety lifecycle (as a minimum Phases 14 to 16), then the clause shall apply to the end-user. This appointment shall be in parallel and in addition to any requirements for functional safety management that the end-user requires a contractor(s) to undertake. This means that the end-user shall appoint a person who shall take overall responsibility for the activities in clause 6.2.1 (which includes meeting the majority of the requirements in clause 6.2). The note to clause 6.2.1 states that the person or persons appointed shall have "sufficient management authority".

It should be noted that the requirements of clause 6.2.1 (and much of 6.2) in applying to the end-user do not suddenly commence at Phase 14. They exist throughout the project (in Phases 1 to 13) and beyond into Phase 14 to 16.

The standard does not support a view that it is reasonable for an end-user to seek to transfer "all responsibilities" or to assign "sole responsibility" for management of functional safety to a contractor.

Planning of Functional Safety Management Activities

The various requirements for management of functional safety include documentation of the policies, strategies, plans, procedures, roles and responsibilities. It has become common practice (though not an explicit requirement of the standard) to bring together this documentation in a Functional Safety Management Plan (FSMP).

Based upon the already established need for the end-user to take on responsibilities for management of functional safety, the logical extension is that the end-user should prepare an FSMP for the project.

The need to carry out management of functional safety creating a need for the preparation of an FSMP shall also apply to any contractor who takes on responsibility for one or more lifecycle phases. The most sensible arrangement is for the end-user to prepare an FSMP for the project at an early stage in the project, to which any contractor shall prepare an aligned subordinate FSMP relevant to their obligations.

AS 61508 Requirements for Establishment of Tolerable Risk Targets

AS 61508 targets achievement of safety by the establishment of overall tolerable levels of risk from identified hazards and hazardous scenarios (in Phase 4). Achievement of this tolerable level of risk is then allocated (in Phase 5) between safety functions implemented by E/E/PE safety-related systems and other risk reduction measures.

Unless a regulatory body has already determined the tolerable risk levels, then since the end-user carries legal responsibility for ensuring workplace health and safety on the facility, it is the end-user who should determine the tolerable levels of risk to be applied.

This responsibility should not be delegated since it is critical to the level of safety achieved. This responsibility can be considered closely aligned to the non-transferable primary duty of the end-user.

AS 61508 Requirements Represented by "Overall" Lifecycle Phases

Ten of the sixteen lifecycle phases in the "Overall safety lifecycle" (Figure 2 of AS 61508.1-2011) are prefaced with the word "overall". It is useful and relevant to gain an appreciation for what this term means. Some background information is necessary to lay a foundation for this discussion.

The AS 61508 standard is ostensibly about E/E/PE safety-related systems [6]. This includes their specification, design, implementation, operation and maintenance. However the specification of the safety integrity level (SIL) for the safety functions carried out by the one or more E/E/PE safety-related systems involves consideration and allocation of risk reduction to "other risk reduction measures". These are non-E/E/PE measures that can include a wide range of "passive" (e.g. bunding of a tank containing potentially harmful contents if spilled) and "active" (e.g. a spring operated pressure relief valve) risk reduction measures.

Hence a key input to the design and implementation of E/E/PE safety-related systems (the SIL allocated to a safety function implemented in such a system) can be directly linked to the risk reduction allocated to non-E/E/PE measures. The standard states it does not consider in detail the implementation of other risk reduction measures [6]. However for the reasons stated they remain as key elements of any functional safety solution

The word "overall" in the ten of the sixteen overall safety lifecycle phases is referring to and describing the scope of the phase to cover the means of achievement of the tolerable level of risk which encompasses both E/E/PE safety-related systems AND other risk reduction measures. For example in Phase 5, "overall safety requirements allocation", the objective is *"…to allocate the overall safety functions….to the designated E/E/PE safety-related systems and other risk reduction measures.*"[7]

But due to its E/E/PE focus, the standard has a logical difficulty to overcome in regards to other risk reduction measures. It recognizes that their identification, specification, design, implementation, commissioning, operation and maintenance are equally critical to achievement of "overall" safety as the E/E/PE safety-related systems. But because the standard is focused on implementation of E/E/PE safety-related systems, it has to exclude treating the other risk reduction measures in any detail. To get past this dilemma it routinely includes the following note:

> *"In order to achieve functional safety, similar requirements are necessary for all other risk reduction measures".*[8]

This note makes the achievement of functional safety contingent upon treating the other risk reduction measures in a similar fashion to E/E/PE safety-related systems. The implication is that focusing entirely upon the safety provided by E/E/PE safety-related systems and neglecting or not paying an equivalent level of attention to the other risk reduction measures means that functional safety will not be achieved.

The crucial nature of the other risk reduction measures in the composite picture of achieving the overall safety targets can be easily understood when considering a typical Layers of Protection Analysis (LOPA), which is a widely used safety allocation methodology to determine SILs especially in the process industries [13]. In a LOPA model various independent layers of protection each provide levels of risk reduction to achieve the overall risk reduction requirements. Failure of any of these layers to be implemented or in some way

not achieve their individual risk reduction and associated levels of integrity, can mean that the required level of overall risk reduction and hence safety will not be achieved.

Responsibility for an overall safety lifecycle phase which incorporates other risk reduction measures as well as E/E/PE safety-related systems, should only be assigned to a party that has the scope and capabilities to address the requirements of both the other risk reduction measures as well as E/E/PE safety-related systems.

Assigning responsibility for a safety lifecycle phase prefixed with “overall” in its title, to a party only contractually responsible for an E/E/PE safety-related system, is clearly leading to a situation in which the other risk reduction measure requirements in that phase will be neglected or omitted. As the standard implies, this is likely to mean that functional safety will not be achieved.

This excursion was pursued because for a significant proportion of functional safety projects, the contractor is responsible to implement a new or modified E/E/PE safety-related systems in a “brownfields” environment. The knowledge of existing and available other risk reduction measures typically rests with the end-user and not with a contractor. Unless the contractor has the knowledge, skills and resources to address all of the expected “other risk reduction measures” necessary to achieve functional safety, they should not be contracted to take full responsibility for lifecycle phases which deal with overall safety. Responsibility for these phases should remain with the end-user.

Suggested Split of Safety Lifecycle Phase Responsibilities for Brownfields Projects

Based on a need to implement a new or modified E/E/PE safety-related systems in a “brownfields” environment, the following table represents a suggested split of responsibilities on a per overall lifecycle phase basis. The split of responsibilities can be varied from that shown and the table is intended to be useful as a template for adjustment as required.

It is recommended that an equivalent tabulation of the safety lifecycle activities (supplemented with specific functional safety management requirements) be established as part of an FSMP and the EPC contract scope of work at the outset of a functional safety project.

Notes to the allocation:

1. To make the split of responsibilities as simple as possible it has been made between only two parties: an End User and an Engineering Contractor. It is envisaged that the resources of the End User could include both its own personnel with the support of a Functional Safety Consultant that it directly engages. Similarly the Engineering Contractor could comprise various parties including an overall engineering contractor, an E/E/PE Systems Vendor or Integrator and a Functional Safety Consultant. Additional columns and responsibility codes can be added to more fully elaborate the respective responsibilities for a specific application.

2. It is assumed that the brownfield nature of the project scope means that some other (non-E/E/PE) risk reduction measures are already in place, though the Engineering Contractor has no scope in regards to the other risk reduction measures. The actual project scope may require the upgrade, overhaul or augmentation of the other risk reduction measures.
3. For projects which can be considered as “greenfields”, whereby the project scope involves the design and initial implementation of the other (non-E/E/PE) risk reduction measures, then potential exists to hand over a greater degree of responsibility to an overall contractor.
4. EUC = Equipment Under Control.
5. X = Suggested allocation (though alternate arrangements are also viable).
   O = Allocation to the End User that is recommended to not be delegated to others.
6. The inclusion of the Functional Safety Assessment (FSA) entries in the table are not specified as occurring at these points in the overall safety lifecycle in the standard. Their timing is at the discretion of the relevant parties involved. A minimum of one FSA shall be conducted before the identified hazards are present (usually before operations commences).
7. The table primarily details lifecycle phase activities, supplemented with phase completion verifications and functional safety assessments. Other aspects of functional safety management are not addressed in the table. These comprise an ongoing set of activities and require separate elaboration in one or more Functional Safety Management Plans for the project.
8. A more detailed tabulation and proposed split of end-user and engineering contractor responsibilities (and other sub-contracted parties) for IEC 61508 functional safety projects can be found at [9].

Lifecycle Phase #	Overall Safety Lifecycle Name	Task/Activity/	End-User	Engineering Contractor	Notes
1	Concept	Gathering and documenting information on the EUC, its environment and hazards.	X		Typically done in the project scoping and study phases.
		Phase completion verification (See explanatory note below this table)	X		
2	Overall scope definition	Determining and documenting the boundary of the EUC and its control system.	X		Typically done in the project scoping and study phases.
		Specifying the scope and approach of the hazard and risk analysis (in phase 3).	X		Is effectively a planning step for Phase 3.
		Phase completion verification (See explanatory note below this table)	X		
3	Hazard and risk analysis	Establishment of the risk assessment (for use in this phase) and risk tolerability criteria (for use in the next phase).	O		It is recommended that this activity be retained as a responsibility of the end user.
		Preparing for the hazard and risk analysis (including preparation of terms of reference, arranging attendees).	X		

Lifecycle Phase #	Overall Safety Lifecycle Name	Task/Activity/	End-User	Engineering Contractor	Notes
		Conducting the hazard and risk analysis and documenting the outcomes.	X		If EC engaged at this time, attendance and input to the hazard and risk analysis is beneficial.
		Phase completion verification (See explanatory note below this table)	X		
4	Overall safety requirements	Specification of the overall safety functions and a target safety integrity requirement for each.	X		Often conducted and documented concurrently with Phase 5.
		Phase completion verification (See explanatory note below this table)	X		
5	Overall safety requirements allocation	Allocation of the overall safety functions and their target safety integrity requirement amongst E/E/PE safety related system(s) and other risk reduction measures. This phase establishes the SIL targets for the E/E/PE safety functions – and the relevant safety integrity targets for the other risk reduction measures.	X		Often conducted and documented concurrently with Phase 4. Includes non-E/E/PE "other" risk reduction measures.
		Phase completion verification (See explanatory note below this table)	X		
		Functional safety assessment for Phases 1 to 5 (or scope as determined by prior FSAs).	X		Optional requirement at this point. Refer AS 61508.1-2011 clause 8. Independence requirements are specified in this clause.
6	Overall operation and maintenance planning	Documenting a plan for how the E/E/PE safety related systems (and other risk reduction measures – see Note) shall be operated and maintained. Shall include the context of the operational and maintenance organizational structures and processes.	X		AS 61508 only describes planning for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Documenting a plan for how the E/E/PE safety related systems shall be operated and maintained.		X	To be incorporated or referenced in the overall plan. Shall be elaborated in detailed procedures prepared in Phase 10.
		Phase completion verification (See explanatory note below this table)	X		
7	Overall safety validation planning	Documenting a plan for how the E/E/PE safety related systems (and other risk reduction measures – see Note) shall be validated against the overall safety requirements allocation.	X		AS 61508 only describes planning for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Documenting a plan for how the E/E/PE safety related systems (and software) shall be validated against the safety requirements specification and more detailed specifications prepared in Phase 10.		X	To be incorporated or referenced in the overall plan. Overlap with Phases 10.2 in AS 61508.2-2011 (system) and AS 61508.3-2011 (software).
		Phase completion verification (See explanatory note below this table)	X		
8	Overall installation and commissioning planning	Documenting a plan for how the E/E/PE safety related systems (and other risk reduction measures – see Note) shall be installed and commissioned.	X		AS 61508 only describes planning for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Documenting a plan for how the E/E/PE safety related systems shall be installed and commissioned.		X	To be incorporated or referenced in the overall plan. Shall be elaborated in detailed procedures prepared in Phase 10.

Lifecycle Phase #	Overall Safety Lifecycle Name	Task/Activity/	End-User	Engineering Contractor	Notes
		Phase completion verification (See explanatory note below this table)	X		
9	E/E/PE system safety requirements specification	Preparation of a specification of the E/E/PE system safety requirements.	X		
		Phase completion verification (See explanatory note below this table)	X		
		Functional safety assessment for Phases 6 to 9 (or scope as determined by prior FSAs).	X		Optional requirement at this point. Refer AS 61508.1-2011 clause 8. Independence requirements are specified in this clause.
10	E/E/PE safety-related systems: realisation	Detailed design, implementation, fabrication, software programming, system integration and factory acceptance testing (system validation excluding field connected devices).		X	The requirements for this implementation are detailed in AS 61508.2-2011 (system) and AS 61508.3-2011 (software). Two subordinate safety lifecycles address each of these standards. Validation shall confirm achievement of the system safety requirements specifications and the specifications prepared in phases 10.1 of AS 61508.2-2011 (system) and AS 61508.3-2011 (software).
		Preparation of detailed installation, commissioning, operation and maintenance procedures for the E/E/PE safety related system (and its software).		X	Refer to lifecycle phases 10.2 and 10.5 in each of AS 61508.2-2011 (system) and AS 61508.3-2011 (software).
		Phase completion verification (See explanatory note below this table)	X		Note: A total of 12 subordinate lifecycle phases 10.1 to 10.6 for each of AS 61508.2-2011 (system) and AS 61508.3-2011 (software) also require phase completion verification in addition to the phase 10 in the overall safety lifecycle.
11	Other risk reduction measures: specification and realisation	The specification and implementation of new or upgraded other risk reduction measures to achieve the relevant safety integrity targets established in Phase 5.	X		AS 61508 does not address the specification and implementation of other risk reduction measures, though treatment shall be equivalent to that for E/E/PE safety-related systems
		Phase completion verification (See explanatory note below this table)	X		
12	Overall installation and commissioning	Installation and commissioning of new or upgraded other risk reduction measures in accordance with the overall installation and commissioning plan (Phase 8) and other detailed procedures developed during Phase 11.	X		AS 61508 only describes requirements for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Installation and commissioning of E/E/PE safety-related system(s) in accordance with the overall installation and commissioning plan (Phase 8) and other detailed procedures developed during Phase 10.		X	
		Phase completion verification (See explanatory note below this table)	X		

Lifecycle Phase #	Overall Safety Lifecycle Name	Task/Activity/	End-User	Engineering Contractor	Notes
13	Overall safety validation	Safety validation of new or upgraded other risk reduction measures in accordance with the overall validation plan (Phase 7).	X		AS 61508 only describes requirements for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment. Validation confirms that the originally specified requirements from phase 5 are achieved. Typically this is conducted in the context of commissioning the EUC.
		Safety validation of E/E/PE safety-related system(s) in accordance with the overall validation plan (Phase 7).		X	Validation confirms that the originally specified requirements from phase 5 are achieved. Typically this is conducted in the context of commissioning the EUC.
		Phase completion verification (See explanatory note below this table)	X		
		Functional safety assessment for Phases 10 to 13 (or scope as determined by prior FSAs).	O		At least one FSA shall have been completed before identified hazards are present. Refer AS 61508.1-2011 clause 8. Independence requirements are specified in this clause.
14	Overall operation, maintenance and repair	Operation, maintenance and repair of the other risk reduction measures in accordance with the overall operation and maintenance plan (Phase 6) and other detailed procedures developed during Phase 11.	X		AS 61508 only describes requirements for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Operation, maintenance and repair of the E/E/PE safety-related system(s) in accordance with the overall operation and maintenance plan (Phase 6) and other detailed procedures developed during Phase 10.	X		
		Phase completion verification (See explanatory note below this table)	X		
15	Overall modification and retrofit	Implementing procedures (developed under management of functional safety) for initiating, approving and progressing modifications to the other risk reduction measures.	X		AS 61508 only describes requirements for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Implementing procedures (developed under management of functional safety) for initiating, approving and progressing modifications to the E/E/PE safety-related systems.	X		
		Phase completion verification (See explanatory note below this table)	X		
16	Decommissioning or disposal	Development and implementation of procedures for decommissioning and/or disposing of the other risk reduction measures.	X		AS 61508 only describes requirements for E/E/PE safety-related system aspects – but other risk reduction measures require equivalent treatment.
		Development and implementation of procedures for decommissioning and/or disposing of the E/E/PE safety-related systems.	X		
		Phase completion verification (See explanatory note below this table)	X		
Notes					

Lifecycle Phase #	Overall Safety Lifecycle Name	Task/Activity/	End-User	Engineering Contractor	Notes
1	The Phase completion verification activity (applied at the completion of each phase) involves verifying phase activities and deliverable items are completed. This requires the preparation of a verification plan prior to phase commencement, enactment of the plan and issue of a verification report at the completion of the verification. Independence of verifier to those conducting the work is recommended.				

Competency

The starting point for this paper was the observation by the author that some end-users can assign responsibility for safety lifecycle phases 1 to 13 (and/or associated functional safety management) to an engineering contractor, when it is not appropriate to do so. The paper would be incomplete without some reflection on what the cause of this might be. After consideration, it is proposed that the primary cause may be a lack of appreciation for the overall objective of the safety lifecycle of AS 61508 – namely a piece of equipment or process made safe by a suitable combination of independent risk reduction measures. It seems that a contractual management mindset can sometimes triumph over the intent of the standard. Ultimately this lack of appreciation could be classified as a lack of competence. The second edition of the AS 61508 set of standards (published 2011) contains a greater level of focus on competency and its management [14]. All organisations involved in the overall safety lifecycle (end-users, designers, suppliers and project managers) need to reflect on the competency requirements of the standard and strive to achieve those at all levels of the organisation.

Conclusion

This paper was written in response to the author being involved with functional safety projects in which the contractual arrangements reflected end-users attempt to contract out all responsibilities for both functional safety lifecycle phase activities and functional safety management for Phases 1 to 13, in circumstances that required a much greater role by the end-user. These were perceived by the author to be problematic both from a legal basis and the intent of the AS 61508 standard.

The following reasons have been presented for why end-users should retain responsibilities for both lifecycle phase activities and functional safety management in Phases 1 to 13:

1. Most WHS legislation in Australia makes duties in regards to workplace health and safety either explicitly or implicitly non-transferable. This means that ultimate responsibility for workplace health and safety and any functional safety solution that provides workplace health and safety, sits squarely with the end-user. Contractual arrangements that attempt to transfer this duty to a contractor are likely to be unenforceable.
2. With this legal responsibility and the result that the end-user becomes responsible for functional safety in lifecycle Phases 14 to 16, the requirements of AS 61508.1-2011 clause 6.2.1 apply to the end-user. Hence the end-user shall appoint a person(s) to be responsible for management of functional safety, and for carrying out specified

functional safety activities. These are not limited to commencing at Phase 14.

3. In the absence of a regulatory specification for tolerable risk levels to be applied, an end-user should specify the tolerable risk levels to be applied in Phase 4. Due to close alignment of the primary duty of the end-user for WHS with the achieved level of safety that stems from this specification of tolerable risk levels, this responsibility should not be delegated.
4. Lifecycle phases containing the word "overall" in the title mean that both E/E/PE safety-related systems and other risk reduction measures have to be addressed. Where a functional safety solution incorporates other risk reduction measures, then to achieve functional safety, these other risk reduction measures need equivalent treatment as applied to E/E/PE safety-related systems. Assigning responsibility for a safety lifecycle phase with "overall" in the title to a contractor should only be done where the contractor has the scope and capabilities to address E/E/PE safety-related systems and other risk reduction measures. Otherwise responsibility for the phase should remain with the end-user.

For these reasons end-users need to consider carefully the degree to which they contract out responsibilities for functional safety projects, and to resist the urge to make engineering contractors responsible for all functional safety activities and functional safety management for overall safety lifecycle phases 1 to 13, when in reality they should be shouldering a greater degree of responsibility.

A suggested split of responsibilities for a brownfields functional safety project has been proposed. The assumed basis of the project is that the engineering contractor's scope is limited to a new or modified E/E/PE safety-related system (i.e. the contractors scope does not include other risk reduction measures, which are required for functional safety). The basis of the split considers the above-mentioned rationale. The split can be amended to suit the requirements of any project.

References

1. AS 61508.1-2011
2. Figure 2 of AS 61508.1-2011. Note: Two subordinate safety lifecycles also exist as an elaboration of Phase 10 in the overall safety lifecycle. Each comprise 6 phases and are shown in Figures 3 and 4 of the same standard.
3. AS 61508.4-2011 clause 3.1.12.
4. Model WHS Act, Safe Work Australia http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/model-work-health-safety-act-23-june-2011
5. Johnstone, Richard (2014) Engaging expert contractors: The work health and safety obligations of the business or undertaking. Australian Journal of Labour Law, 27(1), pp. 57-85.
6. AS 61508.1-2011 clause 7.6.2.7 Note 2.
7. AS 61508.1-2011 clause 7.6.1.1.
8. AS 61508.1-2011 clause 7.7 Note 5, clause 7.8 Note 3, clause 7.9 Note 3, clause 7.13 Note 3, clause 7.14 Note 3, clause 7.15 Note 6.

9. The 61508 Association. http://www.61508.org/?page_id=149 Document: EPC_End-User_Issue_02 Controlled doc. Downloaded 24th January 2015.
10. Model Work Health and Safety Bill (Model Bill 23/6/2011), Division 2, Section 19, Sub-section 1 (page 15). Downloaded from http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/model-work-health-safety-act-23-june-2011 on 24th January 2015.
11. Model Work Health and Safety Bill (Model Bill 23/6/2011), Division 1 Subdivision 1, Section 14 (page 13). Downloaded from http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/model-work-health-safety-act-23-june-2011 on 24th January 2015.
12. Model Work Health and Safety Bill (Model Bill 23/6/2011), Division 3 Sections 22 to 26 (pages 18 to 28). Downloaded from http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/model-work-health-safety-act-23-june-2011 on 24th January 2015.
13. AS IEC 61511-2004, Functional safety – Safety instrumented systems for the process industry sector Part 3: Guidance for the determination of the required safety integrity levels. Annex F: Layer of protection analysis (LOPA).
14. AS 61508.1-2011 clauses 6.2.13, 6.2.14 and 6.2.15.