Integrating ALARP and Inherent Safety into Fast-Track Design

David Stephens, Director, Oxford Hazard Management Ltd, 100 Old Road, Oxford OX3 8SX

Simon Round, Manager Design HSE, Amec Foster Wheeler Energy Limited, Shinfield Park, Reading RG2 9FW

Regulatory regimes for several of the more hazardous industries require safety case documentation demonstrating that the design results in risks that are As Low As Reasonably Practicable (ALARP). This implies that in all relevant design decisions, the safest reasonably practicable option has been selected, and further, that inherently safer design (ISD) approaches are chosen where available.

However, on many engineering projects, no evidence of this may be available when ALARP/ISD assessment is attempted. The safety case team then has to search for relevant decisions in unrelated design documentation and back-fit the ALARP/ISD arguments in discussion with the discipline engineers. In cases where the decision appears not ALARP or not inherently safe, it may be too late to seriously consider alternatives without jeopardising schedule commitments.

It was suspected that cumbersome procedures are often a contributor to the inefficiency of ALARP and ISD implementation. A suitable design project was used as a pilot study for a simplified procedure, written to encourage all engineering disciplines to take account of ALARP and ISD principles in design decisions.

The study confirmed the value of using such a simplified ALARP procedure, which can reduce duplication of effort both in redesign to back-fit safety features after a formal ALARP assessment, and also in identifying safety-related decisions made earlier in the design process to record them in the safety case. The simplified ALARP procedure needs to be supplemented by vigilance from the safety team to ensure it is used effectively.

The study confirmed that early consideration of ALARP and ISD, such as this approach encourages, allows greater use of ISD, rather than justifying later in the design process that inferior safety measures are ALARP. In most cases, the resulting simple evaluation was found to be sufficient without recourse to detailed assessment such as Cost Benefit Analysis (CBA).

The Problem

Background

Safety legislation in the UK (such as the Health and Safety at Work Act, 1974) and in other countries requires work to be made safe “so far as is reasonably practicable” (SFAIRP), which may be considered equivalent to reducing risk to a level that is “as low as reasonably practicable” (ALARP). Based on case law, ALARP is defined as a level of safety that could not be reduced without sacrifice (in terms of money, time or trouble) that is grossly disproportionate to the reduction in risk that is achieved (HSE, 2001).

Related to ALARP is the concept of inherently safer design (ISD) (Mansfield et al, 1996). The intent of ISD is to eliminate hazards completely, or reduce their magnitude significantly, by means that are inherent in the design and thus permanent and inseparable from it, thereby eliminating or reducing the need for safety systems and procedures. ISD is often expressed in the form of a hierarchy of safety measures, such as those illustrated in Figure 1.

A number of the more hazardous industries are regulated in the UK as permissioning regimes. The would-be operator of a hazardous facility must demonstrate in advance that hazards are adequately controlled. This includes demonstrating before the start of construction or installation of a hazardous facility that its design is consistent with ALARP and/or ISD requirements. Examples include nuclear facilities (ONR, 2014), facilities covered by the Control of Major Accident Hazard (COMAH) Regulations (HSE, 2015a, HSE, 2015c) and offshore installations (HSE, 2015b, HSE, 2016, HSE, 2006)

Where risks are not so high as to be intolerable, but too high to be considered broadly acceptable, possible measures to prevent or mitigate the event are evaluated by comparing their cost with the risk reduction they achieve. Measures should be adopted as reasonably practicable unless the cost is grossly disproportionate to the risk reduction (HSE, 2001). This may entail a quantitative cost benefit analysis (CBA): however, this is not always beneficial and is not usually considered essential by the regulators (HSE, 2003a, Hart, 2013). In particular, measures should be considered reasonably practicable if they are widely accepted as good practice, whatever CBA may indicate.

Similar approaches have been adopted in other countries; however, ALARP may not always be applied in precisely the same way as in the UK for many reasons. For example "reasonably practicable" may be interpreted differently according to the basis of legal systems or the local culture.

Figure 1. ISD Hierarchy examples

(Mansfield, 1996)	ONR SAP hierarchies (ONR, 2014)	Oil & Gas UK hierarchy (Piper et al, 2014)
1. avoid or eliminate hazard by design; 2. intensify, attenuate or substitute to reduce the severity of the hazard; 3. simplify to reduce the likelihood of the hazard occurring; 4. segregate people and emergency systems from the effects of hazards; 5. use passive safeguards that do not need initiation; 6. use active safeguards; 7. operator and maintenance procedures should be the last resort, especially for control and mitigation.	(a) reducing the inventory of potentially harmful substances to the minimum necessary to achieve the required function of the facility; (b) controlling the physical state of harmful substances to remove or minimise their potential effects; (c) minimising the energy potential within the process consistent with the required purposes of the facility, and of its various components. (a) Passive safety measures that do not rely on control systems, active safety systems or human intervention. (b) Automatically initiated active engineered safety measures. (c) Active engineered safety measures that need to be manually brought into service in response to a fault or accident. (d) Administrative safety measures. (e) Mitigation safety measures.	1. Elimination and minimisation of hazards by design (inherently safer design); 2. Prevention (reduction of likelihood); 3. Detection and control (limitation of scale, intensity and duration); 4. Mitigation of consequences (protection from effects); 5. Evacuation, escape and rescue (EER) arrangements.

ALARP Demonstration in Design Projects

The requirement to demonstrate that the design results in risks that are ALARP is usually addressed as part of risk evaluation of hazardous events. Risk evaluation is the final stage of risk assessment, preceded by risk identification and risk analysis (ISO, 2009). Once hazards have been identified and subjected to qualitative and/or quantitative risk analysis, the predicted risk is compared with tolerability thresholds and classified into one of three bands (HSE, 2001):

- An upper bound above which risks are deemed to be unacceptable (or "intolerable") and, save in exceptional circumstances, must either be reduced, whatever the cost, or the activity giving rise to the risk discontinued;
- A lower bound below which risks are regarded as being "broadly acceptable" and
- A range between the upper and lower bounds in which risks are regarded as being "tolerable" provided that they have been reduced to levels that are ALARP.

Hazardous events with risk falling between these two thresholds (widely known as the “ALARP band”) are subjected to formal ALARP assessment. This typically takes the form of option studies for prevention, control and mitigation measures. Some of the identified measures will be existing features of the design: others will be possible additional design safety features or design changes. All options for additional safety features should be evaluated and raised as design recommendations if found to be reasonably practicable. Thus, ALARP assessment can be considered as an example of making decisions between design alternatives on the basis of safety and cost.

Design decision-making

Decisions between options are an integral part of every design process and many design decisions will have safety implications, which should be taken into account, alongside other considerations such as cost and performance. Such decisions provide the opportunities to implement ISD principles, and could be also considered as much a part of the ALARP process as the formal ALARP assessment itself. Certainly, design decisions and ALARP and ISD assessments should at least inform and support one another.

Risk analysis of a facility that is being designed requires information that is generated in the course of design. Therefore, ALARP demonstration, which follows risk analysis, is usually undertaken towards the end of a design project. At this stage, many of the possible options for risk reduction will already have been evaluated as part of the normal design decision-making process. In principle at least, the formal ALARP assessment can refer to these decisions as supporting evidence. However, this presupposes that the earlier decisions took account of safety in a manner consistent with ALARP and ISD and that the decisions were recorded in sufficient detail. If these conditions are not met, ALARP and ISD demonstration may be undermined in a number of ways.

- If design decisions are not recorded clearly and accessibly, it is very difficult for the ALARP assessor to find out what options have been discarded and why.

- Risk reduction measures that were reasonably practicable at the start of the project may have been effectively ruled out by design decisions before being subjected to ALARP assessment. This is especially likely for the inherently safer options, which have to be "built in" to the design at an early stage. Incorporating such safety features may require substantial unpicking of the design, with unacceptable implications for cost and schedule.
- Even where it is possible to revisit design decisions, the design team may have become committed to the decisions they have made, and may resist any implication that their original decision was incorrect.

From experience across the engineering contracting industry, one or more of these features were observed on several design projects during ALARP and ISD assessment. No records of safety-related design decisions were available when ALARP/ISD assessment was attempted. The safety case team therefore had to search for relevant decisions in unrelated design documentation and back-fit the ALARP/ISD arguments in discussion with the discipline engineers. In cases where the decision appeared not ALARP or not inherently safe, it was too late to seriously consider alternatives without jeopardising schedule commitments.

Regulators (HSE, 2006) and engineers (Renwick, 2013) have also made similar observations that "Experience in the assessment of ……safety cases has confirmed that the achievement of an installation that is designed and constructed such that risks to persons are ALARP depends to a significant extent on the efforts applied to achieve inherently safer design at the earliest stages of the project design process."

It was observed that for many engineering companies, project procedures may be a contributor to the inefficiency of the ALARP and ISD assessment. Companies that routinely execute design of major hazard facilities have in-house procedures for ALARP assessment and most of their client companies have their own equivalents. Often, these procedures are very prescriptive, emphasising detailed ALARP assessment (usually including CBA). Some of the problems discussed above appeared to be unintended consequences of this type of procedure.

- They may reinforce the perception that ALARP need only be considered for risks in the "ALARP Band", forcing ALARP assessment to be scheduled near the end of the project, after risk assessment is completed.
- They are complex and designed to be used by safety experts. As a result, design engineers may see ALARP as something that does not concern them.
- Where they insist on excessive rigour, they are time-consuming and expensive, encouraging a view that ALARP assessment is to be used as sparingly as possible.

In the context of these concerns, the start of a new project presented the opportunity to try out a different approach and attempt to integrate ALARP and ISD considerations into design decision making from the start.

Pilot study - alternative approach to ALARP demonstration

The project

A front-end engineering design (FEED) project executed by Amec Foster Wheeler was identified as suitable for a pilot study of an alternative approach to ALARP demonstration due to a number of favourable features.

- As a FEED project, it could be expected to include numerous design decisions significant to safety.
- In particular, the scope included a number of pre-FEED studies to evaluate process options, alternative power generation configurations, layout, etc. which ensured many of the major design decisions would be formally reported.
- Although the client had in-house procedures, Amec Foster Wheeler's tender had proposed to use its own procedures and the client had accepted this. The Amec Foster Wheeler procedure for ALARP demonstration was written as guidance, rather than being prescriptive.
- The agreed deliverables included terms of reference (TOR) for the main studies, in which ALARP and ISD considerations could be included explicitly. In addition, the client's review of the TOR for ALARP provided a way to ensure their agreement to the alternative procedure.

ALARP procedure

The project-specific ALARP and ISD procedure was developed based on an escalated approach and incorporated in the ALARP TOR. It was explicitly stated to apply to all design decisions where safety is a significant consideration, and in particular, to formal option studies.

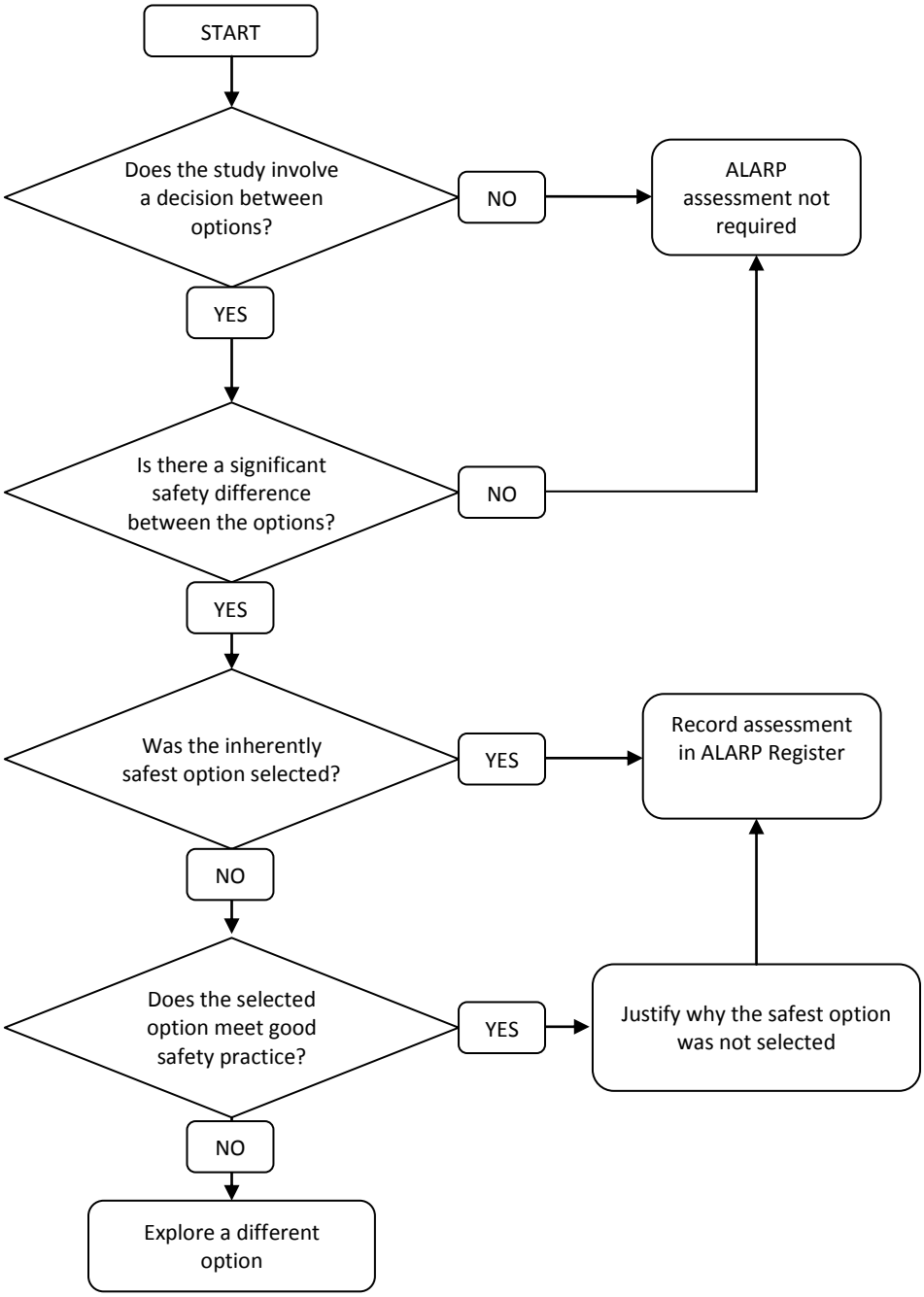
The ALARP TOR covered requirements both for consideration of safety in design decision-making and for formal ALARP assessment as part of risk assessment. This discussion focuses on the former. The TOR also established some general principles for consideration in ALARP decision-making.

- The inherently safest option is ALARP: if this option is chosen, no ALARP assessment is required. (A reference was included to another project document for a description of the inherent safety hierarchy.)
- If safety differentials between all options are essentially negligible, the selection should be made on other criteria without further consideration of ALARP.

- If the cost differential between two options is essentially negligible, the safer option should be selected.
- If a design option is recommended in applicable standards or codes of practice, or is widely applied as relevant good practice within the industry, it should be considered reasonably practicable.
- For higher-probability hazards, compliance with industry actual good practice is usually sufficient to demonstrate ALARP. Such hazards are likely to have a history of previous occurrence and standards for their prevention and mitigation will therefore be well-developed.
- It is necessary only to consider cost and risk differences sufficiently to discriminate between options. Estimation need not be more precise than is essential for this purpose. Costs and risks that are common to all options can be ignored.

A decision chart was provided for discipline engineers' guidance, as shown in Figure 2, as well as a checklist for recording straightforward safety-related design decisions.

Figure 2. ALARP Decision Chart



Arrangements were made clear for anyone to flag up to the project design safety team any complex decisions requiring more detailed analysis.

In addition, a one-paragraph summary of the approach was inserted into the TOR for each of the process and other studies.

The ALARP TOR also presented a simple ALARP Decisions Register template to be used for all ALARP decisions, in the form of a table comprising the following columns:

- reference number;
- ALARP topic;
- source reference;
- options considered;
- summary of ALARP argument;
- decision reached;
- actions raised.

There was the option to reference appendices for fuller analysis (e.g. CBA) where necessary. This allowed the main register to be kept brief. The ALARP assessment done as part of risk assessment was recorded separately in the hazard register (although, as might be expected, there was some overlap).

In preparing the procedure, the emphasis throughout was on simplicity and clarity, to make it as easy as possible for discipline engineers to ensure their decisions were consistent with ALARP and ISD principles and to keep the technical safety team informed. However, rather than relying solely on the procedure, members of the design safety team were alert to design decisions that might be safety-related, such as:

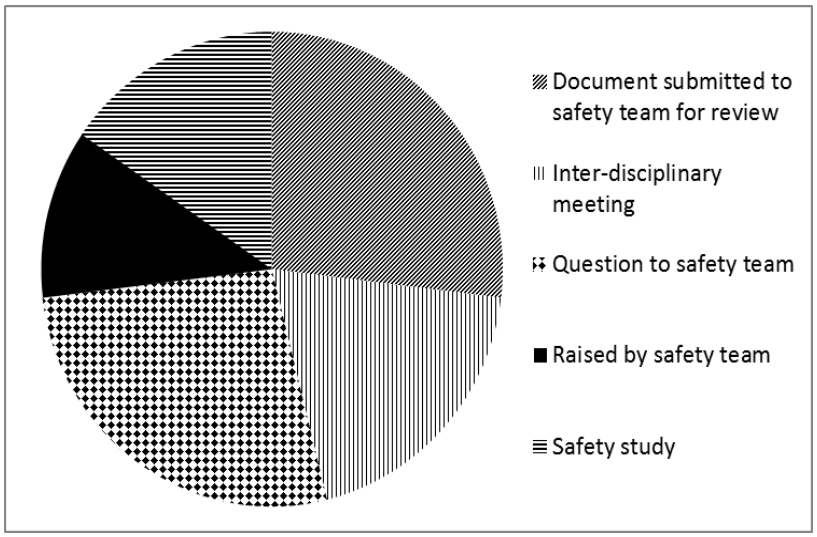
- issues raised in the discipline engineers' weekly meetings;
- implications of questions put to the safety team;
- suggestions made in forums such as the value improvement workshop.

Outcome of the pilot study

At the end of the project, the effectiveness of the alternative ALARP procedure was evaluated in several different ways.

- The ALARP Decisions Register was reviewed to identify the origins of the items listed. It was found that approximately 70% of decisions were flagged up as safety-related by the originating discipline rather than by the Design Safety team. However, the discipline engineers generally did not document issues in strict compliance with the TOR, but tended to raise them informally as questions to the safety engineers, or to record them in study reports circulated to Design Safety for review. For a full breakdown of sources of ALARP items, see Figure 3.

Figure 3. Sources of ALARP Items

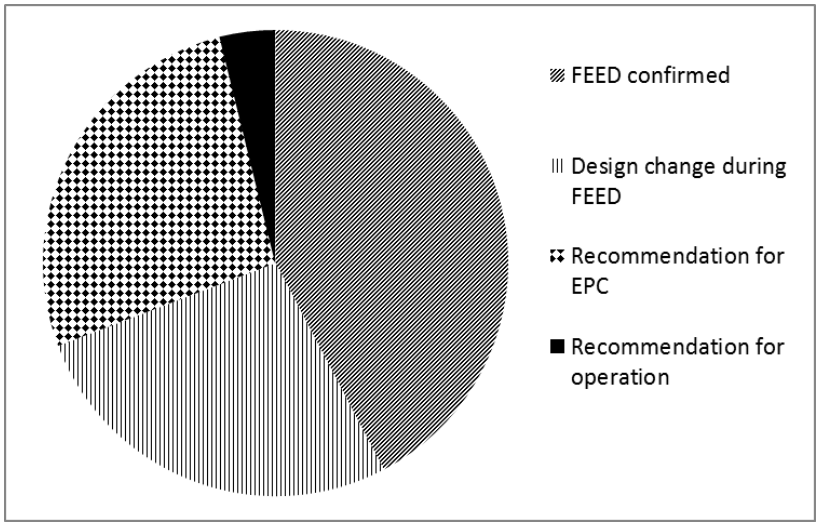


- The design options found to be ALARP were evaluated as to whether they were the inherently safest option, or a more practicable but less safe one. In many cases, it was not possible to distinguish which options were inherently safer: for example, where they were alternatives at the same level of the ISD hierarchy, or where some options

combined elements at different levels of the hierarchy. However, where the ISD option could be identified, it was found always to have been adopted.

- The Register was also reviewed to determine whether ALARP decisions had been closed out without the need for detailed evaluation and without raising actions for design modifications or further investigation during detailed engineering, procurement and construction (EPC). The simple assessment recorded in the ALARP Register was found to be sufficient in most cases: only 11% of items needed detailed assessment. In addition, most of the ALARP assessments confirmed the original design or could be resolved during FEED, as illustrated in Figure 4.
- Items that originated as recommendations from studies by other disciplines were reviewed and it was found that the recommendation in the original study was confirmed by the ALARP assessment in almost all cases.
- Design deliverables were reviewed to identify any safety-related decisions that had not been identified by the methods prescribed in the TOR. In particular, a Key Decisions Register, which was prepared separately by the project engineering team, independently of Design Safety, was reviewed. No new safety-related decisions were identified.

Figure 4. Resolution of ALARP Items



Example ALARP item – heating medium selection

The effect of using this simplified approach to ALARP assessment is illustrated using as an example the selection of a recirculating heating medium to capture waste heat from power generation for use in the hydrocarbon process. A number of alternative media were considered, including steam, pressurised water, synthetic oils, mineral oils, silicone fluids and glycols. The study considered safety issues that differ between options, such as:

- System pressure for effective operation at the required temperature;
- Leakage to/from the process;
- Corrosion;
- Toxicity and eco- toxicity;
- Flammability.

The usual risk and ALARP assessment would require a worked-up process design, for which this decision would already need to have been taken. Indeed, it is likely that the above hazards might not have featured in such an assessment, being overshadowed by fire and explosion risks from the hydrocarbon side. Instead, the simple approach allowed these significant hazards to be taken into account explicitly, both in this design decision and in the safety case.

Comparison with other projects

For comparison, "traditional" ALARP assessments undertaken in some other projects (not by Amec Foster Wheeler) were evaluated in a similar way. Every project is unique, and it is impossible to do a fully controlled comparison, so the results can never be definitive: however, it is at least possible to check whether any differences tend to confirm or refute the effectiveness of the modified method.

Three diverse oil & gas projects are compared in Figures 5 - 8:

- this project (labelled "AFW FEED");
- an onshore EPC project ("EPC1") for which ALARP was evaluated traditionally at the end of the project;
- an offshore detailed design project ("EPC2") for which decisions were reviewed in terms of ALARP during the project, but only by the safety team, without involving other disciplines.

Figure 5 confirms that other disciplines are more likely to flag up ALARP items if they are explicitly asked to do so. It also shows fewer ALARP items raised in safety studies on this pilot project: this is due simply to the use of a separate register for formal ALARP assessment as part of risk assessment, as noted above.

Figure 8 shows that ALARP assessment resulted in ISD features being adopted on this project. This reflects the fact that ALARP decisions were made earlier in the design process, both as a FEED project presents opportunities to implement ISD features that would be difficult to back-fit during EPC, and also as the modified method introduces ALARP earlier in the FEED. Similarly, Figures 6 and 7 indicate a trend for reduced use of CBA and increased opportunity to make design changes if ALARP is assessed early in the project.

Figure 5. Comparison: Sources

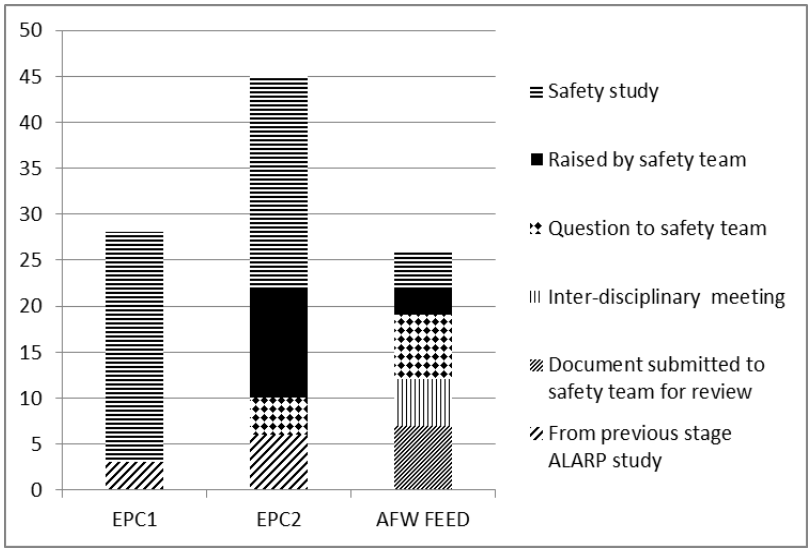


Figure 6. Comparison: Use of CBA

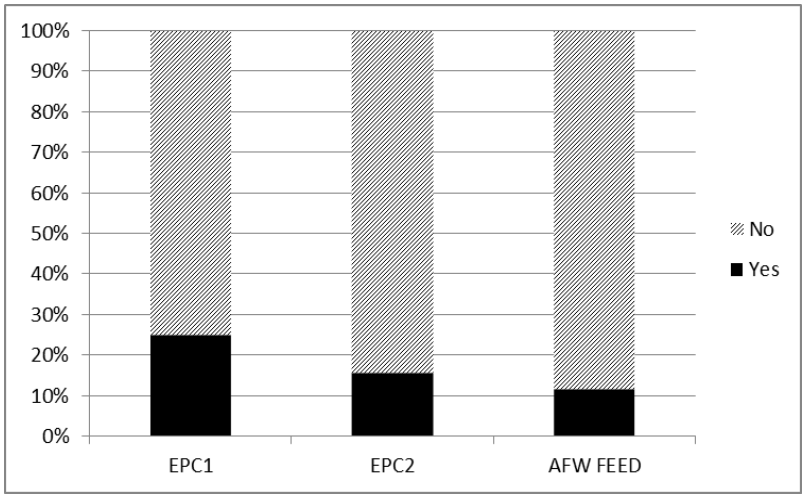


Figure 7. Comparison: Resolution

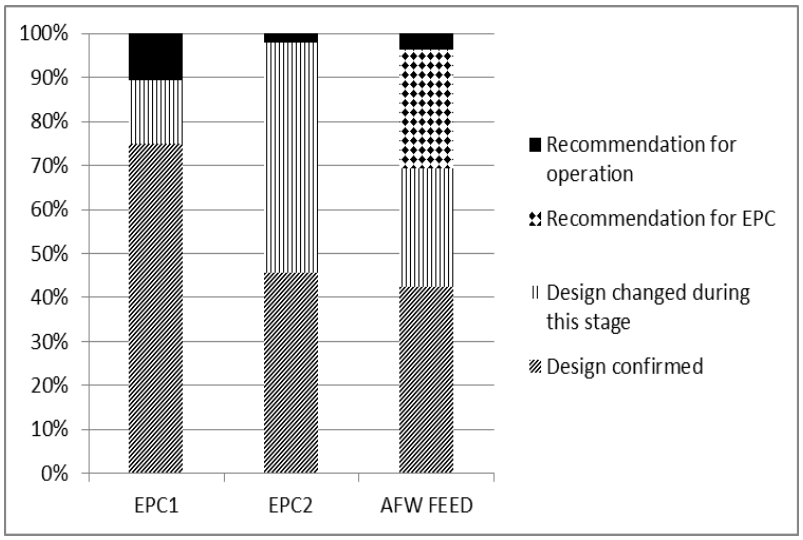
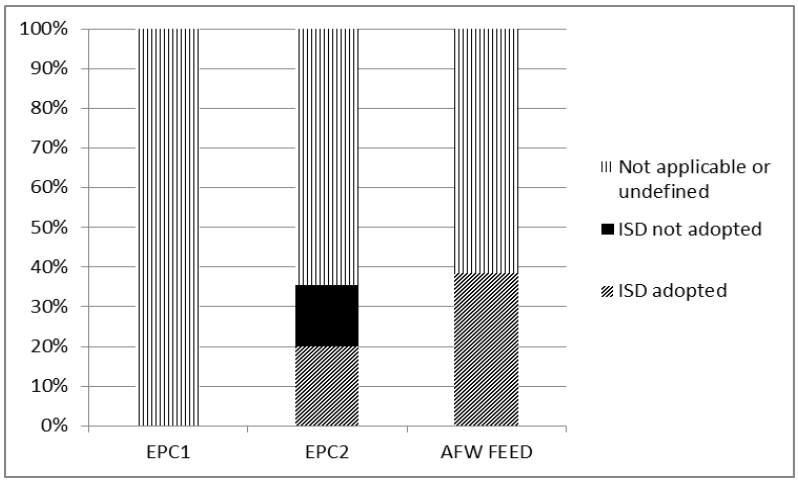


Figure 8. Comparison: Adoption of ISD



Conclusions

The study confirmed the value of using a simplified ALARP procedure to encourage design engineers to take account of ALARP and ISD principles in design decisions. The simplified approach can reduce duplication of effort both in redesign to back-fit safety features after a formal ALARP assessment, and also in identifying safety-related decisions made earlier in the design process to record them in the safety case. However, the simplified ALARP procedure needs to be supplemented by vigilance from the safety team to ensure it is used effectively.

The study confirmed that early consideration of ALARP and ISD, such as this approach encourages, allows greater use of ISD, rather than justifying later in the design process that inferior safety measures are ALARP. In most cases, a simple evaluation was found to be sufficient to demonstrate ALARP without recourse to detailed assessment such as CBA.

References

Hart, A, 2013, ALARP – Recent Developments, *ALARP: Learning from the Experiences of Others*, London: IMechE, 4th June 2013

HSE, 2001 Reducing Risks, Protecting People, HSE's decision making process, Liverpool: Health & Safety Executive

HSE, 2003 (b), Policy and guidance on reducing risks as low as reasonably practicable in design, Liverpool: Health & Safety Executive, http://www.hse.gov.uk/risk/theory/alarp3.htm

HSE, 2006, Assessment Principles for Offshore Safety Cases (APOSC), Liverpool: Health & Safety Executive, http://www.hse.gov.uk/offshore/aposc190306.pdf

HSE, 2015 (a), The Control of Major Accident Hazards (COMAH) Regulations 2015, Guidance on Regulations, Liverpool: Health & Safety Executive, L111 (Third edition)

HSE, 2015 (b), The Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015, Guidance on Regulations, Liverpool: Health & Safety Executive, L154 (First edition)

HSE, 2015 (c), Control of Major Accident Hazards Regulations 2015 (COMAH) Safety Report Assessment Manual (SRAM), Liverpool: Health & Safety Executive, http://www.hse.gov.uk/comah/sram/

HSE, 2016, Prevention of fire and explosion, and emergency response on offshore installations, *Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995, Approved Code of Practice and guidance*, Liverpool: Health & Safety Executive L65, (Third edition)

ISO 31000:2009, Risk management – Principles and guidelines, Geneva: International Organization for Standardization

Mansfield, D., Poulter, L. and Kletz, T., 1996, Improving Inherent Safety, Liverpool: Health & Safety Executive, *Offshore Technology Report*, OTH-96-521

Office for Nuclear Regulation, 2014, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0

Piper, D, Renwick, P, Morgan, J, Johnson, M, Lauder, R, Wicks, C, Spence, T and Borresen, R, 2014, Guidance on Risk-Related Decision-Making, 2nd edition, London: Oil & Gas UK

Renwick, P, 2013, ISD and ALARP in Brownfield Projects, *ALARP: Learning from the Experiences of Others*, London: IMechE, 4th June 2013