Cost-Effective Application of the ALARP Principle

Dr Simon Hughes, Senior Safety Consultant.
01372 367448, simon.hughes@era.co.uk.
Safety Engineering Group, ERA Technology, Cleeve Road, Leatherhead, KT22 7SA.

Keywords:
ALARP, Cost Benefit Analysis.

Abstract:
The ALARP (As Low As Reasonably Practicable) principle provides a means for assessing the tolerability of risk. In essence, it says that if the cost of reducing a risk outweighs the benefit, then the risk may be considered tolerable. The use of the principle is required by HSE guidance, Def Stan 00-56, POSMS (Project Oriented Safety Management System) and various safety JSPs. Hence, all MoD IPTs dealing with safety related equipment and processes must be able to apply the principle accurately and cost-effectively in the management of risk and safety.

However, although it appears simple, the ALARP principle requires significant interpretation and can be very difficult and costly to apply. This paper addresses these practical issues and describes a process for cost-effectively applying the principle that has been successfully trialled for the Apache AH Mk1. Specific problems that are addressed include complete identification of possible risk reduction methods, the potentially significant cost of determining the ALARP status of risks (before any actual risk reduction is achieved) and the application of the principle to software risks.
**Introduction:**

This paper describes a practical process for applying the ALARP principle to hazard and accident risks. It has been successfully trialled for the Apache AH Mk1. This paper does not consider the theoretical basis for the ALARP principle, or the contentious technical and ethical problems that surround it.

The process is based upon the advice given in the ADRP guidance (ref. 5) on Cost Benefit Analysis (CBA). It is intended to interpret and, in particular, extend that guidance as necessary to cover some of the practical issues that IPTs may experience in applying the ALARP principle. For example, the process addresses cost-effectiveness, asset valuation, complete identification of risk reduction methods, software risks, etc.

A brief introduction to the ALARP principle and its practical difficulties is given below, before the process is described. Important issues associated with the application of the process are then considered.

**The ALARP Principle**

The ALARP (As Low As Reasonably Practicable) principle provides a means for assessing the tolerability of risk. The definition of ALARP can be taken to be (this definition is based on the one in Def Stan 00-56, ref. 1, but is simplified):

> A risk is ALARP if the cost of any reduction in that risk is grossly disproportionate to the benefit obtained from the reduction.

This simple statement of the principle hides the philosophical and ethical contentiousness of the principle (which is not considered further in this paper) as well as the practical difficulties in applying it meaningfully and effectively.

**Why is the ALARP Principle Relevant?**

In spite of its widespread adoption in the UK as a means of assessing the tolerability of risk, the ALARP principle is not enshrined in UK law. However, the obviously similar SFAIRP (So Far As Is Reasonably Practicable) principle does appear in the Health and Safety at Work Act. Usually, ALARP and SFAIRP are considered to be equivalent, e.g. by the Health and Safety Executive (HSE), though it is not clear that this equivalence has been demonstrated in law.

In any case, use of the ALARP principle is mandated by the MoD itself, for example in Def Stan 00-56, AEMS POSMS and JSP 553 (refs. 1–3). Hence, all IPTs involved with safety-related equipment or services need to be familiar with the principle and need to be able to apply it.

In the case of the Apache AH Mk1 there are approximately 200 distinct hazards with associated risks that are considered to be in the “ALARP region” and, hence, subject to application of the ALARP principle. Consequently, the AH IPT needed a cost-effective method for applying the ALARP principle and requested assistance from ERA Technology in defining and trialling a process.
The Difficulties of Applying the ALARP Principle

There are significant practical difficulties in applying the ALARP principle. Firstly, to demonstrate that a risk is ALARP, it is necessary to demonstrate that all credible risk reduction methods are impracticable. To do this, it is clearly necessary to first identify all credible risk reduction methods. It is unlikely that a single individual working alone, even with the benefit of peer review, will have the necessary expertise and breadth of thinking to do this. Hence, the identification of risk reduction methods is considered a group activity (analogous to HAZOPS).

The second significant problem is that applying the ALARP principle fully and accurately can be expensive (this is just to determine the ALARP status of risks, not to actually reduce risks, e.g. by system redesign). This is because accurately determining the cost and benefit of risk reduction can be difficult and time-consuming. To counteract this, the process is designed in two stages. The first stage is intended to be a relatively inexpensive and quick assessment, designed to identify risks that can quickly and clearly be shown to be ALARP. Those risks that can not quickly be shown to be ALARP, either because they probably aren’t or because they are marginal, are then subject to the second stage of the process, which involves detailed costings and risk analyses.

The ALARP Process

For each risk, the following process is followed. This is just a summary of the process; there are many details and complications, some of which are considered below.

First stage (inexpensive and approximate)
1. Calculate detriment of risk.
2. Brainstorm risk reduction methods.
3. For each risk reduction method.
   a. Does the cost of this risk reduction method clearly exceed detriment calculated in step 1? If yes, discard risk reduction method. If no, add risk reduction method to list of potentially feasible methods.
4. Are there any potentially feasible risk reduction methods? If yes, go to step 5. If no, then risk is ALARP (and process ends).

Second stage (detailed and costly)
5. Determine accurate costs and benefits of feasible risk reduction methods.
6. Perform accurate CBA to determine risk reduction methods to be implemented.
7. Implement indicated risk reduction methods and reassess risk.
8. Is risk still in ALARP region? If yes, go to step 1. If no, then risk is ALARP (and process ends).

Steps 1 and 2 are considered in more detail below.

Calculate detriment of risk (step 1)

The following formula is used to calculate the detriment of an accident risk (it is similar to the formula in the ADRP guidance, ref. 5):

\[ \text{Detriment} = F \times L \times ((V_H \times D) + V_A) \]
where

- $F$ is the frequency of the accident per operational hour. This is already available from the detailed risk assessment performed for the Apache AH Mk1.
- $L$ is the remaining lifetime of the aircraft fleet (in aircraft hours). For the Apache AH Mk1, this is obtained by multiplying the number of operational aircraft (58) by the expected remaining lifetime (25 years) and the expected flying hours per year for each aircraft (300).
- $V_H$ is the valuation of the accident in terms of fatalities and injuries. This is calculated using the suggested values for the prevention of fatalities and injuries given in the ADRP guidance (ref. 5).
- $V_A$ is the valuation of the accident in terms of assets. Whether and how to value assets, such as an Apache Mk1, is a matter for individual IPTs to decide, e.g., according to the replacement or write-off policy for those assets. It is noted that inclusion of the assets value in the formula increases the detriment, making it more likely that the risk will be reduced, benefiting both humans and assets.
- $D$ is the disproportionality factor. The ADRP guidance (ref. 5) varies this between 1 and 10 according to the initial level of risk$^1$. In accordance with HSE guidance that risks should be reduced unless the cost is “grossly disproportionate” to the benefit, for the AH Mk1, the minimum disproportionality factor used for the Apache is 2. Additionally, HSE guidance dictates that the disproportionality factor should increase as the severity of the accident increases$^2$. Although it does not appear in the published guidance (ref. 5), ADRP’s recommendation is that the disproportionality factor should only be applied to $V_H$, not $V_A$.

By way of example, consider a catastrophic Apache accident involving the death of both aircrew and the loss of the aircraft with frequency $10^{-6}$ per flying hour. The detriment for this accident risk is:

$$10^{-6} \times (58 \times 25 \times 300) \times (((4,000,000^3 \times 2) \times 6^4) + 30,000,000^5) \approx £34,000,000$$

The £34M detriment is a theoretical maximum amount that must be spent to reduce the risk of the accident. If it is possible to significantly reduce the risk of the accident for less than £34M then before the risk can be declared ALARP, it must be reduced. This is only a theoretical maximum for two reasons. Firstly, it may be possible to reduce the risk for much less and, secondly, it may not be possible to significantly reduce the risk without spending more, in which case the risk is determined to be ALARP and nothing need be (can practically be) spent on reducing it.

---

$^1$ This is in accordance with HSE guidance but that guidance appears to be based on a single ambiguous legal statement. It is difficult to rationalize the guidance that the disproportionality factor should increase as the risk does, but it is “official” HSE guidance.

$^2$ This is not recognized in the ADRP guidance (ref. 5) but is easier to rationalize. It is based on research demonstrating that the public are less tolerant of high-severity accidents than multiple low-severity accidents, e.g. the research appears to demonstrate that the public is more tolerant of 100 single-fatality accidents than a single 100-fatality accident.

$^3$ £4M is the value for the prevention of a fatality suggested by the ADRP guidance (ref. 5).

$^4$ This “6” is an appropriate disproportionality factor to use for a risk that is in the middle of the ALARP region for the Apache AH Mk1.

$^5$ £30M is deemed to be the value of an Apache AH Mk1.
Brainstorm risk reduction methods (step 2)

A key aspect of demonstrating that a risk is ALARP is demonstrating that all credible risk reduction methods are impracticable. To do this, it is clearly first necessary to identify all credible risk reduction methods. It is not sufficient to only consider one or two, or those previously identified. To give some confidence that all credible risk reduction methods have been identified, the Apache ALARP process involves a brainstorming session with suitable safety, systems, aircrew, groundcrew, etc. experts. This brainstorming session centres on the accident sequence(s) for the accident in question. To successfully identify potential risk reduction methods, it is necessary to fully understand the accident sequence, including root causes, hazards, mitigations and controls. The brainstorm is aided by a list of generic risk reduction methods (a very long list is given in the ASEMS POSMS procedure on risk reduction (ref. 2), but it may require consolidation since it may be too long to be of direct practical use).

Other Issues

Common Cause Failures

In the above example, the ALARP principle was applied to a particular accident risk. It can be applied to other, different kinds or levels of risk, e.g. to the risk of a whole aircraft. This is the approach implied in the ADRP guidance (ref. 5) and mirrors the way the principle was originally applied to whole systems in the oil and gas industries. However, many IPTs, including AHIPT, do not have a particularly accurate understanding of the overall risk of operating their aircraft but do have very detailed accident and hazard risk analyses. Fortunately, the ALARP principle can be applied at the level of subsystems, accidents or hazards (or even causes). Unfortunately, this introduces the significant complication that certain risk reduction methods can address multiple risks. This makes it difficult to determine that a particular risk is ALARP because a risk reduction method that is impracticably expensive in the context of that single risk may be very practicable in the context of the overall system.

For the Apache, the most common example of this situation arises from the contribution of software to risk. Certain Apache softwares, e.g. the System Processor, contribute to many hazards, many of which have risks in the ALARP region. Consequently, increasing the integrity of the software, though expensive, will reduce the risks of many hazards. Considered in the context of any individual hazard, that cost may be impractically high but considered in the context of all the hazards, it will often be obviously practicable.

Whenever the ALARP principle is applied at a level beneath that of the overall system, this sort of common-cause failure effect needs to be taken into account to ensure that risks are not erroneously determined to be ALARP.

Software Risk Reduction

Most techniques, e.g. static analysis, testing, etc., for addressing a lack of required safety evidence for software are actually risk assessment techniques, rather than risk reduction techniques. Consequently, the techniques, in themselves, carry no direct benefit in terms of risk reduction. The risk reduction benefits only come from fixing the software faults that the techniques identify. Since it is not possible in advance to predict how many software faults will be identified, it is not possible to accurately estimate how much it will cost to fix the faults. The cost can vary from zero, if no faults are identified, to the cost of completely redeveloping the
software if it proves to be so riddled with faults that it needs to be scrapped. Since the ALARP principle demands estimation of the cost of risk reduction, it is not immediately obvious that it can be applied to software.

For Apache, as with many CotS and legacy systems, the problem with software is not that it is known to be unsafe but that there is insufficient evidence to demonstrate that it is safe (there is a lack of evidence of safety, not evidence of a lack of safety). Consequently, pessimistic assumptions are made in assessing the safety of the software. This, in turn, means that more detailed risk assessment can be, effectively, a means to reduce the (estimation of) risk since it will allow the pessimistic assumptions to be relaxed.

For the Apache ALARP process, to apply the ALARP principle to software risks, an implicit assumption is made that any software risk assessment techniques (e.g., static analysis) will find no software faults, demonstrating that the software is of high integrity and thus allowing pessimistic risk assessment assumptions to be relaxed. Hence, it is only necessary to estimate the cost of the software analysis, rather than the cost of fixing any discovered faults. This implicit assumption errs on the side of increasing safety because it makes it more likely that software risk assessment followed, if necessary, by risk reduction, will be done.

Unquantifiable Detriments

The valuation of accidents involving loss of assets is relatively uncontentious. The valuation of accidents involving fatalities and injuries is more contentious but at least a method exists. However, there are other kinds of accidents that present greater difficulties. The definitions of accident severities used in the Apache risk assessment process are, in part, derived from the failure condition categorizations in RTCA DO-178B. Hence, they include clauses associated with a decreased crew ability to maintain safe flight. For example, one of the clauses defining the “major” severity is “difficult for crew to cope with adverse operating conditions”. Since such circumstances involve no injury or loss of assets, it is difficult to attach a financial detriment to such “accidents”.

Any process for applying the ALARP principle to accident risks needs to be applicable to all the different classes of accidents included in the accident severity definitions.

Conclusion

The process, described above, for applying the ALARP principle addresses some of the major practical issues with ALARP. For example, it addresses cost-effectiveness, asset valuation, complete identification of risk reduction methods, software risks, etc. The process has been successfully trialled on several hazard risks for the Apache AH Mk1. It should be readily adaptable for use by other IPTs to help in the management of their hazard and accident risks.

Acknowledgements

The assistance of AHIPT, Westland Helicopters and QinetiQ in trialling the ALARP process is gratefully acknowledged.
References

3. JSP 553, Military Airworthiness Regulations, 1st Edition
5. Guidance for Applying Cost Benefit Analysis to Safety Decisions in Aviation Projects, ALTG/06/10/07, 28 Jan 05.

Biography

Simon Hughes, Senior Safety Consultant.
01372 367448, simon.hughes@era.co.uk.
Safety Engineering Group, ERA Technology, Cleeve Road, Leatherhead, KT22 7SA.

Simon Hughes graduated from Oxford University with a maths degree and moved on to Imperial College, where he was awarded his PhD, to research the theory of computation, static analysis and programming language integrity. In 1992, Simon joined Lloyd’s Register to take a leading technical role in the static analysis of the Sizewell B PPS software. Subsequently, he was also involved in the ESPRIT CASCADE project, designing a Software Conformity Assessment Scheme, the static analysis of the Jaguar XJ8 electronic throttle software and the Hercules C-130J software static analysis and avionics safety cases.

In 1997, Simon joined RPS consultants where he was a safety consultant to the UK TACC and the software ISA for SHOLIS. In 1998, Simon joined his current employers, ERA Technology. Since joining ERA, Simon has been an ISA to the Apache AH and FsAST IPTs, assisting in many aspects of risk management and safety. More recently, he has also been appointed as ISA to the Chinook and Sentry IPTs. He also contributes in many other areas, e.g. POSMS and ALARP for the Hercules IPT, safety assurance for Ford and Jaguar cars, etc.