Experiences in ALARP Demonstration

A.G. Rushton, Principal Consultant, M. R. Finch, Consultant,

ESR Technology, 202 Cavendish Place, Birchwood Park, Warrington, WA3 6WU, UK

Under the Control of Major Accident Hazard (COMAH) Regulations, "Every operator must demonstrate to the competent authority that it has taken all measures necessary as specified in these Regulations". This is interpreted as a requirement to demonstrate that risks have been managed, by implementation of suitable risk reduction measures, to As Low As is Reasonably Practicable (ALARP).

The requirement extends to a broad range of activities in scope of COMAH, but, except that it requires the dutyholder to share their thinking with the regulator, the requirement does not add greatly to the duties applicable to comparable non-COMAH sites.

The findings of a risk assessment, together with the appropriate preventative and mitigation measures, will usually provide sufficient evidence to demonstrate safe operation. Nevertheless, there is still much debate about what an ALARP demonstration looks like (How long is a demonstration? What are the essential elements?).

This paper shares experience of supporting dutyholders in presentation of ALARP demonstrations, in a COMAH context or otherwise, and highlights the roles of:

- Codes and standards;
- Design philosophy and basis of safety for management of residual risks;
- Hierarchy of risk reduction measures;
- Reasonable practicability evaluation.

Ultimately, the requirement is to provide reasonable answers to reasonable questions that, in the case of major hazard control, need to be aired with the regulator on behalf of the public. Inevitably, there is a degree of variation in how deeply any party to the discussion believes these questions and answers should be explored in the specific demonstration and how much the demonstration can rely, implicitly or explicitly, on reference out to other sources.

A “road map” is presented to help dutyholders understand the way to meet expectations of all stakeholders when developing ALARP demonstrations.

The discussion will focus on the high-level approach that should provide initial proportionate assurance to the dutyholder and regulator (though may be subjected to testing in depth in due course).

Keywords: COMAH; Seveso; ALARP Demonstration; Risk Reduction Measure; Basis of Safety; Good Practice.

Introduction

This paper shares experience of supporting dutyholders in presentation of “ALARP demonstrations” (i.e. demonstrations that risk has been reduced so far as is reasonably practicable), in particular in relation to major hazard control. The background section provides context for the discussion by reference to milestone major accidents that have shaped the requirements for major hazard control, and by reference to UK legislation that frames the expectations for “ALARP demonstrations”. A brief account of the ALARP concept, its place in relation to COMAH and the consequent expectation of ALARP demonstration in COMAH follows. An account of the experience base for ALARP Demonstration, drawn upon here, is presented. Features of ALARP demonstration documentation are discussed. Key elements of ALARP Demonstration are discussed, highlighting their roles. Finally, a "road map" to ALARP demonstration is presented summarising the main topics discussed and their relationships.

Background

Control of Major Accident Hazards

This paper is focused on major hazards of fire, explosion and toxic release arising from oil, gas and chemical process industries. Specific controls for other industrial major hazards (e.g. nuclear, explosives), or natural major hazards, are not discussed.

Milestone Major Accidents - Flixborough and Seveso

In Great Britain, the approach to control of major hazards was profoundly influenced by a disastrous explosion at a chemical plant at Flixborough in 1974 (Parker, 1975). The plant was destroyed, 28 workers were killed and there was extensive damage to property off site. Following that accident, a committee of experts, the Advisory Committee on Major Hazards, was appointed by the then Health and Safety Commission to consider the problems of major accident hazards and make recommendations. They proposed a three-part strategy:

- Identification of the sites;
- Control measures to prevent major accidents; and
- Mitigatory measures to limit the effects of any accidents which could occur.

Several other major accidents occurred in Europe during the 1970s, the most significant of which took place in Seveso, Italy, in 1976. At Seveso, the accidental production and release of a dioxin, as an unwanted by-product from a runaway chemical reaction, led to widespread, persistent contamination. Such incidents, and the recognition of the differing standards of controls over industrial activities within the European Community, led the European Commission to propose a Directive on the control of major industrial accident hazards. The three-part strategy proposed in the UK was highly influential in shaping the Directive.

The first European Directive on the Major Accident Hazards of Certain Industrial Activities (82/501/EEC) was adopted on 24 June 1982, and is generally known as the Seveso Directive. The current (2012) Directive is known as Seveso III.

Current UK Major Hazards Legislation

The Control of Major Accident Hazard (COMAH) Regulations 2015 (HSE, 2015) implement the majority of the Seveso III Directive (2012/18/EU) in Great Britain. The land-use planning requirements from the Directive are implemented through planning legislation and are not discussed here.

Under the COMAH Regulations:

- "Every operator must take all measures necessary to prevent major accidents and to limit their consequences for human health and the environment." (Regulation 5 (1)); and
- "Every operator must demonstrate to the competent authority that it has taken all measures necessary as specified in these Regulations" (Regulation 5 (2)).

HSE makes no distinction between what is implied by "take all measures necessary" in the COMAH context, what is required to ensure health and safety so far as is reasonably practicable (SFAIRP), or what is required to reduce risks to As Low As is Reasonably Practicable (ALARP); all call for the same set of tests to be applied (HSE, Undated-1).

The guidance for Regulation 5(1) includes "Prevention should be considered in a hierarchy based on the principles of reducing risk to a level as low as reasonably practicable (ALARP)."

Regulation 5 (2) is generally interpreted, therefore, as a requirement to demonstrate that risks have been managed, by implementation of suitable risk reduction measures, to ALARP. From this point on, here, the phrase "ALARP demonstration" is used to label the demonstrations required by COMAH Regulation 5 (2).

Related UK Legislation

The COMAH Regulations are "Relevant Statutory Provisions", as referred to in the Health and Safety at Work Act (UK Government, 1974). That Act places a duty on employers to effectively:

- "ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees." (Section 2); and
- "ensure, so far as is reasonably practicable" the health and safety of persons not in his employment" (Section 3).

The Management of Health and Safety at Work Regulations (UK Government, 1999), which are also Relevant Statutory Provisions under the Act, and which are of wide applicability, require:

> "suitable and sufficient assessment of ... the risks";

and, in specified circumstances, require the employer to

> "record ... the significant findings".

The significant findings should typically include:

- The preventive and protective measures in place to control the risks;
- What further action, if any, needs to be taken to reduce risk sufficiently;
- Evidence that a suitable and sufficient assessment has been made.

HSE offer a template for such records (HSE, 2014-1) which focuses on:

- What are the hazards?
- Who might be harmed and how?
- What are you already doing?
- Do you need to do anything else to control this risk?
- Action by who?
- Action by when?
- Done [i.e. "closed out"].

The related Approved Code of Practice (HSE, 2000-1, withdrawn 2013) stated that:

> "in the majority of cases, adopting good practice will be enough to ensure risks are reduced sufficiently".

Guidance that is still current does, however, state that:

> "In the great majority of cases, we can decide by referring to existing 'good practice' that has been established by a process of discussion with stakeholders to achieve a consensus about what is ALARP. For high hazards, complex or novel situations, we build on good practice, using more formal decision making techniques, including cost-benefit analysis, to inform our judgement." (HSE, Undated-2); and
>
> "in high hazard situations … where the circumstances are not fully within the scope of the good practice, additional measures may be required to reduce risks ALARP." (HSE, 2003).

In summary, the requirement is for a documented ALARP position for each scope of activity within an undertaking (including but not limited to COMAH activities).

At shortest the documented position will claim:

- The scope of activity falls entirely within scope of relevant good practice (RGP); and
- The RGP is being followed.

As necessary, and at longest, the documentation will:

- Review coverage of the activity by RGP;
- Adopt RGP to the extent relevant and, for new RGP that is not prescribed, close any gaps SFAIRP;
- Explore options for additional risk reduction measures (RRM);
- Adopt additional measures (wherever reasonably practicable, RP) or justify (by proportionate argument) non-adoption of measures.

ALARP

Much of the UK Health and Safety regulation relies on the concept of reducing risk SFAIRP either explicitly or (as in the case of "all measures necessary" in COMAH) implicitly. Where regulation is prescriptive, however, the question of whether what is prescribed is or is not more than required to reduce risk to ALARP is not relevant. Generally, prescription is used only where considered necessary to establish no doubt of practices that are considered to reduce risk to ALARP.

A full discussion of reducing risk to ALARP is outside the scope of this paper. However, Reducing Risks Protecting People ("R2P2") provides a high-level review of the concept and how it influences HSE's decisions (HSE, 2001).

ALARP in COMAH

The role of ALARP in COMAH has been discussed elsewhere. Rushton and Reston (2006), argued that as ALARP has been the cornerstone of "goal-setting" safety legislation (including but not limited to major hazard control) since 1974, the requirement to establish risk control SFAIRP is not new, and the requirement to document that control (i.e. set out the elements of an ALARP demonstration) has been established for all but the smallest undertakings since 1999. In other words, the controlling mind of an undertaking has had the duty to assure itself that risk is managed to ALARP since 1974 and to document that assurance since 1999. The only "new" requirement in the COMAH context is that the expression of that assurance must be presented to the "competent authority" (HSE and the relevant environment authority) as ALARP demonstrations.

As, in most cases, COMAH regulated sites are substantial, complex, undertakings, it is normal for the dutyholder (normally the operator of the site) to be organised (e.g. into operations, safety, technical "limbs") in such a way that the self-assurance of the dutyholder, consistent with good corporate governance, would inevitably require documentation and communication internal to the dutyholder. From a corporate point of view, major hazard risks are among many operational and other risks that have to be managed. Essentially, COMAH requires dutyholders to share oversight of their self-assurance process with the competent authority. The COMAH report will provide a "snapshot" through a "window" to the self-assurance process/documentation of the dutyholder. Ideally, the dutyholder will maintain the safety report as a "living document" between submissions to the competent authority ("keeping the camera rolling" as part of their internal process).

ALARP Demonstration in COMAH

The COMAH requirement for ALARP demonstration extends to a broad range of activities in scope of COMAH, but as explained in the ALARP discussion above, except that it requires the dutyholder to share their thinking with the regulator, the requirement does not add greatly to the duties that would have been applicable had the undertaking been categorised as a non-COMAH site, but was otherwise comparable.

This view is confirmed in the guidance to the current COMAH Regulations (HSE, 2015, paragraph 92):

> "The findings of a risk assessment carried out to comply with regulation 5(1) (as well as the general regulation 3 requirement for risk assessment of the Management of Health and Safety at Work Regulations 1999 (MHSWR), and similar requirements in environmental legislation), together with the appropriate preventative and mitigation measures will usually provide sufficient evidence to demonstrate safe operation."

Nevertheless, there is still much debate about what an ALARP demonstration looks like (How long is a demonstration? What are the essential elements?).

Experience Base for ALARP Demonstration

This paper shares experience of supporting diverse dutyholders in presentation of ALARP demonstrations. The focus here is on COMAH (which explicitly sets out requirements that can be met by ALARP demonstration) and the case studies mentioned here are drawn from COMAH controlled activities. However, the experience informing this paper is wider, including:

- Existing COMAH establishments;
- Design of new installations at existing COMAH establishments;
- Seveso (but non-UK) installations;
- Design of new offshore oil and gas installations (UK and non-UK);
- Operation of existing offshore oil and gas installations (UK and non-UK);
- Non-EU onshore installations (where the operator and/or regulator seeks risk reduction ALARP);
- UK undertakings not controlled by COMAH.

Suitable and sufficient risk assessments documented to meet requirements of MHSWR are scoped to match the expectations of ALARP demonstrations. So, the insights gained in relation to COMAH ALARP demonstration, as presented here, have wider applicability (not limited to COMAH sites or activities).

Documentation

Features of ALARP demonstration documentation are discussed here, in particular the benefits of a documented ALARP position and the essential elements of the documented position.

Documentation - Benefits

Benefits accrue from a documented ALARP position. The benefits include:

- Helping to formalise and communicate engineering support / judgement for:
  –management approval,
  –internal review (as changes arise),
  –external review (by regulator or other stakeholders);
- Helping to deal with "groundhog-day" questions from new stakeholders
- Potentially providing evidence for an "ALARP" defence.

Communication of engineering positions is a necessary part of any undertaking and, to the extent that those positions have a role in ALARP decisions then clarity of the position and access to it by decision makers is indispensable.

Newly inducted personnel (internal or external) tend to raise the same ("groundhog-day") questions (whether about the plant, procedures or personnel) that have been addressed many times before – with potential for significant wasted time and effort if the historic position is inadequately documented.

Should a major accident occur (or should a pre-emptive prosecution be attempted), the dutyholder may need to prepare a defence that aims to show that all reasonably practicable measures had been taken. Such a defence would have to stand in the context of Section 40 of the Health and Safety at Work Act (UK Government, 1974):

> "In any proceedings for an offence under any of the relevant statutory provisions consisting of a failure to comply with a duty or requirement to do something so far as is practicable or so far as is reasonably practicable, or to use the best practicable means to do something, it shall be for the accused to prove (as the case may be) that it was not practicable or not reasonably practicable to do more than was in fact done to satisfy the duty or requirement, or that there was no better practicable means than was in fact used to satisfy the duty or requirement."

A documented ALARP position should provide the basis for such a defence.

Case Study:

A safety report shows the entire circulation of the document as:

1 the company HSE manager; and

2 the control room.

How did the controlling mind become aware of and "buy in" to the Safety Report (which directors read and approved)?

From this point of view, COMAH asks the dutyholder to "get their defence in first" by presenting all necessary measures (ALARP) demonstration in the Safety Report. A strict reading of Asquith's judgement (Asquith, 1949, discussed later) also suggests that only a defence prepared before the fact (whether or not part of the Safety Report) will be of help to the defendant.

The best advice to dutyholders is, therefore:

1 Do not have accidents;
2 Use ALARP considerations to help avoid accidents;
3 Make clear (to the controlling mind) what you rely on to avoid accidents -
  Facts (including facts about the hazards in scope of the undertaking),
  Plant (including plant configuration, design, installation, maintenance),
  Staff (including competence, training, management of human factors),
  Procedures (ensuring the assumed relationships between all of the above);
4 Prepare demonstrations, on the basis of the above, that are robust as evidence that all RP RRMs are in place.

Documentation - Key Features

Building on the HSE template for risk assessment records already discussed (HSE, 2014-1), key features that should be covered in the documentation are:

- Set the scope;
- Bring forward information from previous assessments;
- Capture existing risk reduction measures and deal with gaps from good practice;
- Capture the "before" risk view;

- Where proportionate, contemplate further risk reduction measures and generate a list of prospective risk reduction measures;
- Taking account, normally qualitatively, of the costs (strictly "sacrifice ...") and of the benefits (risk reduction achievable) decide upon measures (with attributed timescale, responsibility ...).

Gadd et al. (2003) have authoritatively discussed pitfalls in risk assessment which are to be avoided in risk assessment and, therefore, to be avoided in ALARP demonstrations. Anyone preparing documentation for ALARP positions needs to be wary of those pitfalls.

Key elements of ALARP Demonstration

The following sub-sections highlight the roles in ALARP demonstration of key elements informing the demonstration (Rushton and Reston, 2006):

- Codes and standards;
- Design philosophy and basis of safety (for plant, people and procedures) for management of residual risks;
- Hierarchy of risk reduction measures;
- Reasonable practicability evaluation.

Codes and Standards

If there is RGP (including but not limited to recognised industry codes and standards) covering the full scope of the activity under consideration, then further work to find and implement additional potential RRMs may be considered disproportionate.

Design philosophy and basis of safety

For a new design, the philosophy for achieving safe operation, including the basis of safety, should be explicitly stated in the design documentation. This will cover all relevant hazards but, in particular should cover hazards that are “resident” following the high level design choices. A “resident” hazard, in this context, is one which has not been eliminated by the high level design choices, and typically, therefore, the active management of resident hazards will have been a specific goal in the detailed design (Mannan, 2005). For example, the chosen suitable materials/means of containment may rely on:

- Exclusion of water;
- Maintenance of temperature above a process fluid natural boiling point;
- Avoidance of hydraulic shock;

with commensurate design detailing, to exclude water, prevent depressurisation, or avoid shocks accordingly.

Resident hazards may include, for example:

- The accepted potential for toxic effects consequent on selecting a toxic solvent; or
- The accepted potential for polymerisation inherent in the choice of a chemical route that includes a monomer that may, given time or other unintended conditions undergo polymerisation.

However, much of the “basis of safety” design of existing plant (or packages, sometimes referred to as “legacy systems”) is not explicitly documented. Rather, the facts of the documentation and the plant, people and procedures in place imply the basis of safety that was in the mind of the designers. Clearly, in all cases, one supposes that there was a time at which the designers believed that all necessary measures (as perceived at that time) were in place. Nevertheless, for legacy systems, it can be quite challenging to show that:

- Implicit evaluation was correct and defendable at the time;
- Since that time, changes in plant, people and procedures do not justify changed measures; and
- Changes in available technology and prices do not justify changed measures.

“Basis of safety” is a phrase predominantly used in relation to the design and operation of acceptably safe chemical reaction processes (Barton and Rogers, 1997, HSE, 2000-2 and HSE, 2014-2). More broadly, however, “basis of safety” refers to the specified safety measures, compatible with the engineering, production, economic and commercial criteria for the process (Gibson et al. 1987). Gibson et al. emphasised the need for these measures to be recognised by plant operators, and to be implemented and maintained (there are parallels with safety critical elements in an offshore context). For many parts of the industry, the basis of safety is so consistent that the term may not have much currency.

Examples of where variation in the basis of safety may be found include:

- Reactor cooling (high reliability systems, auxiliary systems);
- Reactor “killing” (dumping, injecting, “crash” cooling);
- Overpressure protection (containment, relief);
- Transit though flammable limits (inerting to avoid, elimination of ignition sources).

The choice will often depend on the scale, complexity and detail of the process.

Explicit statement of the basis of safety (even if it is normal practice for that type of activity) is generally a good starting point for discussion.

Statement of the basis of safety will typically require (Haight, 2013):

- A brief description of the process;
- A list of the process substances and their hazards;
- A list of the process hazards, their causes and consequences;
- The safety objectives that must be achieved to operate safely;
- The safeguards implemented to achieve the safety objectives;
- The safe operating envelope.

Case study:

A reactor loop is monitored for oxygen content and reactant content (fuels).

The Regulator infers – from discussion and review of available documentation - that maintenance of fuels above upper flammable limit in the reactor loop is the basis of safety and challenges the non-safety-related status of reactant concentration monitoring.

The Dutyholder confirms that maintenance of oxygen below minimum oxygen concentration for combustion is the basis of safety, confirms therefore the safety-related status of oxygen concentration monitoring, but establishes the operability status (only) of the reactant concentration monitoring.

For many common situations the basis of safety is implied or assumed in guidance (including much HSE guidance and RGP). However, the dutyholder is normally free to consider, in all the circumstances of their undertaking, what is the appropriate basis of safety to be adopted.

Complications linked to the basis of safety can also arise where technology (whether process technology or risk reduction measures technology) is associated with intellectual property rights.

Generally, it is not the role of the Regulator to eliminate all but one technology option whether by:

- Identifying a most inherently safe process technology (for a particular process); or by
- Identifying a most effective risk reduction component (for a specific risk reduction measure element).

Either behaviour would not only take the Regulator into a prescriptive position (which may prove false or become outdated) but would also be anti-competitive. Rather, the assumption is that any process technology or component of a risk reduction measure (that is not otherwise unsuitable) can be implemented in a context where risk is reduced ALARP (along with additional measures if necessary).

It follows that when a dutyholder is choosing a licensed process or a patented component for a risk reduction measure then they are not wholly constrained in their choice, though in principle if they do not select the intrinsically "best" option they may be required to adopt commensurate additional measures. The ALARP question becomes: "given my choice of process/component, is there more that I need to do to reduce risk SFAIRP?". The "time and trouble" element of any measures which compromise the terms of the licence for a process technology may become substantial in the balance of what more can be done.

In summary, the basis of safety adopted helps to identify the safety critical plant/people/procedures that will inform the scope of the ALARP demonstration. Some scopes are covered well by standards and regulation. Some scopes need to be explicit (depending on the specific philosophy adopted for pressure relief, runaway reaction control etc.). Legacy systems can present particular challenges when articulating the basis of safety and aligning this with expectations (e.g. in modern RGP).

Hierarchy of Risk Reduction Measures

The idea of a hierarchy of measures, and the associated idea of preferring inherently safer solutions, embody the old adages:

- Prevention is better than cure – it is more desirable and often easier to stem a cause than a consequence; and
- A stitch in time saves nine – the complexity and cost of dealing with features of a design that have been allowed to become established often exceeds the cost of designing out the feature or its effects at the earliest opportunity.

There are many published hierarchies of risk reduction. At a high level they are broadly consistent, but their details are variable and to some degree, therefore, are inconsistent.

An example of a simple, high level, hierarchy, used in the COMAH context (HSE, 1999), is:

- Inherent safety;
- Prevention;
- Control;
- Limitation/mitigation.

A more detailed hierarchy is implied in the Dangerous Substances and Explosive Atmospheres (DSEAR) Regulations (Regulation 6, HSE, 2013). There are many other hierarchies which emphasise to a greater or lesser extent the importance of inherent safety, human factors or dependability of measures. The Management of Health and Safety at Work Regulations, for example, sets out General Principles of Prevention (in Schedule 1, as set out in Article 6(2) of European Council Directive 89/391/EEC).

The point of the hierarchy is not to prescribe which measure must be adopted, but to promote for early consideration the measures which are likely to be most effective. From a given starting position, potential RRMs can, in principle, be ranked by either cost effectiveness (change in risk per unit sacrifice attributable to the measure) or by risk effectiveness (change in risk achieved by the measure) and those rankings will not necessarily be the same even in the shorter list of potential RRMs that are (from that starting point) reasonably practicable. In practice the uncertainties will blur the ranking of individual measures, but the use of a hierarchy does aid the early consideration of measures that are more likely to be risk effective.

Generally, measures that sit higher in the hierarchy will be:

- more dependable (capable and reliable or available, dependent on the role);
- less prone to error in design, installation and operation (e.g. leaving a trip "unarmed");
- more likely to have complete coverage (protecting against all realisations or more realisations of the hazard).

In other words, and most importantly, measures that sit higher in the hierarchy are less prone to failure of management (which, for a well-designed, installed and operated plant is the usual common cause of the collapse of whatever barriers were initially in place). However, this correlation of position in the hierarchy with risk reduction effectiveness is not absolute and a good ALARP review process is one which selects effective risk reduction measures (irrespective of the order in which the measures were considered).

So, in summary:

- The hierarchy used should be consistent with the high level promotion of prevention over control over mitigation (but the detail of the hierarchy is not prescribed and can be suited to the context of the work taking into account e.g. familiarity and precedence);
- The team using the hierarchy should be open-minded about whether an item sitting lower in the hierarchy may be more risk effective in all the circumstances.

In particular, the team should avoid dismissing items low in the hierarchy on the specious grounds that to adopt a "low" measure implies an admission that a "high" measure should have been adopted.

When identifying RRMs it is normal to decompose the problem to manage discussion (e.g. hazard by hazard, or activity by activity). In principle, however, each measure needs to be evaluated for all its benefits (not just those in scope of a discussion that has raised the measure as a potential step forward).

Reasonable Practicability Evaluation

Interpretation of the phrase "reasonably practicable" is informed by a decided case in which was stated (Asquith, 1949):

> "Reasonably practicable" is a narrower term than "physically possible" and seems to me to imply that a computation must be made ..... in which the quantum of risk is placed in one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them - the defendants discharge the onus on them. Moreover, this computation falls to be made ..... at a point of time anterior to the accident."

This judgement, and the context given to the application of the phrase in Health and Safety legislation places the emphasis on the dutyholder to seek reasonably practicable risk reduction measures and, if found, to implement those measures. There is general agreement that with modern approaches to plant, people and processes we are able (at worthwhile cost) to manage risk better than in the past. Holstvoogd et al. (2006), for example, have argued that incident rates have been driven down by successive waves of improvement in technology and standards, HSE management systems and safety culture.

The ALARP principle, and the goal-setting regime built upon it, recognises that opportunities to improve can arise from new technology, changes in operation, changes in costs etc. Whereas a prescriptive approach would have to be regularly revised to take advantage of these opportunities, the ALARP principle puts the onus on the dutyholder to scan, continually, for improvements that may have become reasonably practicable in the course of time or between one project and the next.

If we suppose that the level of risk achievable by reducing risk to ALARP, for a typical undertaking, can be represented as a falling function of time, then compliant positions are any positions below the curve. In reality, of course, progress will occur in steps (due to "breakthroughs" in technology). The real state of a particular undertaking will tend to stay at a level until some additional measure is introduced. The aim of a dutyholder should be to continuously be "ahead" of the ALARP balance (i.e. following a path below the ALARP curve). Because there is almost always a lag between prescription and compliance, a prescriptive regime would tend to lag the ALARP curve or else would insist on measures that are grossly disproportionate in cost. The management system must operate to

- Seek, sort and if appropriate adopt risk reduction measures to keep the undertaking continuously on the "right side of ALARP";
- Be sensitive to change (of plant, people, and process) by change management; and
- Be sensitive to external changes, learning from events, awareness of technical options etc.

ALARP decisions must be taken with an understanding of the balance defining reasonable practicability. However, most decisions are not (and should not be) determined simply by mechanistic application of a computational algorithm. Clearly, for example, it is undesirable to have ALARP evaluation processes that are over-sensitive to change (bearing in mind that costs

can go up and down). It would be a sign of oversensitivity if a small change in interest rates reversed an ALARP decision. The question of how far to go in bringing various information and analysis to bear on ALARP decisions is not simple. In the offshore context, for example, guidance (Oil and Gas UK, 2014) has been provided which helps to classify the type (and therefore proportionality) of the decision being taken and to ensure that suitable information and analysis is brought forward in support of the decision. However, further discussion of cost-benefit analysis and other detailed techniques in informing ALARP decisions is out of scope of this paper.

Kletz (1999) pointed out that increased possible spending on safety (from a low base) typically goes through four phases:

- Good Business (the likelihood of a return on the investment is high);
- Poor Business (there is a return on the investment, but not as high as on other investments);
- Bad Business - Good Humanity (money is spent so that people do not get hurt, but we do not expect to profit);
- Going Out of Business.

Normally the line to be drawn is between the last two phases. However, dependent on the nature of the undertaking, not all of these phases may arise. Major accident hazards vary in the extent to which events with potential for injury correlate with incidents with potential for loss of assets and business interruption. For fire and explosion hazards, the potential for loss of assets and business interruption is usually high (compared with toxic release and environmental pollution). With hindsight, it is often clear that positions the Regulator may press for as "Good Humanity" would in fact have been demonstrably "Good Business".

Ultimately, the requirement is to provide reasonable answers to reasonable questions that, in the case of major hazard control, need to be aired with the regulator (acting on behalf of the public). Again, this is not peculiar to COMAH (i.e. it is not fundamentally different from other interventions between the Regulator and dutyholders), but the Safety Report provides a means to focus these interventions. The need to promote these discussions for high hazard plants derives from the experience of Flixborough and Seveso where the public were surprised by the scope of the potential consequences of activities that were under the control of the dutyholder but where there was no more scrutiny than at sites with lesser potential. Inevitably, there is a degree of variation in how deeply any party to the discussion believes these questions and answers should be explored in the specific demonstration and how much the demonstration can rely, implicitly or explicitly, on reference out to other sources.

In other words, the test of the answers put forward in the ALARP demonstration lies in whether they bridge the gap represented by the expectations of the stakeholders (informed by the scale, complexity and novelty of the major hazards at issue). This idea of the ALARP demonstration (as part of the Safety Report) bridging the gap in the expectation of stakeholders suggests an analogy with bridge building.

The bridge analogy:

Making a demonstration is like bridging a river. The river is the major hazard. The span of the crossing is the technical and managerial challenge of being responsible for a major hazard.

The load the bridge must support is the individual and group dependence on success in meeting the challenge.

COMAH site operators – the bridge builders – have at their disposal all the raw materials. The bricks needed to build the bridge are many and varied – Safety Data Sheets, Piping and Instrumentation Diagrams, plant layout, equipment specifications, etc.

Reading some Safety Reports (not all, but many to some extent) one feels that the bridge builder has stood with their back to the river casting bricks over their shoulder so that the reader of the Safety Report can conclude that there is a pile of bricks in the river (there is a lot of raw material in the Safety Report).

Along comes the bridge inspector (the Competent Authority) and sees (in the Safety Report) the pile of bricks in the river. Will it bear the load they wonder? "I see no bridge" they say (unless the pile is high, the river is not wide, and the load is small, in which case they may walk away).

The bridge builder is upset by the bridge inspector's attitude: "What do you mean you see no bridge? Look at all the bricks. It took a lot of time and effort to lob those bricks in there. Some of those are state of the art gold-plated bricks. How many more bricks will it take?"

The Competent Authority scratches its head, and asks, again, for an account of why the bridge builder thinks the bridge is fit for purpose to span the bridge and carry the load.

To deal with the challenge, the bridge builder needs to

Face the river;
Estimate the span;
Estimate the load;
Show that the bricks, appropriately arranged and held together by a management system that is sensitive to change, is fit for purpose and is, crucially, to their own design (the "corporate mind" has satisfied itself that the design meets the company objectives including discharging their duties under the COMAH Regulations, the MHSW Regulations and the HSW Act).

The bridge inspector is there to ensure that only bridgebuilders capable of building suitable bridges carry on. However, crucially, the bridge inspector is not there to design the bridge (and may not be capable of doing so). A key aim of the goal-setting regime is to allow fit for purpose bridges to be built that a prescriptive regime might otherwise bar or under-specify, and to encourage a self-critical industry to avoid bridge designs that a purely reactive prescriptive regime might not have barred, but which would not take advantage of all reasonably practicable measures.

Inevitably, deciding when "enough is enough" will require consideration of:

- Technical limitations (what options for further or replacement measures are available);
- Cost implications (are the measures worthwhile);
- Logic (given the facts, the plant, the people, the procedures, the options, and the costs why are we content with the status quo – or, if not, how and when are we to change it).

If these elements of the information needed to assure risk reduction to ALARP are spelled out clearly then it becomes easier to:

- Review, from time to time, whether more needs to be done;
- Induct new stakeholders (internal or external) to the rationale of the status quo;
- Debate with stakeholders the rationale for any change.

Case study:

A COMAH Operator has embedded risk assessment into all aspects of their activities. At each opportunity, the team carrying out an element of the suite of activities aimed at managing major hazard risks is encouraged to consider and, as required for that activity, to evaluate:

- *Causes and their frequency;*
- *Consequences and their extent and severity.*

For some activities, these considerations are linked to a matrix offering classes of event frequency and severity. For other activities the consideration and evaluation may be divorced from matrix classes.

Frequency and consequence of a variety of scenarios is considered, and to the extent necessary evaluated, in:

- *Hazard Identification (HAZID);*
- *Hazard and Operability Study (HAZOP);*
- *Safety Integrity Level (SIL) determination:*
- *Hazardous Area Classification;*
- *Quantified Risk Assessment.*

Whereas the scenario scopes may vary, nevertheless it is likely that there will be qualitative and/or quantitative inconsistencies between these considerations. Perhaps, for example, the HAZID was used to "scope in" the items for further consideration, so may have taken a much more cautious/pessimistic view than is held later (e.g. when a similar scenario - or subset or superset of the scenario - is the subject of QRA). Given the different scopes (for scenarios in different studies) and different views (which may reflect best estimates of a particular team on a particular day), it may not be proportionate or practical to reconcile all of the evaluations explicitly. However, the resulting lack of coherence leaves open some interesting questions:

- *Which consideration/evaluation forms the basis of the opinion of the dutyholder that the residual risks are ALARP:*
  One superseding assessment (QRA?) which postdates and supplants all others (is this explicit in an ALARP workshop report or explicit in the Safety Report?)
  All of the assessments viewed in the round in relation to the ALARP question?
  Different assessments depending on the risk reduction measures at issue (e.g. the SIL study for Safety-Related System decisions, the (DSEAR) Hazardous Area Classification study for specification of electrical equipment in zones)?
- *How are inconsistencies managed:*
  Inconsistencies may not be actively managed – outcomes of each element may be taken at face value;
  Periodic review of one element may be informed by, but not overridden by, consideration of the outcomes of other elements (processes);
  Inconsistencies may be actively managed by iterating related processes to ensure an agreed, coherent, overarching view (at the expense of loss of "ownership" by the task-related teams).
- *How do changes (internal or external) trigger re-evaluations:*
  Systematically (management of change process includes triggers)?
  Periodically (management of change process calls for a cycle of reconsideration – refreshment of the elements)?
  Never (generally, this is not an acceptable answer).
- *How is comparison of assumptions underlying the elements tested (and how are conflicts, where identified, resolved):*
  Actively ("leading" indicators are monitored, experience internal and external is monitored to identify conflict with assumptions)?

Reactively (internal events that evidently conflict with assumptions are explored) – generally not an acceptable answer?

Without clarity on these points, there will be an inability on the part of external stakeholders (most importantly the regulator) to conclude what the "controlling mind" of the dutyholder had considered when concluding that residual risks are ALARP. It is clarity rather than consistency that is the main issue here. The record of a meeting where a team's views were recorded (e.g. at a qualitative HAZID) is not necessarily invalidated by another process (e.g. a QRA). It may or may not be that the team would reconsider their view in the light of the QRA information, it may or may not be that a decision maker chooses to rely more on the QRA than the HAZID. However, the decision and the basis for decision should be made clear.

By creating a culture where all can see and can (to the extent possible) agree that the dutyholder has "done enough", the dutyholder (and by intervening to achieve this, the Regulator, on the public's behalf) can avoid a culture where some assume that there is no interest in the question of whether enough has been done.

Once stakeholders (internal or external, but especially internal) believe there is no interest (attention from the controlling mind of the dutyholder) in the question of whether enough has been done, then this question is likely to be avoided and ignored with corrosive effect on the operation of the HSE management system. In other words, if a culture develops where there is no interest in the question of whether enough has been done, then the likelihood of suitable risk control measures remaining in place begins to fall. Good practice in development of ALARP demonstrations (including but not limited to cost-benefit analysis where appropriate) helps to achieve HSE's aim to create: "A culture in HSE that values the principles of risk assessment and management; and working practice that embeds proportionate and effective risk governance." (HSE, Undated-3).

Road Map to ALARP Demonstration

A "road map" can be set out to help dutyholders understand the way to meet expectations of all stakeholders when developing ALARP demonstrations. An early route to ALARP demonstration in the context of COMAH was given in the Annex to Rushton (2003). That paper posed the questions, to be answered in the Safety Report:

- How does the Operator perform hazard identification (HAZID) and what satisfies the Operator that this approach to HAZID is suitable and sufficient in all the circumstances of their business?
- How does the Operator estimate the frequency and consequences of potential major accidents?
- How does the Operator judge the overall risk position to be tolerable (or more rarely broadly acceptable)?
- How does the operator ensure that opportunities to take further measures are identified and reviewed appropriately?
- What justification does the operator have for not taking any practicable further measures and what satisfies the operator that this approach to justifying taking [or not] any further measures is suitable and sufficient in all the circumstances of their business?

A flowsheet, broadly consistent with the route in Rushton (2003), is given in HSE internal COMAH guidance as "ALARP Demonstration Flow sheet" (Figure 6 in HSE, Undated-1). That flowsheet is presented by HSE as one way of approaching ALARP demonstration but, as noted in that guidance, "HSE choose not to be prescriptive on how Dutyholders make their demonstrations that all necessary measures have been taken".

A "Road Map" to ALARP demonstration, summarising the discussion presented here is shown in Figure 1. As has been discussed, ALARP positions need to be updated from time to time in response to new information (new costs, new technology, new experience of incidents). The "Road Map" is not, therefore applicable once and for all but needs to be followed (with proportionate revision at each "turn") on a regular basis. The scope for using the "Map" will depend on how the undertaking has been broken down (e.g. by hazard, by activity) for the purposes of articulating ALARP positions (so a particular "journey" through the map may be broadly focused or narrowly focused). Normally there will be a raft of previous assessments (elaborating the basis of safety, taking into account established RGP at the point of design or of the last ALARP review) that needs to be brought forward to inform the new "journey". Based on that raft of information, and information about changes to RGP etc. that the dutyholder has accumulated, it will be possible to set down the current risk reduction measures and known potential gaps (which hitherto, by implication, have not been considered to be reasonably practicable to fill). This list should then be supplemented by a proportionate exploration of what more could be done, based on a suitable hierarchy matched to the needs of the dutyholder, producing a long-list of candidate risk reduction measures for evaluation.

In principle the next steps are the same, i.e. for each candidate:

- Evaluate risk before the measure; and
- Evaluate risk after the measure, and evaluate, by difference, the "quantum of risk" (i.e. benefits) at issue;
- Evaluate the cost (strictly the "sacrifice … (whether in money, time or trouble)");
- Sentence the measure for implementation (or not) based on the balance (and case specific view on "gross disproportion").

In practice, it is normal for the process to include some form of triage of the candidates to classify:

- Candidates which are considered to show no prospect of being reasonable practicability;
- Candidates which are "borderline";
- Candidates where the reasonable practicability (unless subsequently negated) can be assumed so that implementation (timing and responsibility) becomes the focus.

A short-list of “borderline” risk reduction measures is, therefore, taken forward for proportionate (more or less explicit and numerical) evaluation.

As a short cut, risk after the measure (in scope of the measure) is sometimes assumed to be zero (which shifts the balance in favour of adopting that measure).

In every case, however (with whatever high level or detailed analysis, as the case may be), the “controlling mind” should satisfy itself that wherever the cost (whether or not evaluated in detail) is not “grossly disproportionate” to the benefit (whether or not evaluated in detail). The process is highly analogous to sanctioning of projects, where for easy wins (or for hopeless proposals) a relatively shallow costing approach may be used to justify sanction (or not) but more detailed costing is needed for more borderline projects.

The decision point, where what is required is to sentence a measure for implementation (or not), informed by weighing the “cost” against the “benefit” is, in effect, the "computation" referred to by Asquith and is implicitly (though not always explicitly) a cost-benefit analysis with some appropriate case-specific bias in favour of implementation.

Conclusions

There is no prescription for the format or content of ALARP demonstrations. Rather, the demonstrations whatever their form, must meet the goals of effective communication of proportionate attention to the securing of reasonably practicable risk control measures. As each stakeholder may have a different view of whether and when these goals have been met, a degree of iteration in any discussion of ALARP demonstration is to be expected. Nevertheless, there are common features of ALARP demonstration, developed from a range of experiences, that have been reviewed here and from which a high-level “Road Map” to assist in ALARP demonstration has been developed.

ALARP demonstrations, given proportionate attention and documentation, provide dutyholders with the opportunity to communicate effectively with internal and external stakeholders, to respond efficiently and effectively to change and to stay on the “right side” of the ALARP balance as that balance shifts over time.

The discussion has focused on the high-level approach that should provide initial proportionate assurance to the dutyholder and regulator (though may be subjected to testing in depth in due course).

References

Asquith, Lord, 1949, in Edwards v. The National Coal Board (1949), 1 All ER 743.
Barton, J.A. and Rogers, R.L., 1997, Chemical Reaction Hazards (Second edition), Gulf Professional Publishing.
Gibson, N., Rogers, R.L. and Wright, T.K., 1987, Chemical Reaction Hazards: an integrated approach, Hazards from Pressure, IChemE Symposium Series 102, 61-84.
Gadd S., Keeley D. and Balmforth H., 2003, Good practice and pitfalls in risk assessment, RR151, HSE.
Haight, J.M., 2013, Handbook of Loss Prevention Engineering.
Holstvoogd R., van der Graaf G., Bryden R., Zijlker V. and Hudson P., 2006, Hearts and Minds Programmes the Road Map to Improved HSE Culture, IChemE Symposium No. 151 Hazards XIX, IChemE 2006.
HSE, 1999, Preparing safety reports: Control of Major Accident Hazards Regulations 1999 (COMAH), HSG 190, available at http://www.hse.gov.uk/pubns/books/hsg190.htm.
HSE,2000-1, Management of Health and Safety at Work Regulations Approved Code of Practice, 2nd Edition, L21, (withdrawn 2013).
HSE, 2000-2, Designing and operating safe chemical reaction processes, HSG143, available at http://www.hse.gov.uk/pubns/books/hsg143.htm.
HSE,2001, Reducing risks, protecting people, HSE’s decision-making process, ISBN 0-7176-2151-0, available, and supported by a suite of associated guidance, at http://www.hse.gov.uk/risk/theory/r2p2.htm.
HSE 2003, Assessing compliance with the law in individual cases and the use of good practice, available at http://www.hse.gov.uk/risk/theory/alarp2.htm.
HSE, 2013, Dangerous Substances and Explosive Atmospheres, HSE ACoP, L138 (Second edition).
HSE 2014-1, Risk Assessment and Policy Template, available at http://www.hse.gov.uk/toolbox/managing/managingtherisks.htm.
HSE 2014-2, Chemical reaction hazards and the risk of thermal runaway, INDG254, available at http://www.hse.gov.uk/pubns/indg254.pdf.
HSE, 2015, The Control of Major Accident Hazards Regulations 2015, Guidance on Regulations, L111.
HSE, Undated-1, Guidance on ALARP Decisions in COMAH, SPC [semi-permanent circular]/Permissioning/37, Version 3, available at http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/.
HSE Undated-2, ALARP "at a glance", available at http://www.hse.gov.uk/risk/theory/alarpglance.htm.
HSE, Undated-3, HSE principles for Cost Benefit Analysis (CBA) in support of ALARP decisions, available at www.hse.gov.uk/risk/theory/alarpcba.htm.
Kletz, T.A., 1999, HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards, 4th Edition, IChemE.
Mannan, S., 2005, Lees' Loss Prevention in the Process Industries, 3rd Edition, 30-72, Butterworth Heinemann.
Oil and Gas UK, 2014, Guidance on Risk Related Decision Making Issue 2.
Parker, R.J., 1975, The Flixborough Disaster - Report of the Court of Inquiry, Department of Employment, available through https://www.icheme.org/communities/special-interest-groups/ .
Rushton, A.G., 2003, Key Elements of Risk Decisions in the Control of Major Accidents Hazards, Hazards XVII, IChemE Symposium Series No. 149, pp 773-784, IChemE.

Rushton A.G. and Reston S.D., 2006, CBA, ALARP and Industrial Safety in the United Kingdom, Journal of the Safety and Reliability Society, 26(3): 24-33.
UK Government, 1974, Health and Safety at Work etc. Act 1974, available at https://www.legislation.gov.uk/ukpga/1974/37.

UK Government, 1999, The Management of Health and Safety at Work Regulations 1999, available at http://www.legislation.gov.uk/uksi/1999/3242/made.

Figure 1: A "Road Map" to ALARP Demonstration