Model Code for the Management of Risk Issues
The Institution of Chemical Engineers

Martin Goose FIChemE CEng

Model Code for the Management of Risk Issues
The Institution of Chemical Engineers

Introduction

In May 2007 the Institution of Chemical Engineers published its 'Roadmap for 21st Century Chemical Engineering' outlining the beneficial contributions that chemical engineers could make to society over the years ahead. The section of the roadmap that deals with the topic 'Health, Safety, Environment and Public Perception of Risk' proposes the production of a model code for risk management. This document presents a 'model' of how major hazard risks in the *process industries* should be managed in the context of the UK regulatory system. Many of the principles of this model can be applied internationally, and in other topic areas where risk management is required.

Risk Management

Risk management is a process that we are all applying continuously throughout our lives, although most of us would not necessarily describe it using those words. From the moment we are born we face *hazards* that might cause us *harm*. Some *hazards* are recognised instinctively but others need to be learnt. Initially we have others to care for us, but as we grow older the task of risk management, for that is what it is, passes progressively to become our own responsibility. In turn we have the responsibility to pass on those skills to the next generation.

Although we think first about hazards that might cause us the physical harm of injury or illness, the concept of risk management also applies in other areas such as managing our money, particularly savings and investments. Although only risk management specialists might actually say it, it is not too far fetched to say that life is one long risk management exercise.

In all situations we are seeking to obtain a benefit of some kind, and in order to obtain that benefit there is a possibility that the results of our actions lead to a mishap that causes us harm rather than to the beneficial outcome that we hoped for. We are inclined to take the action to gain the benefit if we judge that the value of the benefit outweighs the negative aspects of the potential harm. When weighing up the negatives we take account of both how bad the potential harm would be and also how likely it is that the harm will be felt.

In our own lives, valuing the benefits and weighing them against the potential harms is a very personal matter. We each have our own *attitude to risk* that we apply, and society generally allows us to get on with making our own life choices.

Public Risk Management

When we start to think about major hazard risks in the process industries, we are in a situation where many people may be affected. Benefits may accrue to one group of people but the potential harms could affect a different group. It is clear that individual risk/benefit balances may be in conflict and that it is necessary to move from a personal risk attitude basis to an aggregated public risk attitude basis (and one that commands the widest possible support).

In the UK, the public attitude to major hazard risks in the process industries is defined by society's elected representatives in Parliament, supported by a wide range of experts and in consultation with those who may benefit or be harmed. The framework for major hazard risk management is incorporated into legislation and the UK Health and Safety Executive (HSE) is empowered by Parliament to regulate the operation of major hazard installations to ensure that they comply with the legislation.

Put simply, the HSE's task is to provide assurance to the public and Government that the industries that it regulates are managing risks in an appropriate way. In order to do this it is given the power to make inspections, investigate accidents, and take enforcement action, including prosecutions, where corrective action by companies is required. It is impractical to describe all the details of major hazard risk management in the UK process industries in such a short document, but in summary, it consists of three basic steps.

- step one requires the *duty holder* to apply the safety experience accumulated so far in the process industries.
- step two reflects the fact that many hazardous situations are sufficiently unique that accumulated safety experience has been insufficient for the necessary safety measures to be completely codified. In these cases safety must be considered from first principles.
- step three reflects the fact that once safety risks have been analysed and all the necessary safety measures have been identified and implemented, there is an ongoing need to ensure that these measures remain in place and effective.

These steps are simply described but in practice the risk management process requires a great deal of professional experience and judgement to deal with the inherent uncertainties and to be able to explain to others how the process has been carried out, in order to maintain their trust.

Note that this three step approach is also applicable in an international context.

Application of Accumulated Safety Experience

The first step in the management of risks requires the *duty holder* to apply the safety experience accumulated so far in the process industries. This experience is usually to be found in the requirements of standards and codes of practice produced by authoritative organisations such as national or industry standards bodies or the regulators themselves. It is also found in technical articles in peer reviewed journals. It is expected that the requirements of all relevant codes and standards will be met without exception for new plant. New requirements will be considered for retrofit at existing plant during periodic safety reviews.

Information on standard safety measures will generally be in written form if it is authoritative. Occasionally, where there is a lack of written information, a duty holder will have to research which safety measures have been applied in analogous situations. If there is an apparent consensus about adopted safety measures, then the required measures do not have to be in written form in order to be authoritative. Irrespective of the information sources leading to the measures adopted, it is most important to record the sources of information and discussions held to justify conclusions and actions required.

In many situations outside the *process industries* this single step is an adequate response to risk management because the necessary safety measures have been fully codified. An example of this might be the guarding of dangerous parts of machinery where compliance with British Standard BS EN 953 would usually be regarded as a sufficient response to manage the potential for injury to the machine operator.

Analysis of Risks from First Principles

The second step in the management of risks reflects the fact that many hazardous situations are sufficiently unique that accumulated safety experience has been insufficient for the necessary safety measures to be completely codified. In these cases safety must be considered from first principles. The *duty holder* must ask 'what more could I do (to improve safety)?' and 'why am I not doing it?'. Behind these questions are the core steps that make up the risk management process. These are listed below.

- **What if?** Identify the hazards and what might lead to those hazards being realised.
- **What then?** Predict how widespread the area over which the hazardous effects might be experienced.
- **Then what?** Predict the harmful consequences for people in the area where the hazardous effects might occur and how likely those effects are to occur.
- **So what?** Compare the consequences and likelihoods with appropriate risk criteria (the public *attitude to risk*)
- **Do what?** Apply any additional safety measures that are necessary to reduce risk to tolerable levels, using a depth of cost benefit analysis appropriate to the level of risk to be reduced, having regard to the hierarchy of measures (Inherent Safety > Prevention > Control > Mitigation).

The tools and techniques used in these core steps are examined in more detail in Appendices 2 – 7 where the options available and comments on their suitability for particular situations are presented. Some tools and techniques will only be applied where the hazards are high. The options are listed generally in the order in which they would be used. Some tools/techniques cover more than one step in the risk management process. They are introduced at the first step that they cover.

Ongoing Safety Assurance

The third step in the management of risks reflects the fact that once safety risks have been analysed and all the necessary safety measures have been identified and implemented, there is an ongoing need to ensure that these measures remain in place and effective. Any system or process can degrade over time for a variety of reasons unless it is monitored. For this reason additional steps are necessary to provide assurance that risks continue to be adequately controlled. Senior management will require that systems of assurance are in place so that they can demonstrate to owners/shareholders and regulators that risks are being appropriately managed.

The tools and techniques used for ongoing safety assurance are examined in more detail in Appendix 7.

The Business Case for Good Risk Management

The need for good risk management is not driven exclusively by regulatory or even ethical demands. The business case for risk management, particularly directed at managing process safety risks, is clearly demonstrated by events over the past decade including the major accidents at Texas City, Buncefield, Jaipur, Puerto Rico, Macondo (Deepwater Horizon) and others. Lack of attention to safety risks can threaten the existence of even the largest company and often destroys the careers of the most senior management team involved. The Center for Chemical Process Safety in the USA has produced a useful guide[1] which highlights the benefits of systematic safety risk management:

- Risk reduction - reducing the likelihood of deaths, injuries, environmental damage and property loss, any one of which can be extremely costly, as well as the distress and loss of reputation;
- Efficiency gains - systematic examination of plant, processes and the people that manage and control them, can lead to elimination of waste, greater reliability and quality;
- Improved relations with staff, regulators, community and investors who will all appreciate the rational approach to risk identification, prioritisation and control.

1 CCPS Business Case for Process Safety, <http://www.aiche.org/ccps/about/business-case-process-safety-pdf>

Glossary

Attitude to risk: An individual's perception of risk and their response to it.

Duty holder: A term used by regulators such as HSE to refer to those individuals and organisations that are required to meet legal requirements.

Harm: Physical injury or death of persons or damage to the natural or built environment.

Hazard: A physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these.

Individual risk: The frequency at which an individual may be expected to sustain a specified level of harm from the realisation of specified hazards.

Occupational safety: A cross-disciplinary activity concerned with ensuring the safety of people engaged in work or employment.

Piping and instrumentation diagram: A diagram which shows the interconnection of process equipment and the instrumentation used to control the process[2].

Process flow diagram: A diagram showing the major vessels in a chemical plant and the connections between them, including the substances present, their temperatures pressures and flow-rates[3].

Process industries: The branch of industry that applies science to the process of converting raw materials or chemicals into more useful or valuable forms. It includes the oil, chemical, biochemical, polymer, and pharmaceutical sectors.

Process safety: A cross-disciplinary activity concerned with ensuring the safety of all people from hazardous, chemical or biochemical, plant or processes. It is part of the wider activity of *occupational safety.*[4]

Risk: The likelihood of a specified undesired event occurring within a specified period or in specified circumstances.

Societal risk: The relationship between frequency and the number of people sustaining a specified level of harm in a given population from the realisation of specified hazards.

2 See also <https://en.wikipedia.org/wiki/Piping_and_instrumentation_diagram>
3 See also <https://en.wikipedia.org/wiki/Process_flow_diagram>
4 See also <https://en.wikipedia.org/wiki/Process_safety>

Abbreviations

ACDS: Advisory Committee on Dangerous Substances

ALARP: (To reduce risk to) As Low As (is) Reasonably Practicable

BATNEEC: Best Available Technology Not Entailing Excessive Cost

BPM: Best Practical Means

EA: The Environment Agency <http://www.environment-agency.gov.uk/>

HSE: The Health and Safety Executive <http://www.hse.gov.uk/>

LPG: Liquefied Petroleum Gas

SEPA: The Scottish Environment Protection Agency <http://www.sepa.org.uk/>

SFAIRP: So Far As Is Reasonably Practicable

General References

"Nomenclature for Hazard and Risk Assessment, 2nd Edition ", Edited by David Jones, Institution of Chemical Engineers, January 1992, ISBN: 978 0 8529 5297 9

"Safety Performance Measurement", European Process Safety Centre (EPSC), January 1996, ISBN: 978 0 8529 5382 2

"Risk" by John Adams, UCL press, first edition, 16 February 1995, ISBN: 978 1 8572 8068 5

OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response, 2nd Edition, Organisation for Economic Co-operation and Development (OECD), 2003

A Flexible Framework for Addressing Chemical Accident Prevention and Preparedness, United Nations Environment Programme, 2010, ISBN: 978-92-807-3094-4

ISO 31000:2009 "Risk management – Principles and guidelines"

Appendix 1. What first? - Good Engineering Practice, Codes and Standards

It is important that the processes of risk management described in the following appendices are not regarded as the starting point for safety. The most important lessons for safety and risk management are often to found in history, whether it is relatively benign engineering failures or major accidents killing thousands

Good Engineering Practice

Good engineering practice is an ill defined term that is essentially the 'core' consensus about how any engineering task is to be carried out. It is based on the accumulated experience of process sector plant operators, contractors and regulators. It covers the complete engineering life-cycle from initial design through to completed decommissioning. Good engineering practice is always 'reasonably practicable'. Once established it may be codified into documentary form, but the absence of a document does not imply that a consensus has not been established.

Codes, Standards and Guidance

Codes, standards and guidance are the documented outcomes of good engineering practice. They are produced by a wide range of organisations such as industry organisations, regulatory bodies, and standards making bodies authorised by national governments. Some standards have wider objectives than simply implementing good engineering practice and are intended to implement free market objectives.

Appendix 2. What if? - Hazard Identification

Hazard Identification

Hazard identification is the starting point for all risk analysis, assessment, and management processes. It consists of the following basic steps:

- Specify and document the scope of the identification process, stating which plants and processes are being studied.
- Specify and document the hazardous substances present, their location, quantity and physical conditions, such as temperature and pressure.
- Specify and document any hazardous substances that are not present in normal operation but might be produced following a process upset, predicting their release location, quantity and physical conditions, such as temperature and pressure.
- Specify and document the mechanisms by which the hazardous substances present might be released from containment or produced in a process upset.

Many books are available giving detailed advice and guidance on hazard identification. Two are available from the IChemE[5][6].

HAZOP

A hazard and operability study (HAZOP) is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation. A HAZOP is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team during a set of meetings[7]. The inputs to the study include a *process flow diagram* and a set of *piping and instrumentation diagrams*. The outputs of the study include suggestions for additional safety measures to reduce risk.

The method was developed in the 1970s by Imperial Chemical Industries (ICI) and was described at the time in several publications[8][9].

HAZOP is also well described in a more recent IChemE book[10].

---

5 "Hazard Identification & Risk Assessment", Geoff Wells, Institution of Chemical Engineers, May 2004, ISBN: 978 0 8529 5463 8

6 "Hazard Identification Methods", Frank Crawley & Brian Tyler - European Process Safety Centre (EPSC), May 2003 , ISBN: 978 0 8529 5457 7

7 https://en.wikipedia.org/wiki/Hazop

8 Hazard and Operability Studies. Process Safety Rep. 2, Imperial Chemical Industries, 1974

9 A Guide to Hazard and Operability Studies, Chemical Industries Association, Alembic House, London, 1977

10 "HAZOP : Guide to Best Practice, 2nd Edition ", Brian Tyler, Frank Crawley and Malcolm Preston, Institution of Chemical Engineers, April 2008, ISBN: 978 0 8529 5525 3

Layer of Protection Analysis (LOPA)

Layer of protection analysis (LOPA) is a semi-quantitative tool for analysing and assessing risk[(11)]. It takes account of both the magnitude of the effects of realised hazards and their predicted frequency of occurrence, in orders of magnitude. Dealing with frequencies in this way is consistent with the treatment of frequencies in "Functional safety - Safety instrumented systems for the process industry sector" IEC 61511 and related standards.

A range of failure scenarios are considered for a plant which might lead to harm. The assumed frequency of a failure scenario is taken to be reduced by one or more independent protection layers (IPLs) either in place or proposed. The reduced frequency and magnitude of the harm are compared against relevant risk tolerability criteria to decide whether more needs to be done to reduce risk.

LOPA does not consider the cost of additional safety measures so cannot alone demonstrate compliance with the UK legal requirement of SFAIRP. It does provide much of the analysis about what additional safety measures might be applied and how effective those measures might be.

Human Factors Analysis

This considers the capabilities, behaviour and performance of everyone involved in the design, construction and operation of plant and equipment in the process industries. It is a major topic supported by a vast body of technical literature. Much of the analysis carried out is qualitative, but there are a range of quantitative techniques that can be applied when human factors analysis is part of a wider quantitative risk analysis.

Quantitative techniques include 'Technique for Human Error Rate Prediction' (THERP)[12], 'Success Likelihood Index Method' (SLIM)[13], and 'Human Error Assessment and Reduction Technique' (HEART)[14].

The Energy Institute has produced on-line awareness training on this topic[(15)].

---

11 Layer of Protection Analysis - Simplified Process Risk Assessment, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2001

12 'Design Techniques for Improving Human Performance in Production', A D Swain, 1972

13 'The quantification of human reliability using expert judgement: current findings and future developments', D E Embrey, Instn Chem. Engrs Conf. On Human Reliability in the Process Control Centre, London, 1983

14 'HEART - a proposed method for assessing human error', J C Williams, Ninth Symp. on Advances in Reliability Technology, 1986

15 Human factors awareness: web-based training course, <www.eihoflearning.org>

Appendix 3. What then? - Source Terms and Effects Modelling

Releases from Plant and Equipment

Once failure scenarios have been identified by which hazardous substances can be released from containment, it is necessary to predict how much might be released and at what flow-rate. These are sometimes referred to as the 'source terms'. Failure scenarios may lead to an instantaneous release, typically where a vessel fails catastrophically, or a continuous release, typically from a leak in a vessel or pipework. Leaks from vessels and pipework may occur through holes of varying sizes.

The properties of the substance being released will affect the flow-rate for a continuous release. Predictive models are available for gas releases, liquid releases and 2-phase releases, where the liquid is boiling as it is being released. An example of a two phase release would be LPG which is stored as a liquid under pressure but rapidly boils when released.

Some plant and equipment is installed in buildings. In this situation, continuous releases into the building initially accumulate inside before being released from the building. This leads to two release rate calculations being performed.

One important situation that does not involve release from a vessel or pipework, is that of hazardous substances involved in a fire. Release rates need to be predicted for toxic combustion products and/or toxic substances carried away in the combustion plume.

These calculations are usually performed by computer software available from a range of vendors.

Gas Dispersion Modelling

When gases are released from containment, their behaviour is dependant on the physical and chemical properties of the gas and the atmospheric conditions at the time. Denser than air gases may initially 'slump' towards the ground especially when released instantaneously and in a large quantity. After a time the 'slumping' behaviour changes to passive behaviour where the gas is carried along by the wind. As the gas is carried along by the wind the concentration of the gas reduces and, therefore, becomes less harmful.

The behaviour of lighter than air gases will initially be determined by the direction of any release jet if they are released from high pressure. These releases also become passive eventually and are carried downwind rising above the ground and hence becoming less harmful at ground level.

Some gases that are lighter than air are stored in large quantities as a refrigerated liquid. If these are released then the gas which is formed by the boiling liquid is likely to be sufficiently cold that it behaves as a denser than air gas initially. Eventually it will warm up as it is carried downwind and becomes lighter than the surrounding air and rises above the ground.

Combustion products from fires are initially lighter than air and will usually rise rapidly. However where fires occur in buildings, the building structure may contain the products of combustion for sufficient time to allow them to cool and become much less buoyant. Once outside the building these cooler combustion products may be hazardous at ground level especially if the wind speed is high.

These behaviours and concentration calculations are usually performed by computer software available from a range of vendors.

Thermal Effects Modelling

When flammable substances are ignited the combustion process releases large amounts of energy, much of it in the form of heat technically called thermal radiation. The thermal radiation is determined by a range of factors. Thermal effects modelling usually recognises four types of fire described below. Real fires will often have aspects of more than one type, either together or sequentially.

Pool fires occur when a release forms a large pool which is then ignited. The resulting fire can be very large, burn for a long time and the thermal effects can be very damaging to people and property over large distances.

Jet fires occur when a continuous release is immediately ignited. The direction of the release determines the direction of the jet fire.

Cloud fires occur when a large quantity of flammable gas has accumulated in the area around the release point. If it finds a source of ignition as the cloud periphery advances, the cloud ignites and the combustion process moves back through the cloud to the point of release. If enough turbulence is generated in the cloud, the combustion rate increases to the point where significant pressure effects are generated.

Fireballs occur when a large instantaneous release of gas or boiling liquid is immediately ignited. The combustion process generates sufficient buoyancy to cause the flammable substances to rise into the air as they continue to burn, in an approximately spherical shape.

These calculations of thermal radiation, produced by the fire and affecting persons and structures, are usually performed by computer software available from a range of vendors.

Explosion Overpressure Effects Modelling

Explosions are caused by a sudden release of energy that generates large volumes of gas, usually combustion products, which rapidly flow away from the point of initiation, exerting a pressure on obstacles in their path.

Historically the most widely encountered explosions were from explosives used in mining and quarrying. Explosives have always been present in sufficient quantities to cause damaging effects in the event of an accident. Over the last 60 years the process industries have developed larger plants which now contain sufficiently large quantities of flammable gases and liquids that they also present substantial explosion hazards.

The effects from most explosions of solid and liquid substances are assessed by equating them to an equivalent amount of a reference explosive, normally TNT. The variation of overpressure with increasing distance from an explosion of TNT has been well studied experimentally and established correlations may be used(16).

Explosions of gaseous substances are more complex due to the variability of the combustion process in the gas phase caused by the presence of obstacles which generate turbulence. This topic has been the subject of large amounts of research in the technical literature which is still ongoing.

Practical methods for explosion overpressure assessment range from basic methods requiring less detail and computational effort(17), to computationally intensive methods that may take several days computing time to assess a single configuration(18).

These calculations are usually performed by computer software available from a range of vendors.

Hand Calculations

Hand calculations can be carried out for many of these release phenomena and hazardous effects using methods published by authorities in the Netherlands(19)

16 A Review of the State-of-the-Art in Gas Explosion Modelling, HSL report CM/00/04, 2002, section 2.1.2

17 A Review of the State-of-the-Art in Gas Explosion Modelling, HSL report CM/00/04, 2002, sections 2.1 and 2.2

18 A Review of the State-of-the-Art in Gas Explosion Modelling, HSL report CM/00/04, 2002, sections 2.3 and 2.4

19 PGS2 Yellow Book - Methods for the calculation of physical effects 1997/2005 <http://www.publicatiereeksgevaarlijkestoffen.nl/publicaties/PGS2.html>

Appendix 4. Then what? - Frequency Modelling and Vulnerability

Having carried out analyses of the magnitude of the hazardous effects that might be anticipated following a release of hazardous substances, the next step is to consider how often this might occur and what the consequences might be for people and structures.

Frequency Analysis

Frequency analysis is generally performed either using numerical values derived from historical data or by producing situation specific numerical values using predictive techniques such as fault tree analysis and event tree analysis as described below.

Numerical values derived from historical data are obtained from databases which contain aggregated operating experience, the numbers of failures that have occurred during that period, and failure rates derived from them[20]. HSE has published the failure rates it uses for land use planning work[21].

Fault Tree Analysis

Fault tree analysis (FTA) is the systematic analysis of precursor events that alone or in combination lead to a single, usually undesirable, event. The combinations of precursor events, including their likelihoods, are evaluated using logic in order to predict the likelihood of the single top event. Examination of the completed tree can also give an insight into the significance of the individual event sequences that lead to the 'top event' and from this insight, suggest possible safety measures that might be applied to reduce risk.

A thorough description of FTA is given in a publication by authorities in the Netherlands[22].

Event Tree Analysis

Event tree analysis (ETA) is the systematic analysis of possible event sequences that might result from a single, usually undesirable, event. The event sequences, including their conditional probabilities, are evaluated using logic in order to predict the likelihoods of the various outcomes. Examination of the completed tree can also give an insight into the significance of the individual event sequences that lead to the various outcomes and from this insight, suggest possible safety measures that might be applied to reduce risk.

A fault tree and event tree are often combined. The result is called a Bow-Tie Diagram.

A thorough description of ETA is given in a publication by authorities in the Netherlands[23]

---

20 Guidelines for Process Equipment Reliability Data, with Data Tables, 1989, Center for Chemical Process Safety <http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0816904227.html>

21 Failure rate and event data for use within land use planning risk assessments <http://www.hse.gov.uk/landuseplanning/links.htm>

22 PGS 4 Red Book - Methods for determining and processing probabilities, section 8, <http://www.publicatiereeksgevaarlijkestoffen.nl/publicaties/PGS4.html>

23 PGS 4 Red Book - Methods for determining and processing probabilities, section 10, <http://www.publicatiereeksgevaarlijkestoffen.nl/publicaties/PGS4.html>

Vulnerability to Thermal Effects

The low level effect of thermal radiation on people is well known to us all as it causes high pulse rate, increased and laboured respiration, high sweat losses and increased body core temperature. At higher levels, thermal radiation causes pain and burn injury.

A thorough analysis of human vulnerability to thermal radiation is given in an IChemE monograph(24). This monograph allows predictions to be made of fatality probability given a known exposure to thermal radiation for a person of various age ranges. Criteria have also been published for vulnerable populations(25).

The effect of thermal radiation on structures is also important, both for the direct damage caused, but also the possibility of people being exposed to thermal radiation within a burning building. A review of vulnerability criteria has been published by the Health and Safety Laboratory(26).

Vulnerability to Overpressure Effects

The low level effect of overpressure on people and structures is well known to most people in the form of buffeting by the wind and wind damage to structures. At higher levels, overpressure can cause direct harm to people and substantial damage to structures. Collapsing structures can cause harm to any occupants.

An analysis of human and structural vulnerability to overpressure is given in an IChemE monograph(27).

Vulnerability to Toxic Gas Exposure

Exposure to toxic gas can cause a wide range of effects from minor distress to death. Process safety assessments are concerned with life threatening exposures. Vulnerability is determined by the concentration of the toxic substance and the time of exposure. The combination of these two factors is called the dangerous toxic load (DTL).

A document giving more detail about the derivation of DTLs, and values for a range of hazardous substances encountered in the process industries, has been published by HSE(28).

Vulnerability to Environmental Harms

Vulnerability of flora and fauna, and the environment generally, is not discussed here.

---

24 "Thermal Radiation 2 - The Physiological and Pathological Effects", Ian Hymes, Warren Boydell and Belinda Prescott, Institution of Chemical Engineers, January 1996, ISBN: 978 0 8529 5328 0

25 Contract Research Report 285 - Thermal radiation criteria for vulnerable populations, HSE, 2000

26 Review of HSE Building Ignition Criteria – HSL/2006/33, Graham Burrell and John Hare, Health and Safety Laboratory, 2006

27 "Explosions in the Process Industries, 2nd Edition", Institution of Chemical Engineers, January 1994, ISBN: 978 0 8529 5315 0

28 Assessment of the Dangerous Toxic Load (DTL) for Specified Level of Toxicity (SLOT) and Significant Likelihood of Death (SLOD), <http://www.hse.gov.uk/chemicals/haztox.htm>

Appendix 5. So what? - Comparison with Criteria

Introduction

Criteria for the tolerability of harm are essentially political in nature, hence they will tend to vary from country to country. The following discussion concentrates on UK practice which is largely 'risk-based' in concept. This practice is considered to be a good model which can be applied or adapted for use in other countries.

In the UK the key concept is the requirement in the 'Health and Safety at Work Act (1974)' for the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable (SFAIRP), safe and without risks to health. For practical purposes this is usually interpreted to mean that health and safety risks to employees and the public are reduced to be 'as low as reasonably practicable' (ALARP). However care needs to be taken to include the practicalities of actually implementing additional measure(s) required to become ALARP. Plant may remain safe SFAIRP for some time after measure(s) needed to become ALARP have been identified.

ALARP is obviously a very broad concept and considerable work has been done to define it more closely in the decades since 1974. Detailed guidance on this subject is given in the 'ALARP Suite' on the HSE website[29] but the following explanations outline the main points.

In order to be ALARP an industrial activity must conform with **all** of the following:

- comply with specific legal requirements
- use relevant good engineering and good industrial practice
- not operate at intolerable individual fatality risk
- not operate at intolerable societal fatality risk
- meet cost/benefit analysis (CBA) criteria which go beyond the consideration of fatality (this is discussed in more detail in Appendix 6)

Note that compliance with specific legal requirements and good engineering/industrial practice is a minimum requirement in order to '*achieve the standards of relevant good practice precautions, irrespective of specific risk estimates*'.

In the UK context the presumption is that if an activity cannot be shown to be ALARP, then further risk reduction measures must be applied to make it ALARP, or the activity must cease.

Specific Legal Requirements

In the UK (and in most other countries) there is prescriptive ('rule-based') legislation to deal with specific health and safety risks which takes precedence over the 'risk-based' part of the 'ALARP/SFAIRP' approach.

29 HSE ALARP Suite, www.hse.gov.uk/risk/theory/alarp.htm

Individual Fatality Risk Criteria

'Individual fatality risk' is the simplest parameter that can be considered after 'prescriptive legislation' and 'good practice' so received early attention when formulating the ALARP concept in the UK. The first substantial document was the Royal Society Study of 1983[30]. This concept was further developed in an HSE report in 1992[31], based on an assessment of the existing public tolerance of fatality risk. The currently definitive individual fatality risk criteria for the UK are defined in an HSE report from 2001[32], in paragraphs 128 – 133.

The criteria define:

- whether the individual fatality risk is 'intolerable' in which case the activity cannot continue without improvement
- whether the individual fatality risk is 'tolerable if ALARP' in which case a CBA must be carried out to demonstrate ALARP
- whether the individual fatality risk is 'broadly acceptable' in which case a CBA based on individual fatality risk is not necessary

Societal Fatality Risk Criteria

Societal risks can impact on the fabric of society through effects such as:

- multiple fatalities arising from a single incident
- long term disability or health effects
- damage to infrastructure and the environment
- inhibition of economic activity

The concept of societal risk is considerably more complex than that of individual risk, so specific proposals on societal fatality risk criteria for onshore hazardous installations did not appear in the UK until an HSE Report in 2001[33] in paragraphs 134 - 139. The criteria proposed were based on an extension of the analysis of the hazards from oil and chemical installations at Canvey Island in 1981[34] and in a report from 1991[35]. The currently definitive societal fatality risk criteria for the UK are detailed in an HSE internal guidance document[36].

The criteria define regions analogous to those described in the previous section including requirements for a CBA.

It should be noted that the derivation of the HSE societal fatality risk criteria is much more rudimentary than that for individual fatality risk criteria. This results from the application of

30 'Risk Assessment – A Study Group Report', The Royal Society, January 1983, ISBN 0 85403 208 8

31 'The Tolerability of Risks from Nuclear Power Stations', HSE, 1992

32 'Reducing Risks, Protecting People - HSE's decision-making process', Health and Safety Executive, 2001, ISBN 0 7176 2151 0, <http://www.hse.gov.uk/risk/theory/r2p2.htm>

33 'Reducing Risks, Protecting People - HSE's decision-making process', Health and Safety Executive, 2001, ISBN 0 7176 2151 0, <http://www.hse.gov.uk/risk/theory/r2p2.htm>

34 'Canvey - a Second Report', HMSO, 1981, ISBN 0118834592

35 'Major Hazards Aspects of the Transport of Hazardous Substances, ACDS, 1991, ISBN 011885676 6

36 'Guidance on ALARP Decisions in COMAH', HSE Semi Permanent Circular SPC/Permissioning/37, <http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/index.htm>

simplifying assumptions necessary to derive the relatively simple criteria selected by HSE. The HSE criteria are for a cumulative formulation of societal risk. More recently the Buncefield Standards Task Group (BSTG) set up after the Buncefield incident has suggested some criteria for a non cumulative, scenario based formulation of societal risk[37].

Environmental Risk Criteria

Environmental risk criteria are much less well developed and are not discussed here. Some discussion can be found in a publication by the UK COMAH Competent Authority[38] and a research report for the UK Maritime and Coastguard Agency[39].

---

37 'Safety and environmental standards for fuel storage sites', Buncefield Standards Task Group (BSTG) final report, Table 8 page 91

38 Guidance on the Environmental Risk Assessment Aspects of COMAH Safety Reports, COMAH Competent Authority, 2nd December 1999

39 BMT Isis Limited, Research Project 591 Environmental Risk Criteria, December 2007

Appendix 6. Do what? - Identification of Further Measures and Cost Benefit Analysis

Expert Group Analysis

When the levels of risk identified indicate that a qualitative approach to risk management is sufficient, then the process of identification of possible additional safety measures, and the decision about whether they are cost-effective and hence whether or not to implement them, is usually carried out by an expert group. The persons forming the group are necessarily required to have an appropriate level of education, training and experience to enable them to perform the task.

Bow-tie Analysis

An earlier step in the risk assessment process may have produced one or more bow-tie diagrams. These provide a useful starting point when a more systematic approach to identifying additional safety measures is required. Each 'branch' in the 'tree' is considered in turn and safety measures proposed that might reduce the significance of the branch or eliminate it altogether.

Scope of Cost Benefit Analysis

The outcome of a cost benefit analysis (CBA) can change if the scope of the costs and benefits being considered are changed. The scope of any CBA needs to be clearly justified and documented. In some cases a CBA is carried out for regulatory compliance purposes alone. In other cases the scope may be widened to include potential costs such as loss of reputation for a multinational company and consequent reduction in share price.

For regulatory compliance CBAs, HSE has published its views[40].

Costing Additional Measures

This is usually straightforward, even when a quantitative assessment is being carried out, because suppliers of safety equipment are keen to provide the cost of additional safety measures in order to facilitate their consideration for possible purchase and installation.

Valuing Harms Averted

Once the scope of a CBA has been set, and the CBA is being carried out, it will be necessary place a value, either qualitatively or quantitatively, on harms averted by the provision of possible additional safety measures. All harms within scope that are averted must be valued and not just fatalities. Where a quantitative approach is necessary it may be necessary to seek the advice of insurance actuaries.

40 Cost Benefit Analysis (CBA) checklist <http://www.hse.gov.uk/risk/theory/alarpcheck.htm>

For regulatory compliance CBAs, HSE has published its views[41] and some additional research[42].

Gross Disproportion

In conventional CBAs the decision is normally based on whether the monetary value of the benefits of a proposed action exceed the costs. For an occupational safety CBA, the law in the UK requires a clear bias in favour of safety. This is expressed in the concept of *gross disproportion* as stated in an important legal ruling[43] about safety in a mine as follows: *'the mineowner must, before the occurrence of an accident, make a computation in which the quantum of risk run by the worker was placed in one scale and the sacrifice of the mineowner involved in the measures necessary to avert the risk (whether in money, time, or trouble) was placed in the other, and, if there were a gross disproportion between them—the risk being insignificant in relation to the sacrifice—the mineowner discharged the onus which was on him.'*

This concept has not been expressed in a numerical form for use where a quantitative risk assessment and subsequent CBA is being undertaken. HSE has published some guidance in the context of the COMAH regulations[44].

---

41 Cost Benefit Analysis (CBA) checklist <http://www.hse.gov.uk/risk/theory/alarpcheck.htm>

42 Research Report 541 - Valuation of health and safety benefits, HSE, 2007

43 All England Law Reports – All ER 1949 Volume 1 – Edwards v National Coal Board

44 Guidance on ALARP Decisions in COMAH, SPC/Permissioning/37, paragraphs 40-45 and annex 1

Appendix 7. What else? - Ensuring the Process Stays Safe

Auditing

Safety auditing[45] is intended to provide confirmation that the intended safety measures are still in place and functioning correctly.

It is vital that any audit is used as a positive boardroom management tool. Use should be made of both external and internal auditors, to ensure effectiveness, independence and objectivity.

Review

Reviewing[46] is intended to check that existing safety measures remain sufficient in the light of changing circumstances. This involves consideration of a wide range of plant and non-plant changes that may have occurred since the plant was constructed, or the previous review. If the existing safety measures are found to be insufficient then the review itself may make recommendations for additional measures or recommend a separate study.

Reviews are often combined with audits as a follow-on activity.

Key Performance Indicators (KPIs)

KPIs are intended to check ongoing safety performance in a relevant, measurable way[47]. Major accidents in the process industries are, fortunately, very rare, so using their frequency of occurrence as an indicator of safety performance is inadequate. KPIs comprise a range of leading and lagging indicators about precursor events that are not necessarily harmful themselves but are important in the chain of events leading to a major accident.

Learning from Accidents/Incidents

Although major accidents in the process industries are, fortunately, very rare at any one plant, the number of process plants worldwide means that major accidents occur sufficiently often that they provide a learning opportunity for those operating similar processes around the world. Information about learning points can be found in a range of publications[48] and databases[49]. Learning from accidents/incidents is always part of a periodic review process. Learning from important accidents/incidents is appropriate at any time.

---

45 Successful Health and Safety Management, HSG65, pages 70-74, HSE, 1997, ISBN 0 7176 1276 7, <http://www.hse.gov.uk/pubns/books/hsg65.htm>

46 Successful Health and Safety Management, HSG65, pages 74-75, HSE, 1997, ISBN 0 7176 1276 7, <http://www.hse.gov.uk/pubns/books/hsg65.htm>

47 HSG254 - Developing process safety indicators - A step-by-step guide for chemical and major hazard industries, Health and Safety Executive, 2006, ISBN 978 0 7176 6180 0 <http://www.hse.gov.uk/pubns/books/hsg254.htm>

48 Loss Prevention Bulletin (LPB), IChemE, <http://www.icheme.org/resources/lpb.aspx>

49 United Nations Environment Programme, Disasters Database, <http://www.unepie.org/scp/sp/disaster/database/>

Monitoring Non-Plant Changes

Managing safety at major hazard process plants is not just about the hazardous substances and ensuring the integrity of the plant containing them. The distinguishing feature of major hazard process plants is that they pose significant *societal risk*. The tolerability of *societal risk* depends on the number and location of people near these plants. Monitoring this is not only part of periodic reviews but also necessary when development proposals are made for adjacent land. Similar monitoring must be in place for new or extended environmentally sensitive sites.

Managing safety is a balance between the costs of safety measures and the monetary value of the safety improvements they bring. This balance can change when new safety measures become available or existing safety measures become available at a lower cost. Monitoring this is part of periodic reviews.

An important part of managing safety at major hazard process plants is the modelling of the harmful effects of released hazardous substances. Modelling techniques are subject to ongoing research and development leading to improvements. Monitoring this is part of periodic reviews.