Legacy Systems:
Basic Principles for Safety

Introduction

Engineered systems are relied upon for safety in a wide range of work environments. There is however, a general lack of awareness of the exact role played by such systems, and whether adequate safety is, in fact, being achieved. This is particularly true of systems that have been in place for many years.

This document describes how to assess the capability of so called Legacy Systems, focussing on how electrical, electronic, or programmable devices achieve adequate safety in conjunction with other technologies such as mechanical systems and operational expectations.

These guidelines have been produced by The 61508 Association to assist its members and others to consider how to deal with legacy systems. The Association would welcome any comments on this publication, sent to legacy@61508.org. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.

Intended Audience

This document is intended to be used by managers and technical staff with roles and responsibilities relating to legacy systems.

It will also be of relevance to those that support these roles, including:

- owners
- company, site and operating unit managers
- suppliers of systems, sub-systems and components
- safety assessors
- regulatory authorities
- consulting engineers
- organisations with contractual obligations

Legacy System:
A safety related system which performs one or more safety functions as defined in IEC 61508 but which was designed and installed before the publication and adoption of IEC 61508.

Note: this document applies to systems using technologies such as Electrical, Electronic, Programmable Electronic Systems, mechanical, and hydraulic systems.

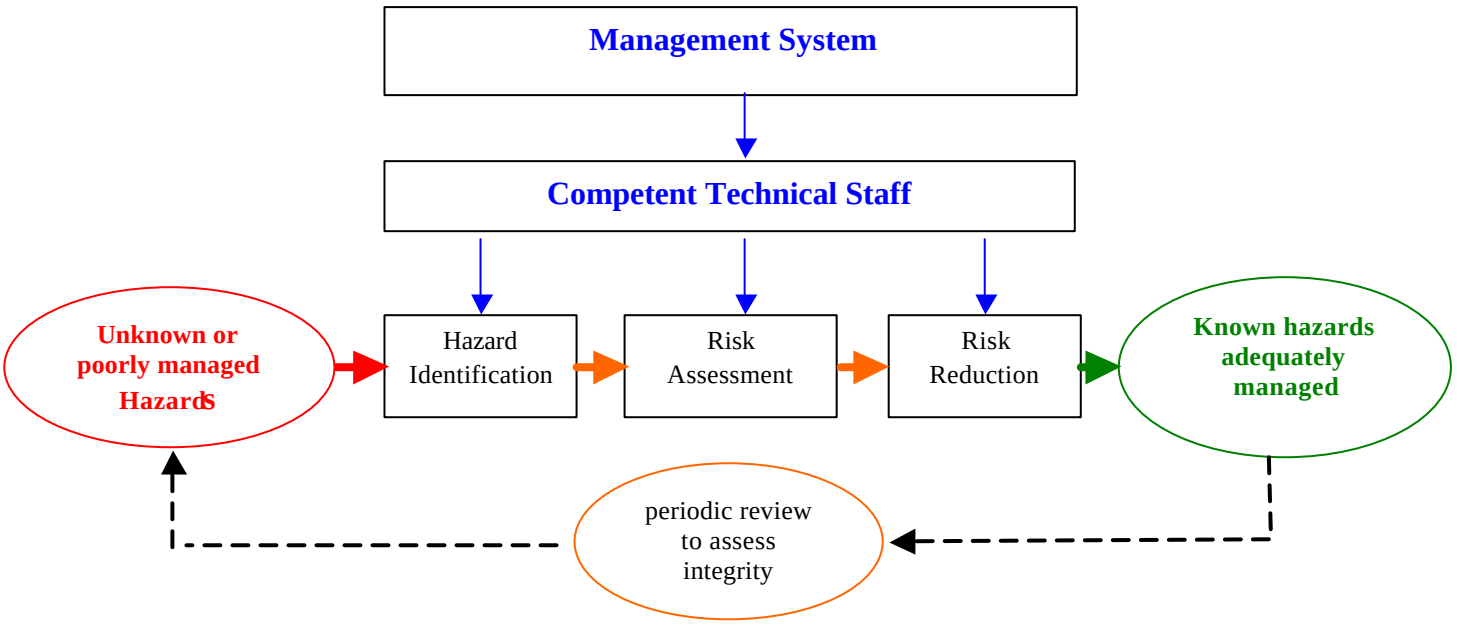


Fig.1 Diagrammatic representation of the management of legacy systems

1 Legal responsibility for safety

An organisation is responsible for compliance with health and safety legislation, which includes reducing risks to people to as low a level as is reasonably practicable (ALARP)[1].

The organisation management needs to:

- *Define the organisational objectives relating to process safety and to safety related systems, including legacy systems. Implicit in this is determination and definition of the organisation's tolerable risk criteria*[2].
- *Ensure that an appropriate management approach for safety related systems is in place and is applied. This approach should take into account technical progress including new standards.*
- *Ensure that competent technical and engineering staff are available, aware of their roles and responsibilities and have sufficient resources and authority to carry out their roles and to discharge their responsibilities.*

2 Advances in safety management and safety technology

What is reasonably practicable can change over time with advances in safety management techniques and in the capabilities of safety technology such as safety instrumented systems. Modern standards such as IEC 61508[3] provide a more effective benchmark for the management, specification, design, implementation, operation, maintenance and modification of safety-related systems than may have existed when legacy systems were originally put in place.

[1] http://www.hse.gov.uk/risk/theory/alarp.htm , http://www.hse.gov.uk/risk/theory/r2p2.pdf

[2] See Annex C

[3] The most appropriate safety standards should be used according to the application and sector, such as IEC 61511which applies to process industries.

It is necessary to periodically review both the management of functional safety and the technical suitability of the safety related systems.

These principles describe two aspects of the management of legacy systems:

- *A one-off review of the functional safety management system (Section 4) and the technical suitability of the safety related systems (Section 5).*
- *The ongoing management of safety related systems.*

3 Impact on legacy systems

Safety-related systems designed and installed before the publication of IEC 61508 are not required to be replaced or upgraded just because the standard has been published. There may be varying degrees of design information and operational records relating to legacy systems that can be used as a source of evidence to assess the adequacy of those systems. The organisation should be able to demonstrate that the measures in place to control the risks of hazardous events are adequate when seen in the light of the standard and the requirements of the law.

4 Management requirements

The law requires that an adequate safety management system is in place[4]. An effective functional safety management system is an essential element in achieving adequate risk control[5]. An assessment of the company's approach to the management of safety-related systems (functional safety management system) should be carried out. The objective is to ensure that the policies and activities follow current good practice and regulatory expectation in regards of functional safety, such as described in IEC 61508. The correction of any identified inadequacies in the safety management system should be included in the Action Plan (Section 12).

5 Technical requirements

IEC 61508 provides a risk based approach to specifying, designing, implementing and using safety related systems. Legacy systems will have been created using different design approaches or standards. The continuing suitability and fitness for purpose of such legacy systems should be confirmed by conducting a technical review as outlined in the following sections.

6 Rigour and prioritisation of technical review

The rigour of the technical review of the legacy systems, and hence the resources allocated to the task, should be related to the hazards, consequences and risks associated with the operating unit. The more serious the consequences and the more likely the hazardous events, the more thorough the review needs to be. A preliminary survey should be conducted in order to identify the likely higher risk areas and to determine the rigour and prioritisation of the review. Justification for the chosen degree of rigour should be documented.

[4] An example of a legal requirement for the adequate management of health and safety is the **Management of Health and Safety at Work - Management of Health and Safety at Work Regulations 1999 Approved Code of Practice and Guidance** (HSE Pubs L21 ISBN 0-7176-2488-9)

[5] FSM is a basic requirement of IEC61508 part 1 clause 6 and all sector guidance standards have matching requirements (e.g. IEC 61511 has the same requirements in Part 1 clause 5)

7 Competence of review team

The technical review should be carried out by people from an appropriate range of disciplines and possessing the necessary competencies. The range of disciplines will depend on the nature of the operations but should include staff with a good understanding of the process under control as well as those with a detailed knowledge of the safety-related systems. Those with day to day hands on experience of the operating units and their maintenance should be included.

8 Use of existing documentation

Existing documentation is likely to have a significant role in the review and ongoing management of legacy systems. Documentation should be used with care as it may not be comprehensive and free from errors.

9 Hazard identification and risk assessment

The objective is to ensure that all hazards are identified and understood, and the consequences and likelihood of hazardous events assessed.

A record of the hazards associated with the plant and process should be available and up to date. In the absence of such a record, a hazard identification and risk assessment should be undertaken. A good starting point is a list of all existing safety-related systems, but care should be taken because there may be hazards

- *that were not previously identified or understood;*
- *against which current safety related system provide no protection;*
- *that have arisen since the last hazard and risk assessment;*
- *that have changed in risk, nature or attributes since the last hazard and risk assessment.*

10 Risk reduction measures

The contribution of all existing safety-related measures used to reduce risks should be reviewed in relation to the principles of ALARP[6]. The review should include not only the electrical, electronic and programmable electronic systems (E/E/PES) but also other measures such as mechanical safety devices and mitigation measures of a mechanical, structural, chemical or work systems nature. The outcome of this stage of the review should be the identification, specification and documentation of safety functions that currently exist.

[6] ALARP: As Low As Reasonably Practicable

11 Technical review of legacy systems (E/E/PES)

All legacy E/E/PES should be reviewed[7]. The objective of the review is to determine the adequacy of the systems to provide sufficient risk reduction for the hazards identified in the previous stages. This adequacy has three properties;

- *that the appropriate safety function will perform effectively.*
- *that the safety-related system implementing the function is likely to have sufficient safety integrity. In practice this means that the safety-related system can, with the required probability, satisfactorily perform the required safety function(s) under all the stated conditions within a stated period of time*
- *that the safety-related system implementing the function is adequately protected from the effects of systematic failures, such as those arising from design errors (including software), poor maintenance, inadequate control of change, and incorrect use of overrides.*

The review should produce documented argument and evidence that demonstrates the adequacy or otherwise of the legacy system. For systems associated with high consequences/risks the justification should be based upon the methods described within modern standards, such as IEC 61508. For systems associated with low consequences/risks the justification may be based upon the application of sector good practice backed up by adequately documented history. Alternatively, justification may be based upon gap analysis with the requirements of modern standards, such as IEC 61508.

The review should identify any deficiencies in the legacy systems which should be dealt with in the Action Plan (Section 12).

The review may identify legacy systems that are no longer needed or proof testing regimes that are more rigorous than is required. In such cases there could be a justification for making changes, which could reduce operating and maintenance burden.

[7] While outside the scope of this document, a similar approach could be taken with safety-related systems which use measures other than electrical, electronic or programmable electronic technology.

12 Action plan

A prioritised action plan should be prepared and implemented to deal with any inadequacies in:

- *the functional safety management system*
- *the safety-related systems.*

In cases of serious shortfall, interim measures will need to be taken while longer term solutions are devised.

Where additional risk reduction measures are required, consideration should be given to the selection of the most appropriate solution that takes account, where relevant, of:

- *individual risk*
- *societal risks and societal concerns*
- *the sacrifice and benefits*
- *the technical feasibility of proposed control measures*
- *the level of risk control they achieve*

Preference should be given to the use of:

- *inherent safety and the elimination of hazards*
- *the avoidance of risk*
- *the control of risk at source by the use of physical engineering controls*

and reduce reliance on :

- *procedural controls*
- *and, personal protective equipment*

The elimination of the hazards, if possible, would be the option of choice. Failing that, the approach should be to use the highest control in the hierarchy where reasonably practicable.

A number of measures may be necessary to achieve the required level of risk control such that when those higher up the hierarchy have been exhausted, measures lower down the hierarchy are used. The aim is to reduce risks to As Low As is Reasonably Practicable.

Personal protective equipment only protects the wearer and only when worn properly all the time.

Risk Control Hierarchy		Notes
Elimination	Engineered controls	Through choice of substances and process used, or choice of process parameters such as temperature and pressure such that hazards are eliminated or more readily controlled
Substitution		
Containment		Design and construction of process e.g. pipe ratings, layout, supporting structures, allowance for aging etc
		Process control systems
		Relief valves, bunds, blast walls etc
		Safety Instrumented systems, ESD systems
Remove People	Engineered controls and/or procedural controls	This may include safe working systems, practices, procedures, access control, introduction of remote or automatic operation of process
Reduce Exposure		
Warnings and Signals		May include alarm systems as well as physical notices, use of different floor colours etc
PPE		This should include training, supervision, and enforcement.
Discipline/Supervision	Procedural controls	
Recovery Systems	Engineered controls and/or procedural controls	e.g. post accident systems and procedures, fire fighting systems, emergency and evacuation procedures.

Note: recovery systems have been included because they may reduce the severity of the consequence from a hazard. They do not prevent the hazardous event from occurring.

When E/E/PES are replaced or upgraded, the new ones should be specified, designed and implemented in line with IEC 61508. A different approach would need to be considered if there are incompatibility problems in relation to other, existing systems and practices.

All risk control measures need to be properly maintained, operated, and regularly reviewed. This may include regular inspection, testing and ongoing management. Workers need to be trained and competent in the use and maintenance of risk control measures.

13 Update operation and maintenance procedures

Where changes have been made or deficiencies in current operating and maintenance procedures have been identified, the procedures should be updated. Note however that appropriate day to day hands on operations and maintenance staff should be involved in the development of any new procedures. Effective record keeping will help to ease future reviews.

14 Periodic audit and technical review

Periodic audits of the effectiveness of the functional safety management system should be conducted in accordance with the publication 'Successful Health and Safety Management' [HSG65], with the results being used to drive on-going improvements in safety and operations.

Periodic technical reviews, sponsored by senior management, should be carried out to ensure that each safety-related system continues to be fit for purpose when compared with current standards and results in sufficient risk reduction to meet the organisation's tolerable risk criteria.

Annex A

Fig.2 Legacy System Management Approach Review Flowchart

This flow chart is relevant to all Operating Units.

The thick solid black line shows the flow of activities making up the initial review. The dashed black line shows the activities that should be undertaken periodically following the initial review.

The grey boxes linked to an activity by a grey line show issues that should be addressed as part of the activity – in this case the various attributes of a functional safety management system. For the explanation of these boxes see the relevant sector guidelines.

Where a (number) is included in a box this refers to the relevant section number in this document.

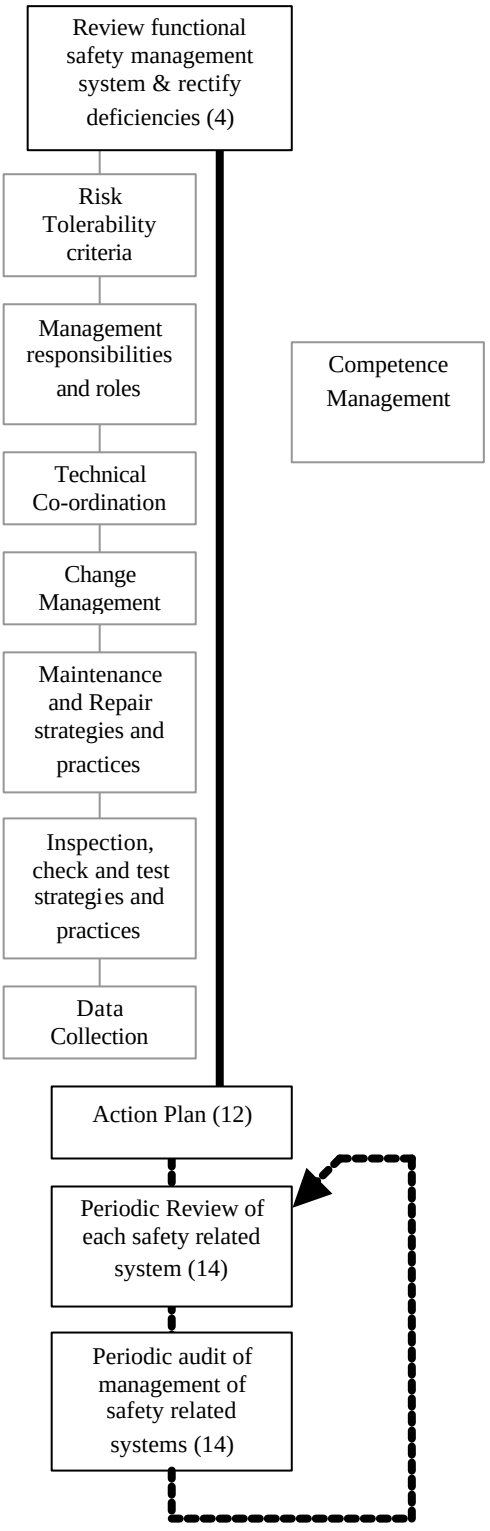
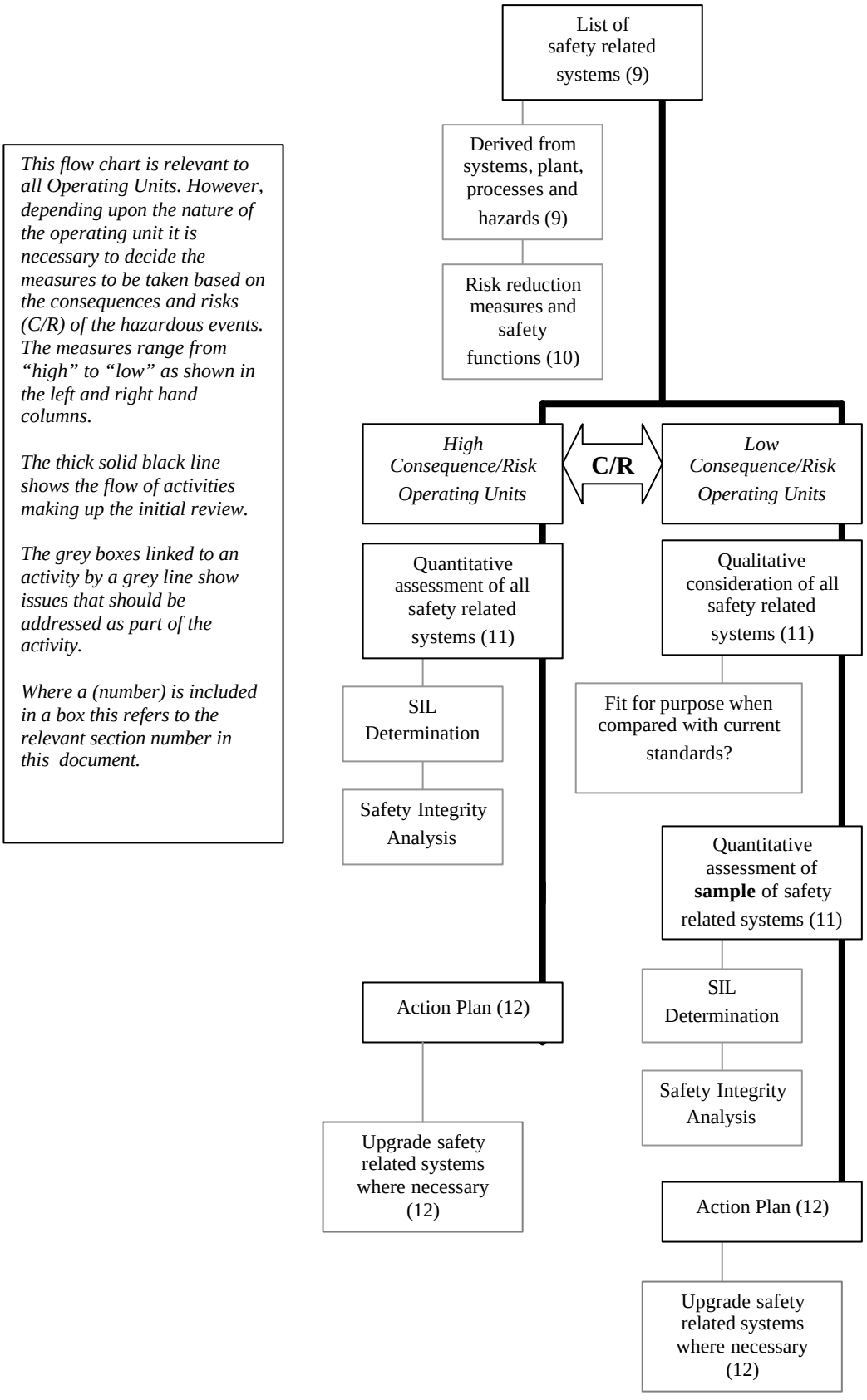


Fig.3 Legacy System Technical Suitability Review Flowchart



Annex B

References

- **The Health and safety at work etc Act 1974**
  http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1974/cukpga_19740037_en_1
- **Management of Health and Safety at Work - Management of Health and Safety at Work Regulations 1999 Approved Code Of Practice and Guidance** (HSE Pubs L21 ISBN 0-7176-2488-9)
- **Safe use of work equipment - Provision and Use of Work Equipment Regulations 1998 Approved Code of Practice and guidance**
  (L22, HSE Publications 1992, reprinted 2001, 2004 ISBN 0717616266)

- The HSE Publication '**Out of Control - Why control systems go wrong and how to prevent failure**' (Second Edition HSG238 ISBN 0-7176-2192-8) gives an introduction to this topic, as well as listing a number of references.
- HSE publication **'Successful Health and Safety Management HSG65**, 1997, ISBN 0717612767', available as a free download at www.hsebooks.com

- http://www.hse.gov.uk/comah/sragtech/discguidciretro.htm Guidance for the COMAH sector that recommends that legacy control systems are considered.
- http://www.hse.gov.uk/risk/expert.htm . Some areas of this guidance is especially relevant to legacy systems.
- http://www.hse.gov.uk/risk/theory/alarp1.htm - Contains general information on reasonable practicability, ALARP and good practice. Paragraphs 51 and 52 describe how the risks present in existing plant should be considered in relation to what may be done on a new plant.
- http://www.hse.gov.uk/risk/theory/alarp2.htm - Assessing compliance with the law and the use of good practice
- http://www.hse.gov.uk/risk/theory/r2p2.pdf - Reducing risks, protecting people (R2P2) gives guidance on HSE's decision making, including the use of good practice

Annex C

Tolerable Risk Criteria

The IEC61508 group of standards require that all companies decide what their level of tolerable risk will be, but does not specify what the level should be. This is the responsibility of the ***company management***, usually at ***board level.***

Tolerable risk criteria can be set using various types of measure – a common one is that of Individual Risk. This is the annual risk from work activities incurred by a nominated individual – when using this in risk assessment the person at greatest risk is generally assessed.

There is common practice and published guidance on the selection of tolerable risk values expressed in terms of Individual Risk; in particular the HSE publication "Reducing Risks, Protecting People" addresses the issue. This publication suggests the use of;

- A value on 1×10^{-6} per year for the boundary between tolerable and broadly acceptable for the Individual Risk of fatality.
- A value of 1×10^{-3} per year for the boundary between tolerable and intolerable for the Individual Risk of fatality for a worker.
- A value of 1×10^{-4} per year for the boundary between tolerable and intolerable for the Individual Risk of fatality for a member of the public.

Another commonly used measure for tolerable risk is that of societal risk. This deals with events that can cause multiple fatalities. Again there is common practice and published guidance on the selection of tolerable risk values expressed in terms of societal risk; in particular the two HSE publications (both should be referred to) address the issue;

- Reducing Risks, Protecting People
- HID's approach to 'As low As Reasonably Practicable' (ALARP) decisions (SPC/Permissioning/09)

These documents suggest;

- An accident causing the death of fifty people or more in a single event should be regarded as intolerable if the frequency is estimated to be more than one in five thousand per annum.
- The unacceptable region: the region above the line of slope –1 through this point on the log F v log N plot.
- The broadly acceptable region: the region below a line two orders of magnitudes below and parallel to the above line.
- The tolerable if ALARP region lies between these two lines.

The two publications are both available from the HSE website;
http://www.hse.gov.uk/risk/theory/r2p2.htm
http://www.hse.gov.uk/comah/circular/perm09.htm