

IGEM/G/7
Communication 1655

Risk assessment techniques



Founded 1863
Royal Charter 1929
Patron: Her Majesty the Queen

IGEM/G/7
Communication 1655

Risk assessment techniques



IGEM/G/7 2016

Copyright © 2016, IGEN. All rights reserved
Registered charity number 214001

All content in this publication is, unless stated otherwise, the property of IGEN. Copyright laws protect this publication. Reproduction or retransmission in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

ISBN 978 1 905903 63 4

ISSN 0367 7850

Published by the Institution of Gas Engineers and Managers

Previous publications:
Communication 1655 (1999) IGE/SR/24

For information on other IGEN Standards please visit our website, www.igem.org.uk

CONTENTS

SECTION		PAGE
1	Introduction	1
2	Scope	3
3	Legal and allied considerations	5
	● 3.1 Health and Safety at Work etc. Act (HSWA)	5
	● 3.2 Environmental Protection Act (EPA)	5
	● 3.3 Construction (Design and Management) Regulations (CDM)	5
	● 3.4 Control of Major Accident Hazards Regulations (COMAH)	6
	● 3.5 Dangerous Substances and Explosive Atmospheres Regulations (DSEAR)	6
	● 3.6 Gas Safety (Installation and Use) Regulations (GS(I&U)R)	7
	● 3.7 Gas Safety (Management) Regulations (GS(M)R)	7
	● 3.8 Management of Health and Safety at Work Regulations (MHSWR)	7
	● 3.9 Pipelines Safety Regulations (PSR)	7
	● 3.10 Pressure Systems Safety Regulations (PSSR)	7
4	Hazards from the assets	9
5	Management of risk	10
	● 5.1 Risk management	10
	● 5.2 Risk assessment	11
6	Risk assessment techniques	14
	● 6.1 Hazard identification	14
	● 6.2 Risk analysis	16
	● 6.3 Risk evaluation	25
	● 6.4 Risk treatment	27
7	Applying risk assessment techniques	30
	● 7.2 Design	31
	● 7.3 Construction	32
	● 7.4 Commissioning	32
	● 7.5 Operation	33
	● 7.6 Decommissioning	33
	● 7.7 Demolition	34
	● 7.8 Specification of required safety studies	34
8	Causes of failure, protective measures and the consequences of failure by asset types	37
	● 8.2 Natural Gas	39
	● 8.3 LPG installations	56
9	Monitoring and review	65
	● 9.1 Process safety KPIs	65

● 9.2 Safety audits	65
● 9.3 Technical surveys	66
● 9.4 Risk registers	66
● 9.5 Investigating accidents and incidents	66
● 9.6 Acting on lessons learned	67

APPENDIX

1	Glossary, acronyms, abbreviations and units	68
2	References and further reading	70
3	Example and use of cost per life saved calculation	77
4	Example of HAZOP	78
5	Common hazards	82
6	HAZID checklist	83
7	Example of a simple risk assessment	86
8	Fault tree example	88

FIGURES

1	A risk management process map – The plan, do, check, act cycle	10
2	Contribution of risk assessment to the risk management process	11
3	First stage in fault tree development	17
4	Second stage in fault tree development	18
5	Event tree (illustrative only)	21
6	An example of a bow tie diagram	22
7	Sample FN criterion	26
8	Life cycle activities of a project	30
9	LPG cylinder filling operation	78
10	Example of a complete fault tree	88

TABLES

1	Risk severity against risk frequency	23
2	Example checklist for selecting FPSA studies	36
3	Risk assessment for rigid pipework, joints and components of OP not exceeding 2 bar	87

SECTION 1 : INTRODUCTION

- 1.1 This Standard supersedes IGE/SR/24, Communication 1655, which is obsolete.
- 1.2 This Standard has been drafted by an Institution of Gas Engineers and Managers (IGEM) Panel, appointed by IGEM's Gas Transmission and Distribution Committee, and has been approved by IGEM's Technical Co-ordinating Committee on behalf of the Council of IGEM.
- 1.3 Risk assessment is the assessment of health, safety and environmental aspects of a particular plant, process or activity (or part thereof) carried out using an established or specified format. Some assessments are specific requirements of health and safety legislation, for example the Dangerous Substances and Explosive Atmospheres Regulations (DSEAR), while others are carried out in order to assist in the management of safety and in discharging general legal responsibilities.

Note: Risk is defined as:

Likelihood of a specified undesired event occurring within a specified period or in specified circumstances, expressed as a frequency (rate of occurrence) or as a probability depending on the circumstances (see IGE/G/4).

- 1.4 This Standard covers the techniques used in risk assessment. The requirements provided are laid out in a general format. Specific problems may need more detailed treatment and the Standard provides the basis on which detailed procedures, appropriate to the circumstances, can be written.
- 1.5 It is widely accepted that the majority of accidents in industry are in some measure attributable to human as well as technical factors in the sense that actions by people initiated or contributed to the accidents, or people might have acted better to avert them.

It is therefore necessary to give proper consideration to the management of these human factors and the control of risk. To assist in this, it is recommended that due cognisance should be taken of HSG48 and HSG65.

- 1.6 The primary responsibility for compliance with legal duties rests with the employer. The fact that certain employees, for example "responsible engineers", are allowed to exercise their professional judgement does not allow employers to abrogate these primary responsibilities. Employers must:
- have done everything to ensure, so far as is reasonably practicable, that there are no better protective measures that can be taken other than relying on the exercise of professional judgement by "responsible engineers"
 - have done everything to ensure, so far as is reasonably practicable, that "responsible engineers" have the skills, training, experience and personal qualities necessary for the proper exercise of professional judgement
 - have systems and procedures in place to ensure that the exercise of professional judgement by "responsible engineers" is subject to appropriate monitoring and review
 - not require "responsible engineers" to undertake tasks which would necessitate the exercise of professional judgement that is not within their competence. There should be written procedures defining the extent to which "responsible engineers" can exercise their professional judgement. When "responsible engineers" are asked to undertake tasks which deviate from this they should refer the matter for higher review.

- 1.7 This Standard makes use of the terms “should”, “shall” and “must” when prescribing particular requirements. Notwithstanding Sub-Section 1.8:
- the term “should” prescribes a procedure which, it is intended, will be complied with unless, after prior consideration, deviation is considered to be acceptable
 - the term “shall” prescribes a procedure which, it is intended, will be complied with in full and without deviation
 - the term “must” identifies a requirement by law in Great Britain (GB) at the time of publication
- Such terms may have different meanings when used in legislation, or Health and Safety Executive (HSE) Approved Code of Practice (ACoPs) or guidance, and reference needs to be made to such statutory legislation or official guidance for information on legal obligations.
- 1.8 Notwithstanding Sub-Section 1.7, this Standard does not attempt to make the use of any method or specification obligatory against the judgement of the responsible engineer. Where new and better techniques are developed and proved, they are to be adopted without waiting for modification to the Standard. Amendments will be issued when necessary and their publication will be announced in the Journal of IGEN and elsewhere as appropriate.
- 1.9 Requests for interpretation of this Standard in relation to matters within its scope, but not precisely covered by the current text, are to be addressed in writing to Technical Services, The Institution of Gas Engineers and Managers, IGEN House, High Street, Kegworth, Derbyshire, DE74 2DA or by e-mail to technical@igem.org.uk and will be submitted to the relevant Committee for consideration and advice, but in the context that the final responsibility is that of the engineer concerned. If any advice is given by or on behalf of IGEN, this does not relieve the responsible engineer of any of his or her obligations.
- 1.10 This Standard was published in March 2016.

.....

SECTION 2 : SCOPE

2.1 This Standard covers hazard identification and includes assessing the consequences of failure along with risk assessment techniques in general and specifically addresses their application in the Natural Gas (NG) and Liquefied Petroleum Gas (LPG) gas industries.

2.2 This Standard covers aspects of risk assessments related to health, safety and the environment.

Note: Specific environmental risk assessment techniques are not detailed in this document, but the philosophy may be applied.

2.3 This Standard covers activities on systems associated with on-shore storage, transmission, distribution and utilisation of NG and LPG throughout their life cycle; that is design, construction, commissioning, operation, maintenance, de-commissioning and demolition.

Note: The principles may be applied to off-shore plant and equipment but specific requirements, for example escape and evacuation plans, are not covered.

2.4 This Standard embraces:

- hazards from assets
- management of the risks, including;
 - risk management
 - risk assessment.
- risk assessment techniques, including;
 - hazard identification
 - risk analysis
 - calculation of the risk
 - risk evaluation.
- applying risk assessment techniques in;
 - design
 - construction
 - commissioning
 - operation
 - decommissioning
 - demolition.
- causes of failure, protective measures and consequences of failure by asset types
- monitoring and review, including;
 - process safety key performance indicators (KPI)(s)
 - safety audits
 - technical surveys
 - risk registers
 - investigating accidents and incidents
 - acting on lessons learnt.

- 2.5 This Standard provides general rather than detailed requirements, gives an indication of who might be expected to carry out assessments and provides information for engineers and managers on where more detailed guidance can be found.

Note: Although the principles of controlling both safety, health and environmental risks are the same, their application often requires a different approach because of the nature of those risks. In particular, the identification of "safety" hazards often will necessitate the input of different specialist expertise compared to "health and environmental" hazards.

- 2.6 Pressures quoted are gauge pressures unless otherwise stated.

- 2.7 Italicised text is informative and does not represent formal requirements.

- 2.8 Appendices are informative and do not represent formal requirements unless specifically referenced in the main sections via the prescriptive terms "should", "shall", or "must".

.....

SECTION 3 : LEGAL AND ALLIED CONSIDERATIONS

This Standard is set out against a background of legislation in force in UK at the time of publication. The devolution of power to the Scottish, Welsh and Northern Ireland Assemblies means that there may be variations to the legislation described below for each of them and consideration of their particular requirements must be made. Similar considerations are likely to apply in other countries, where reference to appropriate national legislation is necessary.

All relevant legislation must be applied and relevant ACoPs, official Guidance and referenced Codes of Practice (CoPs), standards, etc. shall be taken into account.

Where British Standards etc. are quoted, equivalent national or international Standards, etc. equally may be appropriate.

Unless otherwise stated, the latest version of the referenced document should be used.

Appendix 2 lists in detail all references contained in this Standard.

This section addresses only the aspects of risk assessments relating to legislation.

The section deals primarily with gas related legislation. Other legislation will be of relevance when operating in other industries.

3.1 HEALTH AND SAFETY AT WORK ETC. ACT (HSWA)

3.1.1 HSWA applies to all persons involved with work activities, including employers, the self-employed, employees, designers, manufacturers, suppliers etc. as well as the owners of premises. It places general duties on such people to ensure, So Far As Is Reasonably Practicable, (SFAIRP) more usually referred to as As Low As Reasonably Practicable (ALARP) the health, safety and welfare of employees and the health and safety of other persons such as members of the public who may be affected by the work activity. The onus for deciding what is "reasonably practicable" and the responsibility for action, therefore, is placed on those who have direct influence, that is the management.

3.1.2 HSWA is an enabling Act, in that it provides for specific regulations to be made. Many of the regulations which have been made are particularly relevant to IGEN/G/7 as the implementation of risk assessment techniques is necessary to ensure compliance.

3.2 ENVIRONMENTAL PROTECTION ACT (EPA)

EPA makes provision for integrated pollution control. It also makes provision for control of air pollution by local authorities. Prescribed processes require authorisation and, in granting authorisation, the enforcing authority is required to ensure that the best available techniques not entailing excessive cost are employed to prevent or minimise the release of any substance prescribed for any environmental medium.

3.3 CONSTRUCTION (DESIGN AND MANAGEMENT) REGULATIONS (CDM)

3.3.1 CDM applies to the whole construction process on all asset construction projects from concept to completion and beyond. Duty holders include clients, designers, principal designers, principal contractors, contractors and individual workers. Foreseeable risks, such as those that may arise during construction work or in maintaining and using the asset once it is built are required to be eliminated, reduced or controlled.

Note: L153 provides an ACoP and Guidance on CDM

Construction includes the alterations, repair, redecoration, maintenance, de-commissioning or demolition of a structure. It also covers installation, commissioning, maintenance or removal of gas services.

3.3.2 CDM require the client to appoint a principle designer who will co-ordinate the health and safety aspects of the design and planning phases and ensure that a Safety Plan is prepared which contains health and safety information obtained from clients and designers. The information will include items of importance during the construction phase of a project to include the contractors' health and safety policy and their assessment of the risks identified and created during the progress of the project works.

3.3.3 CDM direct the timing of the introduction of risk assessments to the design phase and, for construction work activities, require that a named individual, that is the principal contractor, takes overall responsibility for the manner in which the assessments are actioned.

3.4 **CONTROL OF MAJOR ACCIDENT HAZARDS REGULATIONS (COMAH)**

3.4.1 COMAH applies to sites with defined inventories of specified dangerous substances, and places much emphasis on risk assessment.

3.4.2 For larger sites ("Upper Tier" Sites), COMAH require the preparation of a Safety Report, an emergency plan (both internal and external) and the provision of information to the public.

The Safety Report is an extensive document which has to provide information about the dangerous substances involved, the installation, the management system and potential major accidents, and demonstrate that the measures taken to prevent, control and minimise the consequences of any major accident, reduce the risks to "As low as reasonably practicable (ALARP)".

3.4.3 For smaller sites ("Lower Tier" Sites), demonstration of safe operation is necessary. COMAH require that operators are able to demonstrate that they have identified the major hazards arising from their activities and have taken adequate steps to prevent such accidents.

3.4.4 Many of the assessments described in this Standard assist in discharging the obligations under COMAH.

Note: Further information including the scope of the Regulations is given in L111.

3.5 **DANGEROUS SUBSTANCES AND EXPLOSIVE ATMOSPHERES REGULATIONS (DSEAR)**

DSEAR are concerned with protection against risks from fire, explosion and similar events arising from dangerous substances used or present in the workplace. DSEAR require that risks from dangerous substances are assessed, eliminated or reduced. They contain specific requirements to ensure employees are properly informed and trained to control the risks from the use of dangerous substances. DSEAR also require the identification of pipelines and containers containing dangerous substances.

Note: The following contain details of DSEAR and their application:

- L138
- INDG370.

3.6 **GAS SAFETY (INSTALLATION AND USE) REGULATIONS (GS(I&U)R)**

GS(I&U)R are relevant statutory provisions of HSWA setting out general and detailed requirements dealing with the safe installation, maintenance and use of gas systems, including gas fittings, appliances and flues.

Note: Further information is given in L56.

3.7 **GAS SAFETY (MANAGEMENT) REGULATIONS (GS(M)R)**

GS(M)R place specific duties on gas transporters (GTs) or their emergency service providers (ESPs), for dealing with gas escapes from pipes on their network. Their primary duty is to make the situation safe. They are responsible not only for dealing with escapes from their own pipes, but also for dealing with escapes from gas fittings supplied with gas from pipes on their network. In GS(M)R, the term "gas escapes" includes escapes or emissions of carbon monoxide (CO) from gas fittings.

A further obligation to undertake risk assessments is expressed in GS(M)R as a part of a Network Safety Case submission to regulatory authorities. In part it also requires duty holders to address the risks from escapes and the management of the network such as those covered by safe control of operations procedures. The risk requiring assessment in this case is the security of gas supply to the domestic consumer, which includes the specification of the "gas composition", assessed as suitable to enable the safe and reliable operation of correctly installed and maintained gas installations.

Note: Further information is given in L80.

3.8 **MANAGEMENT OF HEALTH AND SAFETY AT WORK REGULATIONS (MHSWR)**

MHSWR impose a duty on employers and the self-employed to make assessments of risks to the health and safety of employees, and non-employees affected by their work. They also require effective planning and review of protective measures.

3.9 **PIPELINES SAFETY REGULATIONS (PSR)**

PSR require the preparation of a Major Accident Prevention Document (MAPD) for pipelines conveying "dangerous fluids". This document is required to include an identification of the hazards and an assessment of the risk associated with the pipeline.

Note: Further information is given in L82.

3.10 **PRESSURE SYSTEMS SAFETY REGULATIONS (PSSR)**

3.10.1 These Regulations impose duties on designers, importers, suppliers, installers and users or owners to ensure that pressure systems do not give rise to danger. This is done by the correct design installation and maintenance, provision of information, operation within safe operating limits and, where applicable, examination in accordance with a written scheme of examination drawn up or approved by a competent person (as defined in PSSR).

3.10.2 Relevant fluids for the purposed of this document would be NG at a pressure greater than 0.5 barg that is, above atmospheric pressure, or LPG (which is a liquid with a vapour pressure greater than 0.5 barg at ambient temperature). A pressure system would include bulk storage tanks, pipelines and protective devices but not an LPG cylinder (transportable pressure receptacle). Once the pressure in the pipework drops below 0.5 barg, and the user/owner can show clear evidence that the system does not contain, and is not liable to contain, a relevant fluid under foreseeable operating conditions, then that part of the

system is no longer covered by the Regulations. This is likely to be the case after the pressure relief valve associated with a pressure reducing valve which takes the pressure to below 0.5 barg, for example at the entry to a building but note the special requirements placed on protective devices in such systems (see para 110b of L122). The regulations also apply to pipelines and the protective devices in which the pressure exceeds 2 barg (see Sch 1 part 1 item 5 of L122).

- 3.10.3 More information is available in L122 and some information is presented in the HSE free leaflets INDG261 and INDG178.

Copyright Institution of Gas Engineers & Managers
Provided by IHS Markit under license with IGHM
No reproduction or networking permitted without license from IHS

SECTION 4 : HAZARDS FROM THE ASSETS

An NG fuel system usually commences from an onshore gas reception or liquefied gas terminal, then the gas is transported through a high pressure transmission underground pipeline system, incorporating installations such as compressor stations, multi-junction and block valve stations. The pressure is progressively reduced in a succession of pressure reduction installations as the gas is distributed to the point of use. The transmission and distribution system includes facilities for storage. The gas is then metered before its use on customer's premises.

An LPG system normally commences at a refinery, where it is contained in bulk storage. From the refinery the LPG is transported by road, rail or pipeline to local storage facilities or vehicle fuel stations. It is then transferred to cylinders or by road tankers to the user local storage tank. In some cases, there will be local distribution through metered estates.

This section describes the hazards presented from the system; situations which pose a hazard to the system are in the context of this document described as failure causes.

The hazard for all assets is a gas, vapour or liquid release, which could lead to:

- fire leading to flame contact, thermal radiation or escalation to involve property
- a build up of a flammable mixture in an enclosure leading on ignition to both flame and overpressure which in turn can result in structural damage
- a build-up of unignited or non-flammable gas resulting in an asphyxiation and/or toxic hazard
- incomplete combustion leading to the production of CO
- escalation from a small (ignited) release to involve adjacent pipes and vessels leading to a more serious failure (including boiling liquid expanding vapour explosion (BLEVE) where vessels containing pressurised flammable liquids are involved)
- vapour cloud leading on ignition to flash fire or unconfined vapour cloud explosion
- severe cold burns from pressurised liquids above their boiling point.

4.1 The approach to risk management, the role of risk assessment, the techniques, tools and methods available and the specific application of these to the individual sections of the supply systems through their life cycle are described in the following sections. Individual sections describe the measures that should be taken to prevent these hazards arising or mitigate their impact.

Copyright Institution of Gas Engineers & Managers
 Provided by IHS Markit under license with IGHM
 No reproduction or networking permitted without license from IHS
 Not for resale

SECTION 5 : MANAGEMENT OF RISK

5.1 RISK MANAGEMENT

5.1.1 Risk management is defined in BS ISO 31000 as co-ordinated activities to direct and control an organisation with regard to risk, and carried out in a risk management framework. This Standard outlines a set of components for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The process should involve the application of policies, procedures and practices to communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

5.1.2 HSG65 'Managing for Health and Safety' describes the Plan, Do, Check, Act process for the management of health and safety risk (see Figure 1). It also discusses the importance of leadership in managing health and safety, and of competence in identifying, assessing and communicating risks and implementing controls.

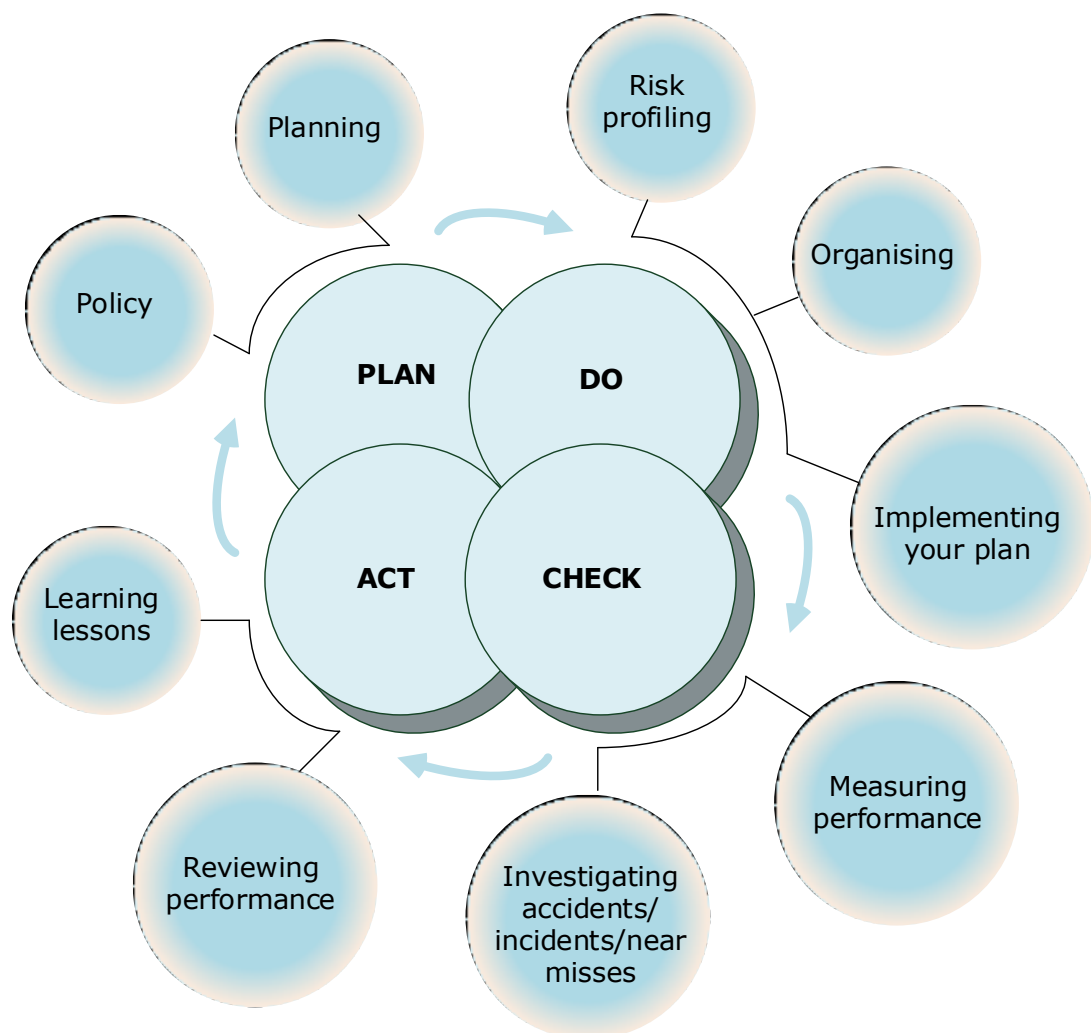


**FIGURE 1 – A RISK MANAGEMENT PROCESS MAP –
THE PLAN, DO, CHECK, ACT CYCLE FROM HSG65**

Plan, Do, Check, Act should not be seen as a once-and-for-all action. The cycle may need to be implemented more than once, particularly when:

- initiating a new design
- developing a new process
- implementing any change to the process.

5.2 RISK ASSESSMENT

5.2.1

Risk assessment is an essential part of risk management. It provides decision makers and responsible parties with an improved understanding of risks that could affect the achievement of objectives, and the adequacy and effectiveness of controls already in place. This should provide a basis for decisions about the most appropriate approach to be used to treat risks. The output of risk assessment is an input to the decision making processes of the organisation.

Risk assessment comprises those elements of the risk management process incorporating risk (or hazard) identification, risk analysis and risk evaluation (see Figure 2).

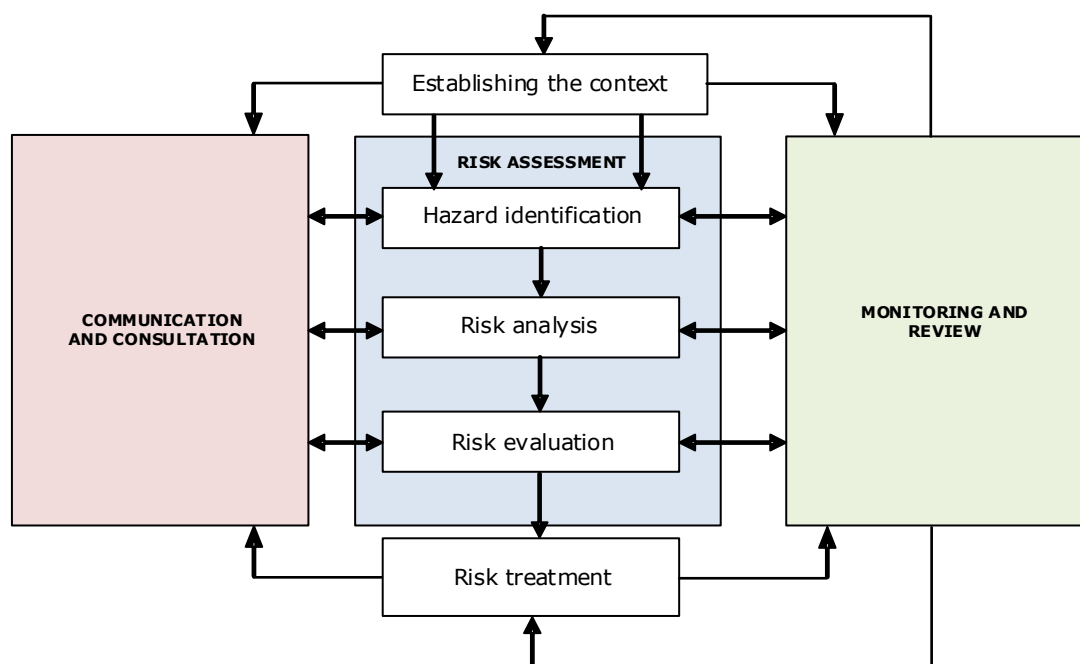


FIGURE 2 – CONTRIBUTION OF RISK ASSESSMENT TO THE RISK MANAGEMENT PROCESS (FROM BS EN 31010)

5.2.2

Regardless of the type of activity being assessed, the principles of risk management are the same. In general terms, the steps based on INDG163, are:

- identify the hazards
- decide who might be harmed, and how
- evaluate the risks and decide on precautions
- record findings and implement them
- review assessments and update, if necessary.

The level of detail should be proportional to the risk presented. The simple process above is adequate for normal or everyday activities. Where there are significant hazards or risks, complex plant, uncertainties or where the straightforward application of industry standards and CoPs do not provide a sufficient demonstration that the risk from the activity is ALARP, the process should be applied in a more structured quantitative way. However, the logical approach to risk assessment set out here is applicable whatever the level of complexity of the equipment or operation.

A more structured approach should take the following form:

Hazard identification

- classify the process or activity
- identify the hazards
- identify people at risk.

Risk Analysis

- assessment of frequency
- assessment of consequences.

Risk Evaluation

- identify existing control measures
- determine risk
- assess significance of risk
- identify any required risk treatment and implement
- record results.

5.2.3 In Figure 2, the risk assessment is followed by a process referred to as Risk Treatment. In practice, this process is not confined to the end of the overall process but is carried out throughout. An important element of risk treatment is the reduction of the hazards implemented by, for example, elimination or substitution. The principle of inherent safety (see clause 6.4) should be applied. The hierarchy of risk reduction measures (see clause 6.4) should also be applied. Where the treatment is aimed solely at reducing risk, it is more usually termed Risk Mitigation.

The risk treatment referred to, relates to the hazards and risks presented by the installation in order to develop an acceptable design. However, this still results in a residual risk which could be imposed on the surrounding population. Further mitigation of the risks, which are a function of the population in the vicinity of the installation should be addressed through land use planning advice and emergency planning. These are not discussed in detail in this document.

5.2.4 The assessment process should be iterative at each stage. For example, after implementing risk treatment, consideration shall be given to carrying out a re-assessment. The process continues until the outcome satisfies both legal and industry acceptability criteria.

5.2.5 The risk assessment, and where necessary, the additional elements of the risk management process, should be reviewed periodically and updated, if necessary.

5.2.6 More details are given on hazard identification in Sub-Section 6.1, on risk analysis in Sub-Section 6.2, on risk evaluation in Sub-Section 6.3, on risk treatment in Sub-Section 6.4, and risk criteria in clause 6.3.1. The requirements for monitoring and review are in Section 9.

This more detailed structured process to risk assessment should demonstrate that:

- the equipment/installation conforms to legislation, standards, design codes and industry best practice
- all failure causes and failure modes have been considered
- the assessed failure frequencies are not directly unacceptable
- failure consequences are not directly unacceptable
- all protective measures have been considered

- residual risk has been calculated
- mitigation measures have been considered
- the assessed risks and predicted losses conforms to relevant individual, societal and company criteria (see Sub-Sections 6.2 and 6.3)
- legal requirements (ALARP) have been satisfied.

5.2.7 The risk assessment should assess the Individual Risk (IR) to both workers on the installation and to the surrounding population; the Societal Risk (SR), normally concerned more with the surrounding population; the predicted risk reduction of possible mitigation measures, and the (cost) benefit of their implementation.

5.2.8 Judgement shall be employed by the risk assessor at all stages of the assessment. IGEN/G/7 is intended to support the application of expert judgement and provide guidance on industry recognised tools and techniques that can be used to identify potential hazards and assess the risks associated with these hazards. It is essential that the assessor is able to justify the approach taken and every key assumption made in the assessment. These key assumptions should be documented as a part of the risk assessment.

SECTION 6 : RISK ASSESSMENT TECHNIQUES

This section covers the risk assessment techniques that are used singly or in combination depending on the type of problem being addressed. The ones most commonly used for gas industry applications are described here in general terms. More detailed descriptions can be found in BS EN 31010, which gives detailed descriptions of a comprehensive range of techniques, or in IChemE Hazard identification methods, which deals with those methods in common use in the process industries.

6.1 HAZARD IDENTIFICATION

A key part of the risk assessment process should be hazard identification. It is now common practice in industry to undertake hazard identification exercises in the form of a range of studies often referred to Formal Process Safety Assessments (FPSAs) or Process Hazard Analyses (PHAs). The most frequently used techniques that can be applied including hazard identification study (HAZID) and hazard and operability study (HAZOP) are discussed in this Section.

6.1.1 Hazard identification is the process of finding, recognising and recording hazards.

The purpose of hazard identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the proposed design. They generally involve the relevant engineering disciplines that have been involved with the design working together as a team and systematically applying a series of guidewords in order to identify any unprotected hazards. The aim is to identify these unprotected hazards at an early stage in the design so that the associated risks can be identified, assessed and, if required mitigated against.

Hazard identification should be carried out throughout the different design phases of a project (see Section 7). However, any design changes required as a consequence of these studies will generally have less impact on the overall project cost if they are identified at the earlier stages of the project. It is therefore often appropriate to undertake these studies at the earliest possible stage even if some of the detailed design information is not available.

6.1.2 A range of hazard identification methods has been developed to provide a structured approach which seeks to ensure that all relevant hazards have been identified and hence can be assessed and managed. These methods should include:

a) *HAZID Checklists*

A HAZID study is a structured assessment technique using guidewords that aims to identify potential hazards arising from the design, siting and operation of the plant. During the HAZID study, the proposed design is systematically examined using the guidewords to generate free ranging discussion to identify potential safety or environmental issues. A checklist with guidewords is provided in Appendix 6.

For a large plant, it is often appropriate to split the plant into a number of plant sections or units and apply the checklist to each plant section in turn.

b) *What if, or structured what if (SWIFT), checklist*

Considers the elements of the installation and applies 'what if' questions based on the type of installation and the likely hazards, identified by 'expert judgements' or 'brainstorming' or from a prepared structure set of

questions. The questions and the responses are recorded for further assessment.

c) *Failure modes and effects analysis (FMEA)*

Considers the failure mode for each item of equipment together with the effect of the failure (consequences). An extension of this also considers the criticality of the failure event (FMECA) (see BS EN 60812).

The above techniques are not concerned with the frequency or the assessed consequences nor of interactions. From the results, the non credible and trivial events can be identified and excluded from further analysis, while the significant events and failures can be progressed for further analysis or investigation.

d) *Design Reviews*

Normally include the identification of barriers or mitigation measures; this could be done by using Bow Tie analysis (see clause 6.2.2.1 f)).

e) *HAZOP*

HAZOP is a more detailed hazard identification technique, normally requiring detailed design drawings (ELD, P&ID), hence is carried out later in the design process than the previous methods. Detailed guidance on HAZOPS is given in IChemE 'A guide to hazard and operability studies' and BS IEC 61882.

The aim of a HAZOP is to identify any potential hazard or operating difficulty in the design of a plant and to agree any necessary actions. It is a powerful tool for identifying the hazards that can arise due to the complex manner in which vessels and other items of plant interconnect. It also helps to identify unexpected hazards that can migrate to other parts of a plant owing to deviations in process parameters such as a change of flow rate.

A HAZOP is a team based exercise which addresses the process with regard to all systems that form the process. As an example, these will be expressed as the fuel gas system, the flue gas system, the waste heat recovery system, etc. Each system is examined on a section-by-section basis in a logical progression from start to finish of the system by applying a series of guide words such as 'more' or 'reverse' and recording the effect of these, taking into account interconnections, trips, safety devices, etc.

A fully documented HAZOP report should be retained for the lifetime of the plant. It will provide a valuable reference document for subsequent plant modifications and improvements and also for preparing various sections to meet the relevant requirements of the COMAH safety report (see Sub-Section 3.4). The HAZOP may need to be reviewed before a plant is modified or in the event of other material changes.

From the outcome of the HAZOP design, improvements are proposed and evaluated, and critical parts of the system are identified for specific detailed assessments.

6.2 RISK ANALYSIS

A range of qualitative and quantitative methods is available and should be used to establish the relative importance of the predicted frequency, predicted consequences, the risks from the hazards that have been identified.

6.2.1 Assessment of frequency

a) *Historical Databases*

Databases are available and are maintained covering a range of systems, plants and events, and are at component, system and plant level. From these, an assessment or indication of the likely frequency of the event being considered shall be gained, or a number of equipment failure rates which can be used in, for example, a fault tree analysis. There are limitations to the use of databases: they are historical hence can be limited for novel equipment or where applications have changed over time plus the data may not be a good enough match in type or application.

b) *Testing*

In certain cases, it should be possible to obtain failure rate data by carrying out specific testing of components.

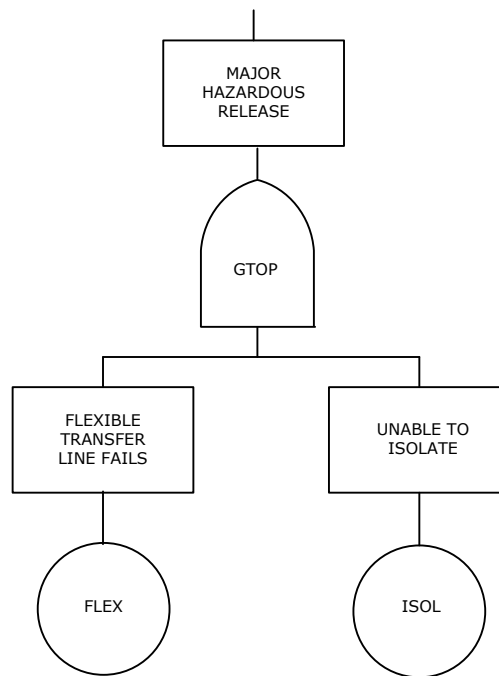
c) *Failure modelling*

Where relevant failure data is not available e.g. for plant items where there is no direct historical experience, or where the failure frequency is very low, any historical data would not be statistically reliable. The failure frequency should be predicted by using non failing data on damage, corrosion, fatigue cycling, thermal stresses, etc. and suitable growth models, supported by experiment where possible.

d) *Fault Tree Analysis*

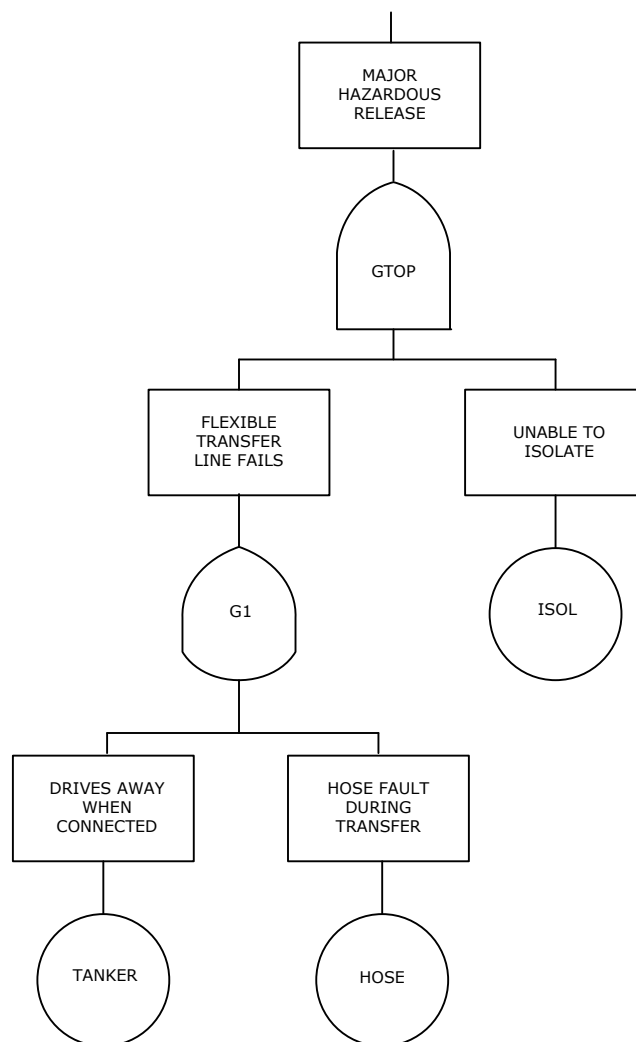
Fault trees enable each of the contributions to a hazardous event to be modelled in a logical structure and the relative importance of each contributing event to be evaluated. When a fault tree has been constructed, probabilities should be assigned to each of the basic events and then an assessment made of the probability (or frequency) of the top event. Using this technique, a top-down approach models the top event in terms of combinations of contributing events. Figure 3 illustrates the first level of this top-down fault tree approach to a major LPG release during road tanker loading. The cause can be seen to be the coincident failures of the flexible transfer line AND an inability to isolate the release. BOTH of these events are necessary for the top event to occur and if either occurred alone then the top event would not materialise. Each of these two events can, in turn, be modelled as shown in Figure 4 for the line failure. The failure of the line may be caused by an unrevealed fault which becomes evident during the transfer or by the driver moving away while still connected. Fault trees can be limited by the need for a failed/not failed logic and it being a static approach – no time dependencies (see BS EN 61025).

The AND/OR gate logic of the fault tree is sometimes expressed in an equivalent reliability block diagram (RBD) approach. The calculation of reliability uses the same mathematical techniques as the fault tree. The choice between these two methods is, usually, one of familiarity and preference on the part of the analyst.



Key: *FLEX* – flexible connection
ISOL – isolator switch or valve
GTOP – top gate

FIGURE 3 – FIRST STAGE IN FAULT TREE DEVELOPMENT



Key: G1 – flexible connection
ISOL – Isolator switch or valve
GTOP – top gate

FIGURE 4 – SECOND STAGE IN FAULT TREE DEVELOPMENT

e) *Simulation*

Fault tree, RBD and Event tree models are deterministic in that they provide one answer based on the mathematical model they represent together with the failure rate and repair time data input to them.

In more complex scenarios, the failure rate may not be constant, the repair time distribution may be unusual, the model may change with time, etc. In these cases, a deterministic approach is not always adequate and more sophisticated computer simulation techniques, including Monte Carlo (random sampling) methods, should be adopted.

f) *Human factors analysis*

Where direct human involvement, for example in operations or maintenance, is a significant part of the process, the likelihood of failure due to human error should be estimated from a range of structured methods. For a review of the methods, see HSE RR679. From such an analysis, the acceptability of the operation, the requirement for ergonomic improvements, or the support of an alarm or trip should be identified.

g) *Software reliability analysis*

Control and protection systems are increasingly software controlled. Safety critical software is typically written in a structured testable format and should be validated and, if required, certificated for example in terms of the Safety Integrity Level (SIL) (see clause 6.4.3 below and BS EN 61508-5).

6.2.2 **Assessment of consequences**

The term consequences here relates to the physical properties of the release from containment of the hazardous fluid or material from which the effects on the surrounding people, plant and property should be assessed (see references Lees, Harris, A.IChemE CCPS).

6.2.2.1 Consequence analysis should be carried out in order to assess the outcomes or impact of the realisation of the range of hazards identified in the plant or process. It should be ensured that there are safeguards in place (hardware or procedural) that are appropriate to these hazards. A full appreciation of the hazards begins with identifying the range of release scenarios which should include:

- discharge from relief and vent systems
- corrosion leak
- impact puncture
- small bore fitting failure
- pipe rupture (of a range of sizes and pressure if appropriate)
- total loss of containment from a vessel rupture (up to and including the largest single item containing each category of dangerous substance).

The consequences of these releases shall be mainly:

- a release rate, either steady state or time varying, leading to a dispersing jet or cloud of flammable or toxic gas or vapour, which in turn can lead to:
 - (unconfined) vapour cloud explosion
 - fireball
 - flash fire
 - steady state fire
 - toxic cloud
 - build-up of flammable mixture
 - confined explosion.

The consequences listed above can also give rise to an escalation of the event such as an explosion resulting in further failures and loss of containment, or a jet fire impacting on an adjacent pipe or vessel leading to a more serious release, including a BLEVE where a vessel containing a pressurised liquid is involved.

An unconfined vapour cloud explosion is possible if the combustible cloud drifts into a congested part of the plant or an adjacent plant where the flame front from an ignited cloud can accelerate up to a flame speed capable of producing destructive over-pressures. In the open air, a vapour cloud explosion is unlikely in the case of NG, and the most credible consequence is a flash fire flashing back to the source of release followed by a steady state fire. A fireball is likely from a massive release of material from a vessel rupture where an ignition source is encountered before any appreciable mixing with the surrounding air has occurred. Steady state fires include jet fires and pool or tank bund fires.

The prediction of the consequences of a release involve the physical properties of the material released; the behaviour of the material on release; the interaction with the atmosphere, the ground, and any surrounding plant, property or topographical features; and for flammable fluids, the behaviour on ignition.

The behaviour of fluid release from containment, dispersion in the atmosphere, interaction, and combustion are complex processes which cannot be predicted with confidence other than in simple or relatively small scale situations. Consequence predictions are therefore obtained from a range of empirical, analytical or combined approaches normally represented as equations or software models depending on the complexity. The predictions have improved over time as more detailed experiments have been conducted and developments in computational fluid dynamics (CFD) have taken place, however even with CFD, validation against experimental data is still normally required.

Due to the sequential nature of the realisation of some of the hazard scenarios, and the fact that a single release may have a range of consequences, their treatment in a risk assessment often requires the development of an event tree.

a) *Event tree analysis*

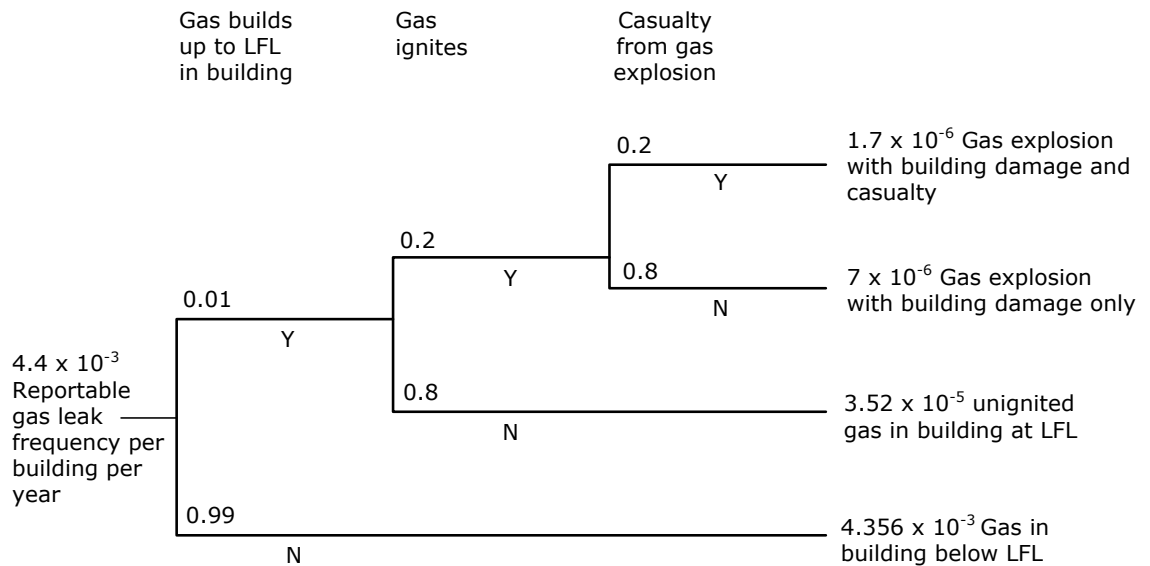
Event trees should be used as a systematic way of developing and identifying all of the possible outcomes from an initial hazardous event and includes the time sequence of the development of the consequences. The example of a release of gas from a small bore pipe in a building is shown in Figure 5. The initial event is the release itself.

There are then two possibilities to be considered for the next event and these are determined by asking whether or not the release will build up to lower flammability limit (LFL) in the building. The decision on ignition is the next branch in the Event Tree. Each new branch of the tree can then be analysed for possible outcomes, producing even more branches of the tree and leading to all possible outcomes. The normal convention is for the positive (yes) outcome of the branch to be at the top with the negative (no) outcome below.

If probability data is available or can be estimated, it is possible to quantify the outcome of the hazardous event. An event frequency for the initial event has to be determined. Then, if probabilities are assigned for each of the branching points, the frequency of each branch can be calculated in order to rank the risks and identify the most appropriate control measures. The probabilities given in Figure 5 are only for illustrative purposes (see BS EN 62502).

Copyright Institution of Gas Engineers & Managers

Reportable gas leak in building

**FIGURE 5 – EVENT TREE (ILLUSTRATIVE ONLY)**b) *Effect/impact*

The output from the consequence analysis should be a physical measure of concentration, thermal radiation or overpressure at a range of distances from the failure. This output is used to determine the effect (or impact) on the surrounding plant, property and population from which the casualty probability of the surrounding population should be estimated, which can then be combined with the associated failure frequencies and event probabilities to enable the risk to be calculated.

The effect of a specific consequence on a person can be almost instantaneous as with an explosion overpressure, or may be cumulative as with thermal radiation or toxic effects. The expected measure of harm would be risk of death. However, this is not easy to calculate with any certainty due to the wide variability of the susceptibility of those affected. To simplify assessments, it has been the convention to define a harm level which represents a casualty, with an understanding of how this might relate to the average likelihood of the person becoming a fatality. This requires the availability of a dose response relationship from which a threshold value relating to the selected measure can be defined. A measure of the risk of death can be obtained from a representation of the dose response relationship in the form of a probit. Historically, a value of "1% lethality" was used, more recently a value representing 50% fatality, or LD₅₀, has been used in order to improve the summation of risks from sites with mixed hazards.

It is to be noted that the IR criteria in R2P2 are based on the historical risk of death. Risk assessments used by the HSE for Land Use Planning purposes have retained the use of the "1% lethality" casualty criterion.

Note: The land use planning casualty criterion is also referenced to as "dangerous dose".

When assessing the probability of casualty, the effects of shelter and escape on the received dose should be taken into account.

c) *Calculation of risk*

Risk analysis is the combination of the frequency and consequence analyses. The complexity, and the degree of quantification, will be related to the significance of the results of the frequency and consequence analysis carried out and the complexity or severity of the outcome of the event(s) considered. A range of qualitative and semi-quantitative approaches are available in addition to the more comprehensive quantitative (or quantified) risk assessment or QRA.

d) *Qualitative methods*

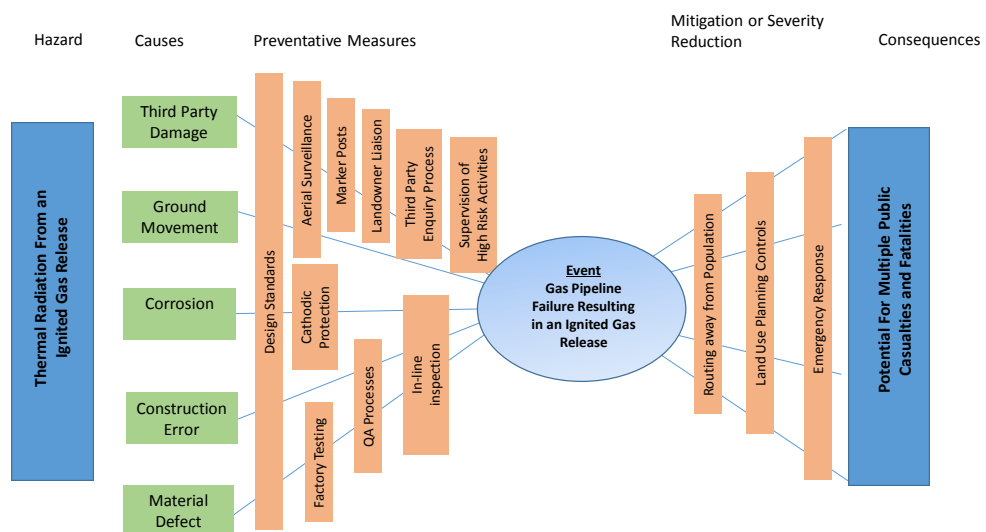
These methods present or combine the causes of an event with their consequences but do not quantify either the frequency of the event occurring or the extent of the consequences.

e) *Cause consequence analysis*

This should incorporate the time related consequences into a fault tree configuration so as to combine the logic of an event tree with that of a fault tree. It is more suitable where the consequences can be represented in a YES/NO logic since the extent of the consequences, such as in a gas release and fire, are not quantified.

f) *Bow tie analysis*

This should be a graphical representation of the pathways from causes through to consequences. (See Figure 6) For each identified hazard, all of the failure sequences or combinations leading to the hazard being realised are separately drawn leading from the left towards the hazard located at the centre of the diagram, and each event sequence leading from the hazard fan out to the right from the hazard. For the cause sequences, the barriers to the failures shall be marked and for the consequences the mitigations shall be marked.



Key: QA – Quality assurance

FIGURE 6 – AN EXAMPLE OF A BOW TIE DIAGRAM

6.2.2.2 Semi-quantitative methods

These methods should include an assessment of the frequency of the event and the extent of the consequences, generally in terms of a scale, or range, of frequency and of severity. The quantification should be extended, or calibrated, based on generic failure frequency data, consequences predictions, or the outcomes of previously performed QRAs.

a) Risk ranking

Here, risk shall be the combination of the severity of the hazard and the likelihood of occurrence.

Consequence, or severity is ranked from slight to major on a suitable scale, for example from 1 to 3 equating to slight, serious or major. The likelihood of occurrence is ranked from highly unlikely to likely on a suitable scale, for example from 1 to 3.

Risk can also be expressed as a single figure when numerical values for the hazard and likelihood have each been assigned.

Note: For example, the risk ranking of a work activity which will frequently result in personal injury resulting in more than 3 days incapacity to work would be a factor of:

$$3 \text{ (serious hazard)} \times 3 \text{ (high likelihood)} = 9 \text{ (risk ranking)}$$

A higher risk would be present if more than one individual could be harmed. The more onerous nature of risk may be taken into account by multiplying the risk value by the number of persons at risk.

b) Risk matrix

Here, the level of risk should be established by presenting the hazard severity and likelihood as in Table 1. The table deliberately uses different terms for severity to those used in clause 6.2.2.2.a) to illustrate the flexibility of the simple approach.

SEVERITY FREQUENCY	SLIGHTLY HARMFUL RISK	HARMFUL RISK	EXTREMELY HARMFUL RISK
HIGHLY UNLIKELY	Trivial	Minor	Moderate
UNLIKELY	Minor	Moderate	Substantial
LIKELY	Moderate	Substantial	Severe

TABLE 1 – RISK SEVERITY AGAINST RISK FREQUENCY

The frequency axis is often expressed in terms of orders of magnitude per year.

6.2.2.3 Quantitative (QRA)

QRA shall combine the assessment of frequency with the consequences for each identified event and the effect (or impact) of the consequences to the surrounding plant and population. The frequency of the event from all causes should be factored by the probabilities relating to, for example, ignition probability, shutdown