UKOPA

United Kingdom Onshore Pipeline Operators' Association

UKOPA Good Practice Guide

A Guide to Pipeline Process Safety Studies and Methodologies

UKOPA/GPG/35 Edition 1

October 2020

GUIDANCE ISSUED BY UKOPA:

The guidance in this document represents what is considered by UKOPA to represent current UK pipeline industry good practice within the defined scope of the document. All requirements should be considered guidance and should not be considered obligatory against the judgement of the Pipeline Owner/Operator. Where new and better techniques are developed and proved, they should be adopted without waiting for modifications to the guidance in this document.

Comments, questions and enquiries about this publication should be directed to:

UK Onshore Pipeline Operators' Association
Pipeline Maintenance Centre
Ripley Road
Ambergate
Derbyshire
DE56 2FZ

E-mail: enquiries@ukopa.co.uk

Website: www.UKOPA.co.uk

Revision and change control history

Planned revision: 2025

Edition	Date	No. of pages	Summary of changes
1	October 2020	35	Issued for use

CONTENTS

1. INTRODUCTION

1.1 Background

The United Kingdom Onshore Pipeline Operators' Association (UKOPA) was formed in 1996 by operators of high pressure pipelines transporting, oil, refined liquids, natural gas, petrochemical liquids and gasses, in order to provide a forum for discussion, knowledge sharing and promotion of good practice across the industry. UKOPA provides a recognised expert industry voice to influence the development of legislation and standards and helps pipeline operators to develop a consistent view of strategic issues that relate to the safe operation and maintenance of onshore pipelines.

The Process Safety Working Group (PSWG) is formed from representatives of the member organisations, and focuses on providing information, direction, and guidance on pipeline process safety matters. PSWG identified the need to develop a pipeline process safety guide to aid members in selecting appropriate safety studies for use within their various areas of operation.

1.2 Scope

This document is designed to provide pipeline operators with guidance in selecting useful and appropriate process safety methodologies and techniques to identify pipeline hazards, and assess and control risks, throughout the asset's lifecycle.

The guide covers the main lifecycle stages of the asset, and for each pipeline lifecycle stage it describes the process safety techniques that could be considered, as well as describing the outputs that the techniques would produce, and potential uses for the outputs.

1.3 Legislative and Regulatory Requirements

The guidance within this document is not designed to ensure compliance with the HSE Pipelines Safety Regulations 1996 (PSR 1996), and should not be considered as a checklist for producing a Major Accident Prevention Document (MAPD), or any other regulatory required documents such as a Control of Major Accident Hazards (COMAH) report.

1.4 Application

This document can be used by members of UKOPA to aid the selection of safety studies, relative to the project requirements and pipeline lifecycle phase. The guide is provided as an aid to decision making and should not be treated as a definitive guide to when particular studies should be conducted, as this will vary by project, risk level, operator, asset age and/or whether the necessary information is available. Rather it provides an overview of applicable techniques, as well as some indicative timings for studies.

The guide is intended for use in new projects, turnkey projects, or to be retrospectively applied for older or existing assets. Where the guidance is applied for mature assets, the techniques can be utilised as required. For example, where studies may not have been performed during the original implementation of the project and specific types of assessment are not available (e.g. quantitative risk values) or where a study is needed to assess any changes or modifications to the operation of the asset.

The studies and techniques within the guide are described at a high-level with the intent of being useful for all members of UKOPA. Therefore, the list should not be considered as exhaustive, as there may be specific studies required to be performed by individual members which are not discussed within this document.

The names of the studies, and the terms used within this document more generally, may vary between organisations and may be different from those used within the following sections.

1.5 Glossary

Cause	Event, situation, or condition that results, or could result, directly or indirectly in an accident or incident.
Checklists	Structured and methodical lists to enhance the process of brainstorming in identifying hazards. Checklists may be structured by hazard categories, causes, consequences, activities, incident scenarios, etc.
Consequences	Potential effects which could occur as a result of a hazard. Consequence descriptions are qualitative or quantitative estimates of the accidental effects on people, assets/production or the environment.
Controls (or Safeguards)	Device, system, or action that would likely interrupt the chain of events following an initiating cause or that would mitigate loss event impacts. Safeguards are risk control barriers. Safeguards can be preventative or mitigative.
ENVID	Environmental Hazard Identification - the process of identifying credible environmental impacts and hazards associated with a facility, operation, or activity.
Harm	Physical injury or damage to the health of people, assets/production, or the environment.
Hazard	Potential source to cause of harm to people, assets/production, or the environment. Hazards can result from the inherent properties of an installation or from unsafe work practices.
HAZID	Hazard Identification - the process of identifying credible and conceivable hazards associated with a facility, operation, or activity. HAZID is sometimes used to describe the process of screening hazards to develop a high level hazard register.
Inherent Safety	Inherent safety is the avoidance/removal of hazards as oppose to controlling them. An inherently safer design may avoid hazards by reducing the amount of hazardous material and the number of hazardous operations, or by choosing not to use hazardous materials when alternatives are available.
Likelihood	The number of occurrences of a hazardous event per unit time (frequency) or per possible cases (probability).
Major Accident/ Major Accident Hazards	Major Accidents/ Major Accident Hazards are those with the potential to cause multiple fatalities, significant effects on the Environment, result in major asset damage, and/or result in major media coverage/ reputational damage.
Mitigative	A mitigative safeguard/control acts to reduce the impact of an event after the incident or accident has occurred, e.g. fire and gas detection, Personal Protective Equipment (PPE).
Node	Section of a facility that a workshop team is focused on at any given time during the study. The nodes are defined by the chairperson prior to the study.
Optioneering	Optioneering is the systematic examination of the performance of alternative methods and designs to better meet major challenges. It takes into account the impact of design method on a project's safety, environmental impact and cost.

Preventative	A preventative safeguard/control acts to prevent an initiating cause from resulting in an accident or incident, e.g. process alarms and trips.
Process Safety	“Process Safety” is a collective name for the measures, systems, procedures, or policies which prevent incidents and/or protect people/environment from effects of Major Accidents.
Qualitative	Qualitative information is not numerically estimated, but is instead evaluated using qualifiers like ‘high likelihood’, ‘low likelihood’, ‘high risk’, ‘medium risk’ etc.
Quantitative	Quantitative information contains a calculated numerical value, for example ’10 times per year’, ‘probability of failure on demand of $3.4x10^{-3}$.
Risk	The effect of uncertainty on objectives. It is expressed as the product of the measure of likelihood of occurrence of an event and the severity of potential consequences which the event may have upon people, assets/production, or the environment.
Risk Assessment Matrix	A graphical tool used for risk rating. The matrix consists of two axes – consequence criticality against likelihood of the event occurring.
Risk Ranking/ Rating	Qualitative or semi-quantitative assessment of the overall risk from a hazard scenario by using a Risk Assessment Matrix to estimate the criticality of the consequence, against the probability of the event occurring.
Semi-quantitative	Semi-quantitative information is a mixture of quantitative and qualitative information, for example ‘more than once per year but less than 10 times per year’, or ‘between £100,000 and £1,000,000’ which can represent bands, or orders of magnitude, rather than definitive numerical values. A Risk Assessment Matrix can often be semi-quantitative as some broad numerical bands may be applied to the different categories.

2. DOCUMENT STRUCTURE

The guide aims to assist pipeline operators in identifying the process safety methodologies that may be applicable to their operations or projects.

The document is split into the following sections:

- **Pipeline Process Safety Study Framework:** This presents an overview of the generic pipeline lifecycle phases, as well as identifying the process safety studies/techniques that may be relevant to that phase. This is presented in Section 3, using a diagram, with references as appropriate to further information within this document.

- **Safety Study Details:** The safety studies and techniques which are identified in the Pipeline Process Safety Study Framework (Figure 3.1) are discussed in additional detail in Section 4. The section provides a high-level overview of the technique, some of the key concepts involved, and how the study would be undertaken.

- **Summary of Safety Studies:** The techniques and studies described in Section 4 are summarised in Section 5. This summary provides an overview, in a table format, of what the technique is used for, the output it provides, as well as any specific relevant software packages.

- **Additional Studies:** Section 6 presents high-level information around additional techniques and studies that may be relevant to supplement the safety studies detailed within Section 4 and Section 5.

3. PIPELINE PROCESS SAFETY STUDY FRAMEWORK

Figure 3.1 presents an overview of the main pipeline lifecycle phases of an asset, namely:

- Concept Development, Optioneering and Project Specification
- Basic Design/ Concept
- Detailed Design
- Construction & Commissioning
- Operation, Maintenance and Modification
- Remaining Life Assessment
- Decommissioning

For each pipeline lifecycle stage, the Figure 3.1 identifies the phase, the studies which may be relevant to the phase, as well as detailing any other key considerations. It is up to the operator or project team to review the study techniques available and decide on those required to adequately assess and manage the risks associated with the asset. This may involve risk based decision making and/or reference to the relevant standards. Additionally, even if a study is not listed against a lifecycle phase, this does not imply that the study cannot be completed in that phase if it is determined (by the project team or operator) to be of benefit.

References are provided within Figure 3.1 to the sections of this document which provide an overview of the studies/ techniques.

The studies and techniques are further described in a shortened tabular format in Section 5 which summarises what the technique is used for, the output it provides, as well as any software tools that may be applicable to the technique.

Figure 3.1: Pipeline process safety study framework overview

Pipeline Lifecycle Phase	**Concept Development, Optioneering and Project Specification**	**Basic Design/ Concept**	**Detailed Design**	**Construction & Commissioning**	**Operation, Maintenance an Modification**
Phase Description	It is during this phase that most of the major hazards and effects will be identified and an initial assessment of their importance will take place. In this phase there is considerable scope for removing potential hazard.	During this phase there is a clear identification and assessment focus, albeit with a more detailed level of application. The emphasis is on incorporating inherently safe features at a detailed level of application, and prescribing passive and active control measures for remaining hazards. These are incorporated into the philosophies and engineering drawings, which constitute the base documents for the remainder of the design phase.	By the time the detailed design phase is reached, the main safeguarding measures will have been considered. The emphasis moves to the detailed engineering required for the agreed control and recovery measures and developing procedural control and recovery mechanisms.	The methods of construction imposed by the design and route will dictate, to a certain extent, the risks associated with the construction and commissioning phases. Where possible the risks associated with construction should be minimised by careful design. Residual risks will be fed forward as input to the construction management process. The execution of the construction phase produces its own hazards, and for major projects separate construction-oriented safety studies may be required (see Section 6.7).	Decisions made during the engin phase should reflect an agreed ope and maintenance philosophy. A handover stage documentation shoul existence which formally documen hazards and effects associated wi pipeline and the methods for their con When the pipeline is operational, studi be re-visited as operational data be available or modifications are ma increase the accuracy of the study inp Modifications themselves can be sub similar studies as the project, fro modification concept develop modification basic design, etc. throu decommissioning considerations.
Relevant Safety Studies					
ISD review - see 4.1	Y				Y - for modifications
HAZID - see 4.2	Y - high level hazard identification	Y - Basic design HAZID	Y - Detailed design HAZID	Y - Construction specific (see also 6.7)	Y - For modifications
HAZOP - see 4.3		Y - High level assessment where sufficient information available	Y	Y - If required pre start-up to assess operating sequences/instructions	Y - For modifications
SWIFT - see 4.4	Y - high level hazard identification	Y	Y		Y- For modifications
FMEA - see 4.5			Y		Y - For modifications
QRA - see 4.6		Y - High level assessment where sufficient information available	Y		Y - Updated data or for modifications
FTA - see 4.7			Y		Y - Updated data or for modifications
Bowties - see 4.8		Y - high level assessment where sufficient information available	Y		Y - Updated data or for modifications
RAM - see 4.9			Y		Y - Updated data or for modifications
LOPA & SIL - see 4.10, 4.11		Y - high level assessment where sufficient information available	Y		Y - Updated data (e.g. revalidation) o modifications
ALARP & CBA - see 4.12		Y	Y		Y - For modifications
Additional considerations	Is the pipeline route close to large centres of population Is the pipeline route through protected wildlife areas	Can a workable Emergency Reponses Plan be developed that addresses all the hazards and scenarios identified? Have all relevant stakeholders been identified	Have all key findings from preceding phases been incorporated into the detailed design	Checklist based study prior to construction handover to operations to ensure constructed as per design, and compliance achieved with codes and standards What activities will be conducted simultaneously that could lead to previously un-identified hazardous situations Does the design need re-visited to remove any intolerable construction risks	What operational data has been co that could inform any of the prev conducted studies Have there been any incidents or acc that require any studies to be revalida Is the process working as planned o there been any unexpected condition require assessment? Are all stakeholders aware of the Eme Response Plans and their obligations

[1] The topic of remaining life assessment is covered by a specific UKOPA Good Practice Guide [14] which details the full remaining life assessment process

4. SAFETY STUDY DETAILS

The following sections present an overview of the safety studies and techniques which are identified in Figure 3.1. As well as a high-level overview of the technique, the following is included in a bulleted list at the top of each sub-section (aside from Sub-Section 4.12 which refers to a separate Good Practice Guide):

- *Pipeline lifecycle phases:* This is the lifecycle phase when the study would normally be conducted in order to gain the most benefit (information as per the Pipeline Lifecycle Phases in Figure 3.1). It is possible to complete the study in a lifecycle phase other than those listed should this fit the requirements of the individual project or operator.

- *Example study inputs:* This is a listing of the minimum information generally required to do the study. It may still be possible to complete the study without this information depending if it is captured elsewhere, known to the team members, or available in another format. Additional inputs that are not listed may also be required depending on the specific project and operator.

- *Study requirements:* Information is provided as to whether a workshop and independent chairperson is required (noting that 'independent' implies independence from the project or asset to be studied), and if any specialist software is required.

In addition, the following bullet point is included at the end of each section:

- *Where to find more information:* Where a useful or relevant specific standard or guideline exists, a reference is provided. The reference list is not intended to be exhaustive and other applicable guidance and standards may be available.

When reading the following sections, it is important to consider that organisations may have existing internal standards that describe the process to follow when performing these studies. When utilising existing (internal or external) standards or guidance, consideration should be given as to if the guidance is appropriate for the asset or operation being assessed. For example:

- If hydrogen were to be transported for the first time, the existing standard or guidance may not be directly useable as the material being transported differs when compared to that which is assumed in the existing standard/guidance (e.g. molecule size, explosive properties, etc.).

- If an organisation which has traditionally only managed pipelines, the addition of a compressor may require consideration additional to that in the guidance/standard (e.g. are the guidewords and methodology appropriate?) as the equipment to be utilised differs from normal.

In such cases it may be necessary to review the methodology in the standard/guidance to determine that it is appropriate prior to commencing any studies.

4.1 Inherent Safety in Design (ISD) Review

- *Pipeline lifecycle phases: Concept Development, Operation & Maintenance and Modifications*

- *Example study inputs: Overview of the concept of the project (purpose, location, substances involved, etc.)*
- *Study requirements: Workshop required; independent chairperson required*

An Inherent Safety in Design (ISD) review should take place as early as possible in the development phase of a project or modification. The objective of the review is to minimise the inherent risks of the pipeline due to the presence of hazardous materials or substances.

The exercise is conducted in a group workshop and guided by a chairperson. Initially the pipeline is broken into sections and hazardous events are identified at each section based on the hazardous nature of the substances involved and related to foreseeable loss of containment / release of energy events. The team are then challenged to remove or reduce these hazards by fundamental re-design of the pipeline, rather than resorting to 'add on' safety features, by applying the following inherent safety principles.

- Elimination - Remove the need for the hazardous substance or material or activity e.g. remove the need for compression
- Substitution - replacing one material with another presenting a lesser hazard, e.g. non-flammable Mono-Ethylene Glycol (MEG) injection rather than methanol
- Minimisation - reducing the amount of hazardous material present at any one time
- Moderation - reducing the impact of an effect, e.g. having a cold liquid instead of a gas at high pressure, or using material in a dilute rather than concentrated form
- Segregation/Separation - can the pipeline be segregated /separated from other hazardous or vulnerable locations and processes.
- Simplification - removing/limiting hazards by design rather than adding additional equipment or features to deal with them. Only fitting options and using complex procedures if they are necessary.

This process can be achieved by asking questions such as the following:

- Are there significant hazards associated with the pipeline?
- Can the need for the pipeline be avoided?
- Can less hazardous substances or subsidiary materials be used?
- Can the hazardous inventory be reduced?
- Can the pipeline be operated under more moderate conditions (i.e. lower temperature and pressure)?
- Can the hazardous inventory be transported some other safer or simpler way?

The ISD review provides a detailed record for pipeline section showing potential improvement options, with initial assessment of the practicability and cost versus benefits. Follow up work is then carried out by the design team to work through these options and develop the most inherently safe process design, only resorting to 'add-on' safeguards/ control measures to reduce risks where absolutely necessary.

- *Where to find more information: Center for Chemical Process Safety (CCPS), Inherently Safer Chemical Processes: A Life Cycle Approach [1]*

4.2 Hazard Identification (HAZID)

- *Pipeline lifecycle phases: Concept Development, Optioneering and Project Specification, Basic Design/ Concept, Detailed Design, Construction & Commissioning, Operation & Maintenance and Modification, Decommissioning*
- *Example study inputs: Overview of the concept of the project (purpose, location, substances involved, etc.)*
- *Study requirements: Workshop required; independent chairperson required*

Hazard identification is generally one of the first safety studies conducted for a project), and is a very important step in risk assessment - a hazard must first be identified as being present in order to enable it to be managed effectively. A HAZID is also an important first stage in a modification to plant or processes, and can be re-visited throughout a pipeline's lifecycle to re-validate that all hazards have been identified and appropriate control measures remain in place

The objective of a HAZID is to systematically identify all health, safety, and environment (HSE) hazards and qualitatively assess the risk (frequency and consequence) associated with these hazards. A HAZID is a brainstorming exercise conducted in a group workshop and guided by a chairperson utilising a hazard checklist. Each hazard on the checklist is discussed, and it is determined if the hazard is present in the project, and where it is present. The guidewords can be taken from an international standard or a company standard, and will contain a large number of items that can be classified as "hazards", e.g. hydrocarbons and chemicals, situations such as working at height, external events (weather, earthquakes, etc.), human actions and errors, and many other items.

For specific pipeline lifecycle phases the hazard checklist can be changed to a list containing specific hazards guidewords related to that phase. The guidewords can also be selected with a view to addressing a specific area of interest, for example:

- In the case of environmental issues, a list of environmental-specific guidewords can be used, and this study is sometimes called an ENVID (Environmental Hazard Identification)
- For the case of specific interest in electric/electronics hazards, specific guidewords can again be used, with this study sometimes called an E-HAZID (Electronics HAZID)
- For the case of construction or decommissioning, these may be considered within the HAZID, however a separate Hazards During Construction (HAZCON) study may be required (see Section 6).

For a high-level HAZID it may be sufficient to determine what hazards are present and where. For a more detailed HAZID, the workshop team will also aim to determine what could be the cause of the hazard being released (e.g. corrosion of piping, dropped object onto plant, etc.), how likely this is to happen, as well as the magnitude of the consequences to people, the environment, assets and reputation if the hazard were to be released. The workshop team will also aim to identify the safeguards in place to control the hazards (e.g. maintenance, dropped object protection, operational procedures).

The basic process undertaken for each potential hazard on the checklist may therefore be summarised as:

- Is this hazard relevant to our project?
- What are the hazard sources/locations?
- What are the potential causes of a loss of control of the hazard?
- What are the worst case credible potential consequences if we lost control of the hazard?
- For these consequence scenarios, what is the frequency/likelihood of an event of this magnitude occurring?
- What are the controls in place to prevent the hazard release, or to mitigate the consequences if it were released?

The consequence and likelihood values for the hazard scenario are typically plotted on a Risk Assessment Matrix, which is a graphical tool used for risk rating. The matrix consists of two axes – consequence against frequency/likelihood of the event occurring. A basic example of a Risk Assessment Matrix is shown in Figure 4.2.

Utilising the Risk Assessment Matrix allows the hazards to be ranked as “Low”, “Medium” or “High”, and for each hazard to therefore receive the appropriate amount of focus (in terms of assessing the risk and managing the hazard). It also aids the workshop team in determining if the hazard controls in place are adequate relative to the risk level, and if not, then additional measures can be proposed in the workshop.

		Likelihood				
		Rare	Unlikely	Possible	Likely	Almost Certain
Consequence	Negligible Effects	**Low**	**Low**	**Low**	**Medium**	**Medium**
	Minor Effects	**Low**	**Low**	**Medium**	**Medium**	**Medium**
	Moderate Effects	**Low**	**Medium**	**Medium**	**Medium**	**High**
	Major Effects	**Medium**	**Medium**	**Medium**	**High**	**High**
	Catastrophic Effects	**Medium**	**Medium**	**High**	**High**	**High**

Figure 4.2: Example Risk Assessment Matrix

All hazards and the associated discussions are recorded in a HAZID worksheet (sometimes called a Hazard & Effects Register) by the HAZID chairperson, normally in conjunction with a HAZID scribe. The HAZID worksheet is normally displayed on a large screen throughout the workshop to allow attendees to see the information being recorded.

- *Where to find more information: IGEM/G/7 - Risk assessment techniques [2]*

4.3 Hazard and Operability Study (HAZOP)

- *Pipeline lifecycle phases: Basic Design/ Concept, Detailed Design, Construction & Commissioning, Operation & Maintenance and Modification*
- *Example study inputs: P&ID drawings*
- *Study requirements: Workshop required; independent chairperson required*

A HAZard and OPerability (HAZOP) study is a structured and systematic examination of a process or system in order to identify hazards and operability issues. The method systematically examines how each part of the 'design' will respond to deviations in key parameters by using suitable guidewords. The HAZOP differs from the HAZID in that is more detailed look at the response of the process to abnormal process parameter deviations, and the risk this may present, as oppose to the HAZID's higher-level overview approach.

As for the HAZID, the HAZOP study is a structured review of the facilities by a multi-disciplinary team, facilitated by a chairperson (who is independent of the project or pipeline operations), in a workshop environment. The 'design' of the process or system is first split into small manageable pieces called "nodes", and this is typically done using engineering drawings, e.g. Process Flow Diagrams (PFDs), or Piping & Instrumentation Diagrams (P&IDs).

Guidewords are then applied to each node of the design to identify potential deviations from the design intent. In discussion, the team then determines the potential causes of the deviation, as well as the associated consequences and likelihood (utilising a Risk Assessment Matrix, see Figure 4.2). Appropriate guidewords and parameters will be selected for each of the defined nodes to guide the discussions (see Table 4.1 for example guidewords and parameter combinations).

		Guidewords						
		No or Not	**More**	**Less**	**As Well As**	**Part of**	**Reverse**	**Other Than**
Parameters	**Flow**	Y	Y	Y	Y	Y	Y	Y
	Pressure	N	Y	Y	N	N	N	Y
	Temperature	N	Y	Y	N	N	N	Y
	Level	Y	Y	Y	N	N	N	Y
	Phase	Y	Y	Y	N	N	N	Y
	Composition	Y	Y	Y	N	N	N	Y

Standard 'Parameter' and 'Guideword' combination	Y
May be used	Y
Not possible	N

Table 4.1: Matrix of example HAZOP parameters

The HAZOP worksheet will be used to record guidewords and identified deviations, the causes and consequences of the deviation, and any actions to resolve issues identified by the HAZOP team. This is recorded by the HAZOP scribe in conjunction with the HAZOP chairperson, with the HAZOP worksheet displayed on a large screen throughout the workshop to allow all attendees to see the information which is being recorded.

Dependent on the complexity of the system and the number of P&ID drawings, a HAZOP is much more detailed process than, for example HAZID, and therefore require a larger effort. The output is subsequently far more detailed also and provides a more robust assessment of the process design. Where modifications are to be implemented to a project (for example a now booster station), it is possible to assess the modification using the HAZOP methodology without having to re do the facility-wide HAZOP.

In addition to a typical HAZOP, sometimes a variation is required, such as a CHAZOP (Control HAZOP), which follows the same basic process as HAZOP but focusses on the control/computer systems associated with the design. Such systems could be covered in a normal HAZOP, however a dedicated CHAZOP provides more focus on the control system architecture and components and can utilise guidewords tailored more towards control systems and their inputs and outputs.

- *Where to find more information: BS EN 61882 - Hazard and operability studies (HAZOP studies) Application guide [3], GEM/G/7 - Risk assessment techniques [2]*

4.4 Structured What-If Technique (SWIFT)

- *Pipeline lifecycle phases: Concept Development, Optioneering and Project Specification, Basic Design/ Concept Detailed Design, Operation & Maintenance and Modification*

- *Example study inputs: Overview of the concept of the project (purpose, location, substances involved, etc.)*

- *Study requirements: Workshop required; independent chairperson required*

The Structured What-If Technique (SWIFT), also known as the what-if technique, is a brainstorming hazard and risk identification methodology that utilises a series of "what if?" questions to identify the effects of deviations from the expected.

The SWIFT is conducted in a workshop led by an independent chairperson, where the workshop team are taken through a set of guidewords (e.g. timing, amount, etc.) that are combined with prompts. The prompts are phrases that generally begin with "what if…..?" or "how could….?". The analysis is applied at a system or subsystem level, so for example in the case of a corrosion inhibitor injection system, the prompts may look as follows:

- What if the corrosion inhibitor is not added?
- What if too much corrosion inhibitor is added?
- What if the wrong inhibitor is added?
- What if the inhibitor makes contact with an operator’s skin?

Similar to a HAZID or HAZOP, the risk related to the scenario can be assessed in the workshop, utilising a risk assessment matrix (see Figure 4.2), and this can be recorded as part

of the output. This allows a register of risk to be produced, which can complement the HAZID or HAZOP process.

- *Where to find more information: BS EN IEC 31010 - Risk management – Risk assessment techniques [13]*

4.5 Failure Modes and Effects Analysis (FMEA)

- *Pipeline lifecycle phases: Detailed Design, Operation & Maintenance and Modifications*
- *Example study inputs: Process Flow Diagram (PFD), component listing*
- *Study requirements: Workshop required; independent chairperson required*

Failure Modes and Effects Analysis (FMEA) seeks to identify hazards by identifying potential failure modes of the various parts of a system.

Whereas a HAZID looks for the hazard first and then identifies where it could be present in the system (known as a “Top Down” Approach), a FMEA generally starts with the component parts of a system and examines what their failure may lead to on a local and system-wide level (known as a “Bottom Up” approach).

As for HAZIDs, the FMEA is normally undertaken in a workshop environment with a multi-disciplinary team led by a chairperson. The chairperson guides the team through a pre-agreed list of elements (where an element is a level of sub-division of a system, item or process hierarchy at which failure modes are to be identified), with the team identifying the expected performance of the element, what would happen if it failed, how it could fail, and how to avoid or mitigate the failure effects.

Once the equipment/elements to be considered is agreed, this makes up the element checklist. Each item on the checklist is then discussed in turn to identify:

- The required functional performance of each item
- The potential failure modes associated with the item
- Detection methods and existing controls
- The local and system effects associated with each functional failure
- The failure causes
- Any engineered and operational safeguards which are in place or proposed to inhibit failure or to mitigate the failure consequences

A Failure Modes Effects and Criticality Analysis (FMECA) extends a FMEA so that each fault mode identified is ranked according to its Criticality (importance), and this can be done using a Risk Assessment Matrix (see the example in Figure 4.2). The Criticality level assumes that the safeguards / mitigation does not exist or fails (i.e. the functional failure occurs, and the consequences of the failure are not mitigated).

The output of the FMEA or FMECA is recorded in a worksheet, sometimes called a Fault Schedule, with an example of the information recorded for each item shown in Table 4.2.

Info Field	Description
Functional Failure	Identifies a specific failure of a component or sub-system in terms of the functionality it is required to provide at the specific operational phase.
Operational Criticality *(for a FMECA)*	Whether the component is considered critical to continued and / or safe operation. This is used as a screening guide as to whether the FMECA should address this item of equipment
Failure Mode	Identifies the cause of the functional failure.
Failure Detection Method	Identifies the means by which each failure will be detected, for example by routine maintenance, specific testing methods or as a result of the effects manifested by the failure should it occur.
Local effect of failure	Identifies the effect of each failure local to the failure itself.
System effect of failure	Identifies the system wide effects (if any) of each failure.
Engineered safeguards / mitigation	Identifies the engineered measures provided to control each functional failure by reducing either the probability of occurrence or the failure consequences.
Operational safeguards / mitigation	Identifies the operational measures (e.g. procedural controls) provided to control each functional failure by reducing either the probability of occurrence or the failure consequences.
Unmitigated Criticality *(for a FMECA)*	Identifies the criticality associated with the occurrence of each identified functional failure assuming the safeguards / mitigation does not exist or fails (i.e. the functional failure occurs, and the consequences of the failure are not mitigated). This can utilise a Risk Assessment Matrix (see the example in Figure 4.2).
Recommendations	Sets out recommendations where additional safeguards / barriers could be implemented, or existing ones improved to ensure that the risks are appropriately managed.

Table 4.2: Example of information recorded in a FMEA/ FMECA

FMEA/FMECA is very good at identifying single point failure modes, but not combinations of failure modes (i.e. multiple failures in combination) or common cause failure (failures of multiple items due to a common event, for example a loss of power to the pipeline system). It can therefore be used in conjunction with other techniques if this information is required (for example the use of fault tress - see Section 4.7).

- *Where to find more information: BS EN IEC 60812 - Failure modes and effects analysis (FMEA and FMECA)* [4]

4.6 Quantitative Risk Assessment (QRA)

- *Pipeline lifecycle phases: Basic Design/ Concept, Detailed Design, Operation & Maintenance and Modifications, Remaining Life Assessment*
- *Example study inputs: HAZID output, equipment details, operational parameters, location details, population information, substance properties, meteorological conditions, failure rate data*
- *Study requirements: No workshop required, specialist software and user normally required*

Quantitative Risk Assessment (QRA), also known as a Pipeline Risk Assessment, is a technique used to systematically calculate the risks from hazardous events. It involves predicting the size of consequences associated with a hazard, and the frequency of those consequences being realised, with these aspects combined in order to calculate a numerical value of risk. This numerical value of risk can then be compared with other numbers - for example, if you calculate the risk value for two different options, you can compare the results to see which option is the lowest risk solution. The calculated risk value can also be compared against criteria which have been set by a company or regulator, in order to determine whether the risk is below intolerable or unacceptable levels.

Having calculated a total risk value, it can also be investigated to determine what makes the biggest contribution to the total – i.e. what is dominating the risk value, and therefore where attention could be focussed in risk reduction efforts in order to bring about the most significant reduction in risk.

A QRA does not generally include every single hazardous event which might occur, just a representative set, but includes all the significant hazards from the HAZID Study. Similar hazardous events are normally grouped and assessed together. The consequence of the hazard event used in the QRA calculations can be taken from the consequence modelling (see Section 4.6.1), and the frequencies can be taken from the frequency and event tree information (see Section 4.6.2) to calculate risk.

The calculated risk is then generally assessed for individual or societal risk, as described in Table 4.3.

Risk Type	Description
Individual Risk	Individual risk is the frequency at which an individual is exposed to a determined level of harm from a hazard event (the consequence), at a specific location relative to the pipeline. All of the risks from the various hazard events can be collated and plotted on a graph showing the risk levels at the various distances. The risk levels can be shown on the y-axis, with the distance from the pipeline shown on the x-axis in a format called the risk transect, an example of which is shown in Figure 4.3.
Societal Risk	Societal risk is the frequency at which one or more fatalities are calculated to occur per pipeline year. Whereas individual risk is concerned with an individual at a location, societal risk considers larger numbers of people who may life or work close to the pipeline. This is generally plotted in an FN Curve which shows the frequency of incidents (F) causing N or more fatalities, an example of which is shown in Figure 4.4).

Table 4.3: Risk types from a QRA

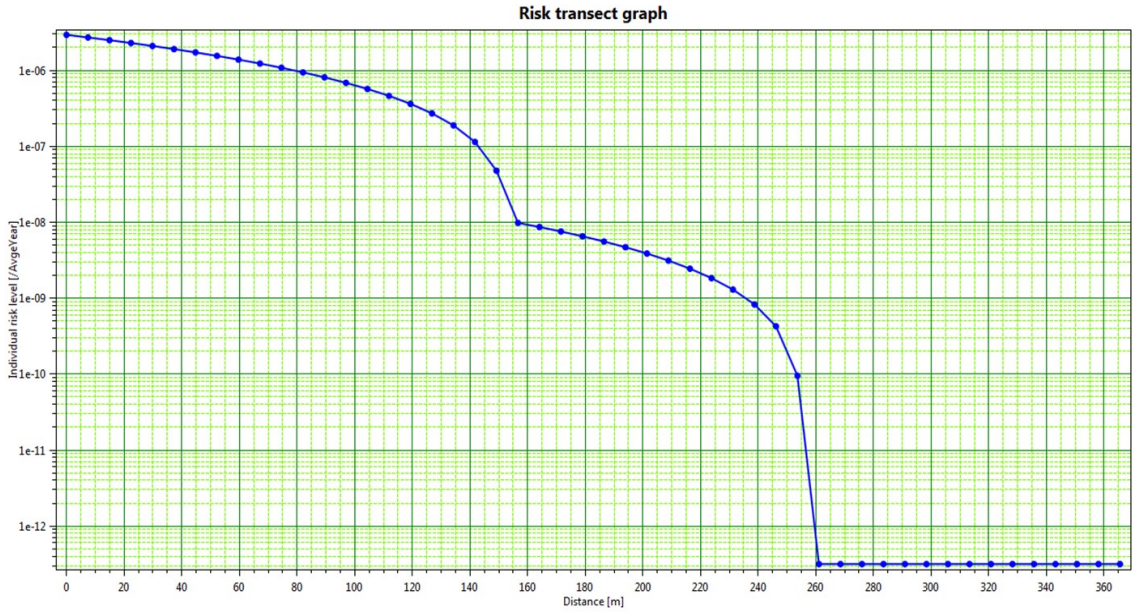

Figure 4.3: Example Risk Transect

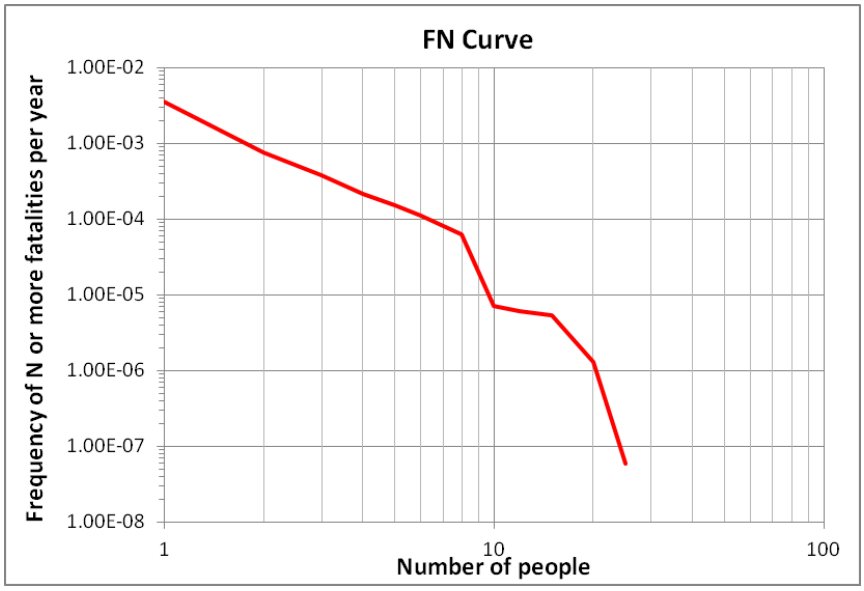

Figure 4.4: Example FN curve

The risk value can also be compared against land use and land use planning along a pipeline route and for determining boundaries (or 'Zones') of risk along the route where required (see Section 4.6.3).

A QRA model requires the input of consequence and frequencies, and these are discussed in further detail in Section 4.6.1 and Section 4.6.2.

- *Where to find more information: IGEM/TD/2 - Assessing the risks from high pressure Natural Gas pipelines [5] , BSI PD 8010-3 - Pipeline systems – Part 3: Steel pipelines on land – Guide to the application of pipeline risk assessment to proposed developments in the vicinity of major accident hazard pipelines containing flammables [6]*

4.6.1 Consequence Modelling

Physical effects consequence modelling involves the quantification of hazardous consequences, for example in the case of jet fire, fireball followed by a jet fire, or flash fire followed by a jet fire. Consequence modelling aims to assess how big an event will be based on the parameters affecting it utilising a series of inputs, for example, some of the inputs would include:

- Information regarding the substance and the substance state (liquid or gas)
- The pipeline diameter and wall thickness
- Operational information such as pressure and temperature
- Orientation of the pipeline
- The atmospheric temperature, wind directions and speeds, and relative humidity

By inputting the parameters into a software model, it can generate an estimate of the consequence magnitude for any given scenario. Once the actual physical parameters are modelled, the next step involves translating that into an equivalent level of harm.

For example, if a fire related to the pipeline was considered, the level of thermal radiation could inform specific probabilities of fatality at a certain location, the higher the level of thermal radiation, the greater the probability of fatality. The same translation of the physical parameters to probability of fatality (or probability of harm to wildlife, for example) would apply for any type of physical parameter, e.g. explosion overpressure, radiation levels, toxic gas levels, etc.

The outputs from consequence models are used in conjunction with event frequencies (see Section 4.6.2) to determine the risk to an individual at given distances from the pipeline.

It should be noted that, as with all quantitative modelling, calculations can be very sensitive to input assumptions, and results should not be used outside the limits of validity for the model.

4.6.2 Frequencies and Event Trees

An Event Tree is a diagram which is used to illustrate the sequence of how an initiating event develops to all its potential outcomes. Each stage of the tree generally has only two possible outcomes; yes/no, success/failure. Event trees are used to map the frequency associated with each credible consequence from a failure. For example, for a pipeline, these consequences are dependent on the substance being carried.

An example is given in Figure 4.5, which shows an initiating event of a large release of flammable Liquefied Petroleum Gas (LPG) on the left hand side of the figure as ‘A’. The event then develops from left to right, for example it might ignite immediately resulting in a local fire (jet fire or pool fire), or it might ignite after a delay resulting in a Vapour Cloud Explosion (VCE) or flash fire, etc.

Each step along the way is subject to a yes/no answer, with a numerical probability attached to each answer. The probabilities at each answer always add up to 1 as can be seen in Figure 4.5.

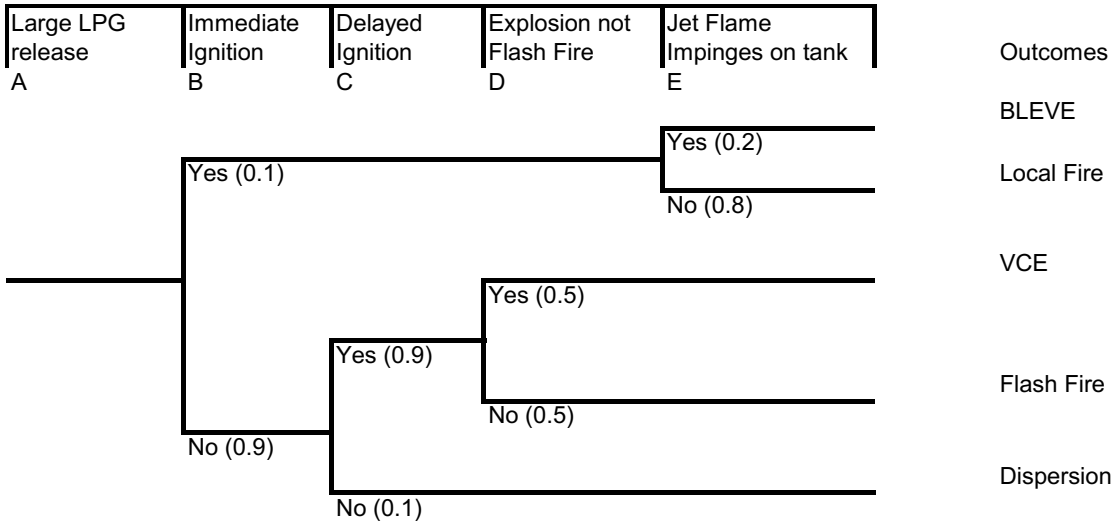

Figure 4.5: Example event tree diagram

Failure rates are used to calculate frequencies for each the initiating event, with the event tree calculating the frequency of the individual consequences on the end branches on the left hand side of the event tree.

The initiating event frequencies are normally determined using an external failure rates model, which can calculate pipeline failure frequencies for various hole sizes from pinhole up to full rupture (if this is possible).

In order to calculate the pipeline failure frequencies for the hole sizes, inputs are generally taken from operational experience data which generates failure frequencies (e.g. for mechanical failures or defects, ground movement, corrosion, third party activities etc.)

The outcomes can be combined with consequence modelling (see Section 4.6.1) to determine the overall risk from the event tree.

4.6.3 HSE Land Use Planning Zones

The UK Health and Safety Executive (HSE) use its own computer code, MISHAP (Model for the estimation of Individual and Societal risk from HAzards of Pipelines), to calculate risk. The calculated risk associated with Major Accident Hazard (MAH) pipelines can then be used to designate the distances to land-use planning zones, with consideration given to the sensitivity of any proposed developments against the Zones, for example normal working populations, general public, vulnerable members of the public (hospitals, schools, etc.) and very large outdoor developments.

MISHAP operates on the same principles as described in the above sections in that input parameters are used to calculate frequencies and consequences in order to determine risk levels associated with various scenarios at various locations.

4.7 Fault Tree Analysis (FTA)

- *Pipeline lifecycle phases: Detailed Design, Operation & Maintenance and Modification*
- *Example study inputs: Component listing and component reliability/failure data*

- *Study requirements: No workshop required, specialist software and user required for detailed studies*

Fault Tree Analysis (FTA) is a method normally used to address specific issues identified in the risk assessment process where specific appropriate data is not available. For example, it can be used to calculate the overall reliability of a shutdown system that contains multiple components, or to determine the likelihood of the fire and gas detection system failing. Failure of the system is defined as the "top event" and FTA builds up a picture of how that top event might occur by considering all the individual failures that are needed to bring it about.

A FTA diagram uses logic gates to describe the combinations of events needed to reach the top event. An example is shown in Figure 4.6 where the events (Fuel, Ignition Source, and Oxygen) lead to an 'And' gate, before reaching the top event of 'Fire'. The 'And' gate indicates that in order to reach the top event, fuel AND ignition source AND oxygen must be present to reach 'Fire'.

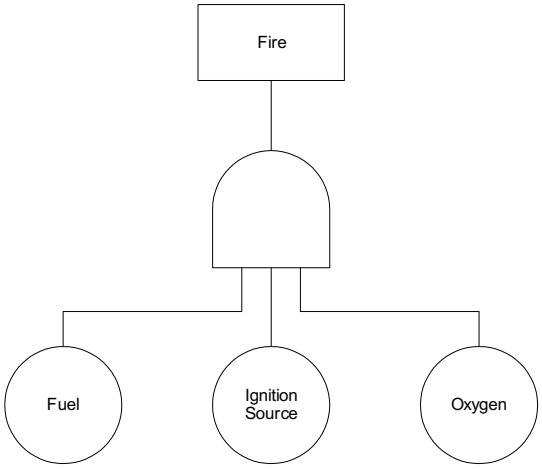

Figure 4.6: Example fault tree 'And' gate

Another commonly used gate is an 'OR' gate. In the example shown in Figure 4.7, the top event is 'ignition source'. This time in order to reach the top event, the events (hot surface, naked flame, spark) are subject to an 'OR' gate as in order to reach the top event we need only have a hot surface OR a naked flame OR a spark.

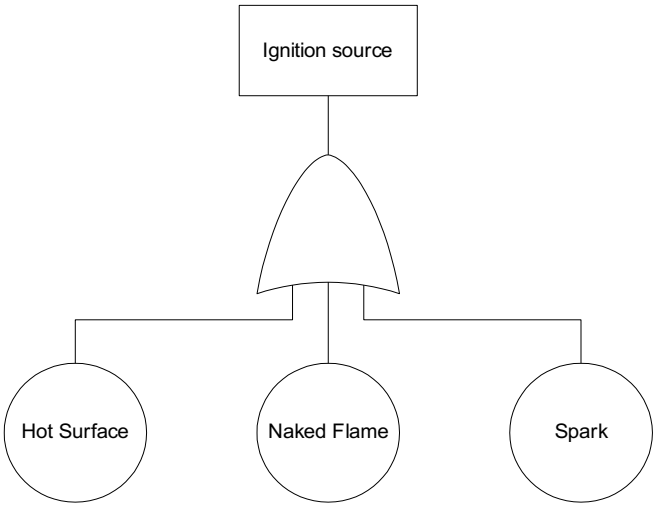

Figure 4.7: Example fault tree 'Or' gate

There are many other gate types available (voting gates, transfer gates to another fault tree, priority AND gates, etc.), and utilising these gates allows the fault trees to be developed, with an example of a fault tree showing the different components leading to the failure of a water supply shown in Figure 4.8.

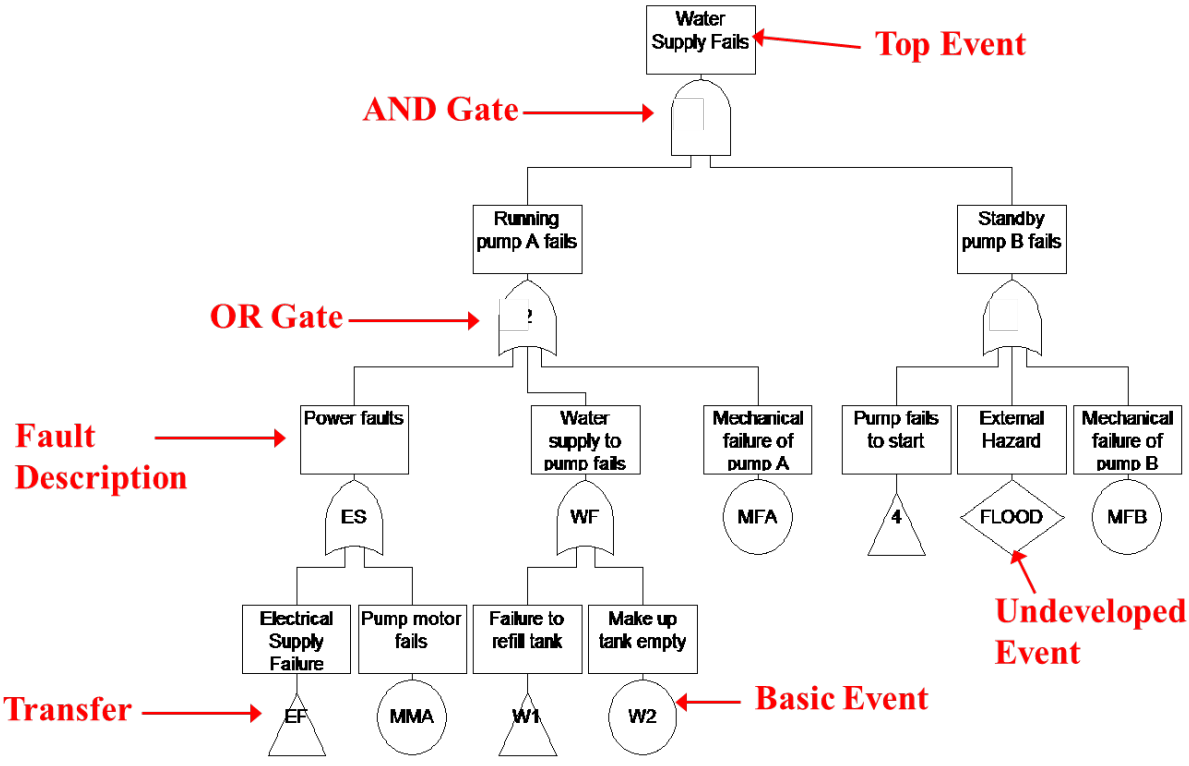

Figure 4.8: Example fault tree for water supply failure

FTA can be done on a purely qualitative basis, to describe how the individual failure combine to result in the top event. However, it is more common for the technique to be used quantitatively, to assign probabilities to each individual failure and combine them to calculate

an overall frequency for the top event. The outputs from the fault tree can be used to calculate frequency values in their own right, or the top events can also be used to define values that are used as inputs in other quantitative techniques (e.g. to define branch probabilities in event tree analysis).

Utilisation of a software package for fault tree modelling can help with the identification of failure causes and modes that affect multiple components (potentially simultaneously), as well as identifying the different chains of events that can lead to the top event (known as 'cut sets').

- *Where to find more information: BS EN 61025 - Fault tree analysis (FTA)* [7]

4.8 Bowties

- *Pipeline lifecycle phases: Basic Design/ Concept, Detailed Design, Operation & Maintenance and Modification*
- *Example study inputs: HAZID output*
- *Study requirements: Workshop required, independent chairperson required, specialist software generally required*

A Bowtie diagram is a pictorial tool used to illustrate the relationships between major hazards, causes, potential consequences and risk controls (known as barriers). Typically a Bowtie can follow on from a HAZID - where a hazard is identified as 'High Risk' or as a Major Accident Hazard (MAH) (utilising the Risk Assessment Matrix, Figure 4.2), each such hazard can be subject to an individual Bowtie analysis in order to look at the hazard in a greater level of detail. Bowties can also be developed to assess any new or emerging hazards that are identified during a pipeline's lifecycle, for example relating to modifications, changing physical or regulatory conditions, in response to operational incidents, or where there are changes to the effectiveness of the risk control barriers (e.g. degradation over time).

Bowties are normally developed in a workshop environment, with an independent chairperson guiding a team through the development of the diagram. The workshop scribe will update the diagram on a large screen so the attendees can see the Bowtie develop.

An example Bowtie is illustrated in Figure 4.9. In the diagram, the hazard is located at the centre of the diagram together with the top event (i.e. the release or loss of control of the hazard). On the left side are the identified potential causes or threats and on the right side, potential consequences.

In between the threats and the top event, the controls (barriers) that prevent the top event occurring are listed.

On the right side of the diagram the defence (mitigation) controls that serve to minimise or prevent consequences, in the event that the top event occurs, are listed.

Also illustrated on the Bowtie diagram are defeating (or escalating) factors on certain control measures. These are factors which can result in the affected control being defeated, removed from service, eliminated, or having a reduced effectiveness. Identifying the factors on the Bowtie is used to illustrate that there are further control measures in place to manage the defeating factor and prevent failure of the control to which the defeating factor is linked.

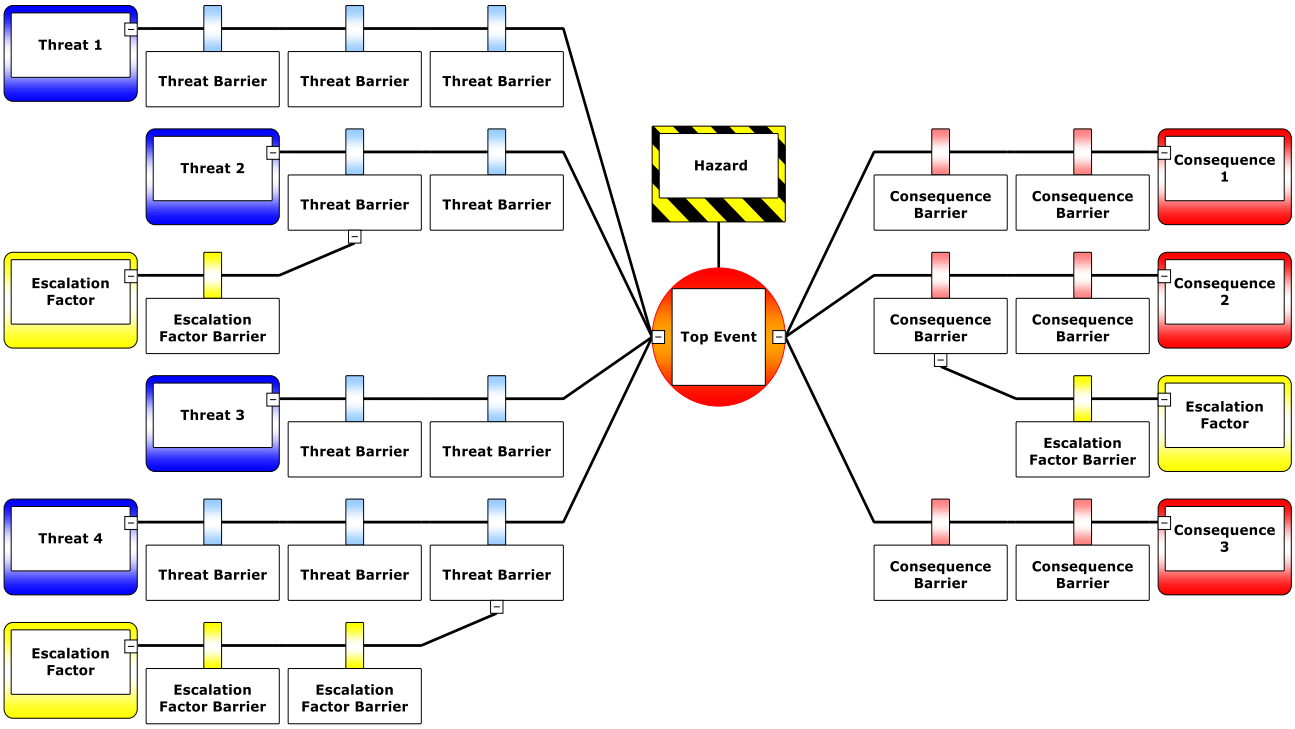

Figure 4.9: Example bowtie diagram

So, in a worked example, the following could apply:

- **Hazard**: Hydrocarbons in a pipeline
- **Top event** (the release of the hazard): Loss of containment of the hydrocarbons
- **Threats**: Dropped object onto pipeline, equipment corrosion or erosion, etc.
- **Consequences**: Multiple fatalities due to an ignited release, asset damage, etc.
- **Prevention/ Threat barrier**: Pipeline pressure relief system and equipment
- **Mitigation/ Consequence barrier**: Firefighting team and equipment available to provide emergency response/ rescue support
- **Escalation/ Degradation factor**: Firefighting equipment is faulty due to being out of use by date.
- **Escalation factor barrier/ Degradation control**: Checks and maintenance of firefighting equipment performed on a regular basis to ensure equipment is fit for purpose.

So in summary, for a specific hazard, the Bowtie diagram (reading left to right) shows the causes (threats) which can lead to the undesirable loss of control (top event) if there are not sufficient controls in place to prevent it and, if the mitigation barriers also fail to control the event, the Bowtie shows the extent of the ultimate potential consequences.

The Bowtie diagram provides a visual demonstration of the way in which risks are managed, allowing widespread understanding at all levels, and giving all personnel the opportunity to review the existing controls in place and to identify any potential improvements.

The diagram also enables the identification of HSE Critical Tasks and HSE Critical Elements as described in the following sections.

- *Where to find more information: CCPS in association with the Energy Institute - Bow Ties In Risk Management - A Concept Book for Process Safety* [8]

4.8.1 HSE Critical Tasks

For the control barriers identified and illustrated on the Bowties, assurance is required that these measures will remain effective. For each barrier, tasks are identified which, if carried out, will ensure the barriers are in place and functional. These tasks are termed “HSE Critical Tasks” as they support controls which reduce the potential risks associated with major hazards.

An example HSE Critical Task could be the maintenance, inspection and testing of the facility gas detection systems. If this task was not carried out, then there is no assurance or confidence that the gas detection system would function on demand and it would not be possible to claim the gas detection system as a credible control.

For the most part these tasks are day-to-day tasks that should be routinely carried out. Verification (e.g. via audits) that these tasks are being carried out provides confidence and assurance that the risk controls are in place and effective.

Mapping the major risks in this manner promotes a structured review of each hazard, identifying not only what controls are in place now, but also how, through HSE Critical Tasks, they will continue to be in place throughout the lifetime of the facility.

4.8.2 HSE Critical Elements

HSE Critical Elements are those engineered systems and items of structure, plant, and equipment where:

- Failure of the element could cause or contribute substantially to a major incident
- The purpose of the element is to prevent a major incident
- The purpose of the element is to mitigate the effects of a major incident

HSE Critical Elements are subject to defined expectations in terms of standards of performance, a programme of performance assurance through application of the facility’s maintenance and integrity management systems, and independent verification of continued performance through, for example, third party surveys.

4.9 Reliability, Availability and Maintainability (RAM) Modelling

- *Pipeline lifecycle phases: Detailed Design, Operation & Maintenance and Modification*
- *Example study inputs: FMECA output, failure, and downtime data*
- *Study requirements: No workshop required, specialist software and user required*

Reliability, Availability and Maintainability (RAM) analysis determines the likelihood of plant failure and the time necessary to return the plant to an operational state. This allows an operator to optimise the design including its configuration, level of equipment redundancy, component selection and supporting maintenance strategy.

As well as suggesting tangible improvements, a RAM analysis provides confidence that the system will meet its operational targets and support the through-life viability of a project.

A RAM study will generally take inputs from a FMECA study (see Section 4.5) to identify the critical equipment within the process. This equipment can then be assigned failure and downtime data, usually from an industry database of some kind (e.g. OREDA). Utilising this information, it is possible to calculate:

- **MTBF (Mean Time Between Failures):** Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.

- **MTTR (Mean Time To Repair):** The mean active corrective maintenance time before the item is repaired. It is part of the Total Repair Time. It is usually expressed in hours.

A model can be built which can be used to calculate the availability of the plant. Simulations can be run within the model to identify many different aspects, for example which components have the biggest effects on availability and therefore how much redundancy is needed, how maintenance planning could be optimised, and what the effects of design changes could mean.

A Reliability Block Diagram (RBD) is generally used within the model to describe the interrelation between the components and to define the system.

A RBD is a graphical representation of the components of the system and how they are connected reliability-wise (which may differ from how the components are actually physically connected). An example RBD of a simplified computerised system with a redundant fan configuration is shown in Figure 4.10.

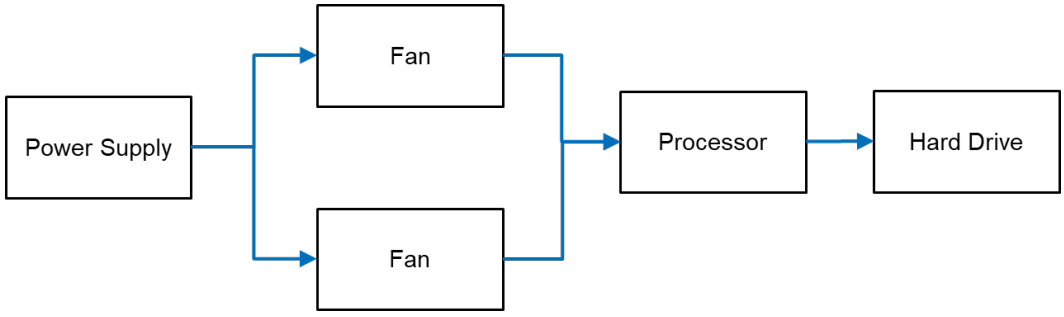

Figure 4.10: Example RBD diagram

- *Where to find more information: BS EN ISO 20815 - Petroleum, petrochemical and natural gas industries. Production assurance and reliability management* [9]

4.10 Layers of Protection Analysis (LOPA)

- *Pipeline lifecycle phases: Basic Design/ Concept, Detailed Design, Operation & Maintenance and Modification*

- *Example study inputs: HAZOP output, reliability data*
- *Study requirements: Workshop required; independent chairperson required*

LOPA is a risk assessment tool that considers all the protection layers within a system in order to establish if there is a risk shortfall against a given target. Typically, this study can be informed by the output of a HAZOP - for example where a HAZOP has identified that a valve failing closed can cause a system to overpressure, there may be some associated safeguards identified (e.g. pump trips on high pressure, relief system initiates, etc.). It is these safeguards, in combination, that can be assessed by LOPA. Like a HAZOP, the LOPA is conducted in a workshop environment and is guided by a chairperson.

If the safeguards in place are considered to fall short of a target (for example a frequency of failure target), then the shortfall is subject to study to determine the best way to achieve the required risk reduction. This may be through use of an Electrical/Electronic/Programmable Electronic System (E/E/PES), in which case the function of the E/E/PES can be designated as a Safety Instrumented Function (SIF).

The safety function in its entirety concerns the identification of the process upset through monitoring (e.g. a sensor), performing some assessment of the monitoring value against criteria, and then exercising an action - an example is shown in Figure 4.11). Safety Instrumented Systems (SIS) are used to implement one or more SIFs, with the SIS being composed of the sensor, logic solver and final control element - an example of a process industry SIS could be an Emergency Shutdown (ESD) system.

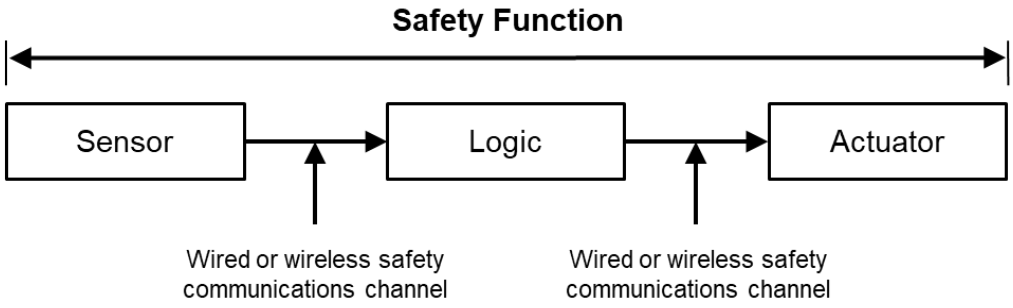

Figure 4.11: Example safety function diagram

The magnitude of risk reduction required by the identified SIF is then used to define the Safety Integrity Level (SIL) required for the SIF (see Section 4.11 for a description of SIL).

LOPA is described as semi-quantitative because although the technique uses numbers and generates a risk estimate, this is based on generic estimates of failure probability rather than actual failure rates of specific equipment. As a consequence, the result tends to be conservative (overestimating the risk), providing an ‘order of magnitude’ approach, but is usually adequate for understanding the required SIL for the SIF.

- *Where to find more information: BS EN 61511-3 - Functional safety — Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels [10]. It should be noted that this standard also discusses alternative methods for determining the SIL level that may be required for a SIF, for example the calibrated risk graph method.*

4.11 Safety Integrity Level (SIL) Determination and Verification

- *Pipeline lifecycle phases: Basic Design/ Concept, Detailed Design, Operation & Maintenance and Modification*
- *Example study inputs: HAZOP output, LOPA output, details of components to be used*
- *Study requirements: Workshop required; independent chairperson required*

Safety-related systems are used in a range of different applications where they are employed in order to reduce risk to acceptable levels. As there is a reliance on their correct operation to perform the intended functions when needed, their failure to perform the intended function could result in an accident, with the consequent loss of life, damage to the environment, or a loss of assets.

IEC 61508 is an international standard published by the International Electrotechnical Commission consisting of methods on how to apply, design, deploy and maintain automatic protection systems. This standard is widely used in multiple industries in order to provide a means of ensuring that safety is reached, where it is based on functionality of Electrical, Electronic or Programmable Electronic (E/E/PE) systems. The linked IEC 61511 standard contains the same lifecycle and SIL concepts as IEC 61508, but is more specific to the process industry and is therefore often used within the industry (note that these standards are available as BS EN 61508 and BS EN 61511 in the UK).

In accordance with IEC 61508/ IEC 61511, where the magnitude of risk reduction required by a SIF (see Section 4.10) has been defined, this can be used to define the Safety Integrity Level (SIL) required, which is essentially the required level of performance needed for the item. This is generally expressed its Probability of Failure on Demand (PFD).

The required average PFD value for the item can then be banded, as shown in Table 4.4 (which is taken from IEC 61508).

SIL	PFD_{avg}		Risk Reduction Factor
4	$\geq 10^{-5}$ to $<10^{-4}$	0.0001 - 0.00001	10,000 - 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	0.001 - 0.0001	1,000 - 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	0.01 - 0.001	100 - 1,000
1	$\geq 10^{-2}$ to $<10^{-1}$	0.1 - 0.01	10 - 100

Table 4.4: Low demand mode SIL bands

For example, where a system has been identified during LOPA as being required to not fail greater than 3.4×10^{-3} times per demand, then the system can be described as being a SIL3 system.

Table 4.4 (taken from IEC 61508) presents the SIL for low demand items, which are items where the frequency of demands for operation made on a safety-related system is no greater than one per year. Where the frequency of demand is greater, a different table is used, as shown in Table 4.5, but with Frequency of Dangerous Failure per Hour (PFH) used to determine the SIL level.

SIL	Frequency of Dangerous Failure per Hour (PFH)
4	$\geq 10^{-9} < 10^{-8}$
3	$\geq 10^{-8} < 10^{-7}$
2	$\geq 10^{-7} < 10^{-6}$
1	$\geq 10^{-6} < 10^{-5}$

Table 4.5: High demand mode SIL bands

The process for SIL selection is probabilistic (i.e. gives a distribution of possible outcomes), and there may be uncertainties and approximations in the data used. It is therefore dependent on the judgement of the people participating in the process.

SIL targets can be selected in either a multidisciplinary workshop or in a desktop process. The latter is a potentially lower effort option compared to the workshop option as it can be conducted by a single analyst but lacks the collective input of a multidisciplinary team. A multidisciplinary team approach to SIL selection is similar to that of a HAZOP, and in fact can be completed as part of a HAZOP, with the group members reaching a consensus view as part of the assessment.

Once the actual safety function is designed, SIL verification is conducted in order to see if the design meets the required SIL target (average probability of failure on demand/probability of failure per hour) in terms of its architecture and the components to be used. This can also be applied retrospectively to ensure that an existing design can be verified relative to the required SIL target.

The SIL determination and validation form only part of the lifecycle of the SIS and there is a requirement in IEC 61511 to manage the SIS throughout the full lifecycle and this is discussed further in Section 4.11.1.

- *Where to find more information: BS EN 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems [11], BS EN61511 - Functional safety — Safety instrumented systems for the process industry sector [10]*

4.11.1 Safety Lifecycle for SIL Rated SIS Systems

The IEC 61508/61511 standards provide the risk management activities targeted towards functional safety assurance over the lifecycle of the SIS. The lifecycle comprises sixteen detailed phases covering all system life stages, from concept through to decommissioning, which broadly fall into three main phases:

- Analysis: Analysis and documentation of the safety requirements (partially covered in Section 4.11)
- Realisation (design and implementation): Use the requirements to develop and document the safety system design, using appropriate software and hardware and design methodology
- Operation: Operate and maintain the system in accordance with accepted procedures and perform and record maintenance to ensure that the required performance standards are maintained

The safety lifecycle helps to ensure the integrity of the SIS throughout its life to ensure that it continues to provide the required level of protection. Implementation of lifecycle management allows responsibility to be taken for all of the lifecycle phases in of a SIS, and for upgrades and back fits to be managed via selective application of elements of the overall safety lifecycle phases. It is therefore important to consider the full lifecycle of the SIS when there are SIL requirements associated with a pipeline.

4.12 Risk Reduction, ALARP and Cost Benefit Analysis (CBA)

The fundamental principle of risk-based hazard management is that whilst risks cannot always be completely eliminated, it should be possible to reduce them to a level that is As Low As Reasonably Practicable (ALARP). The risks must be managed to a level that is tolerable with all reasonably practicable risk reduction measures. The management of hazards, such that the safety risks are ALARP, must be demonstrated.

The level at which risk has been reduced As Low As Reasonably Practicable (ALARP) is when the time, trouble and cost of further reduction measures become unreasonably disproportionate to the risk reduction achieved. The principle helps decision-makers because it recognises that whilst risk reduction is desirable it is not always warranted. Once it is known what there are in terms of hazards and their associated risks (from HAZIDs, HAZOPs, QRAs etc.), there is a need to determine how risks are being controlled, and if this is good enough. A combination of the studies in Section 4 will therefore feed into the ALARP process and the overall demonstration of ALARP.

- *Where to find more information: The topic of ALARP and how to apply Cost Benefit Analysis (CBA) to aid decision making is subject to a separate UKOPA Good Practice Guide* [12]

5. SUMMARY OF SAFETY STUDY USES AND OUTPUTS

Table 5.1 below presents a summary of the safety studies and methodologies described in detail in Section 4.

Technique	Used for	Output	Example Inputs	Specialist Software
ISD review	• Minimising the inherent risks of the pipeline due to the presence of hazardous materials or substances.	• Removing or minimising risks at the start of a project	• Overview of the concept of the project/modification (purpose, location, substances involved, etc.)	• No specific requirement
HAZID Study	• Structured identification of hazards – apply checklist to steps in a process/activity, entire site/facility • Screening of major hazards	• Causes and consequences of hazard scenarios (process releases and external hazards) • Controls in place • Risk associated with each scenario	• Overview of the concept of the project/modification (purpose, location, substances involved, etc.)	• No specific requirement
Risk Assessment Matrix	• Combining event consequence and frequency • Ranking risks as high, medium and low	• Qualitative, semi-quantitative or quantitative measure of risk	• No specific requirement	• No specific requirement
HAZOP Study	• Process system design • Structured identification of hazards and operability problems: apply guidewords to a P&ID, flow diagram or procedure	• Causes and consequences of process upsets and releases, arising from within the process • Controls in place to prevent/mitigate such upsets • Availability/maintainability issues	• P&ID drawings	• PHA Pro • PHA Works
SWIFT	• Identifying hazards and risks at a sytem or subsystem level	• List of hazards scenarios • Risk associated with each scenario	• Overview of the concept of the project/modification (purpose, location, substances involved, etc.)	• No specific requirement
Failure Modes and Effects Analysis (FMEA)	• Hazard identification and frequency assessment (qualitative or quantitative)	• All possible fault modes of systems/components • Consequences of such failures	• Process Flow Diagram (PFD) • Component listing	• No specific requirement

Technique	Used for	Output	Example Inputs	Specialist Software
Quantitative Risk Assessment (QRA)	• Combining numerical frequency and consequence values to estimate risk level for a single hazard or combined risk from all hazards for a facility or activity	• Risk of death to individual workers or members of the public • Frequency of multiple fatalities • Frequency of impairment of buildings	• HAZID output • Equipment details • Operational parameters • Location details • Population information • Substance properties • Meteorological conditions • Failure rate data	• DNV PHAST • DNV Safeti • Shell SHEPHERD • Isograph Reliability Workbench • MISHAP (HSE software) • PIPIN (HSE software)
Event Tree Assessment (ETA)	• Analysing the various outcomes (e.g. fire, unignited spill, explosion) of a hazardous event • Identifying escalation paths	• Frequency of event outcomes, given occurrence of an initiating event • Diagram illustrating escalation of the initiating event (time sequence), through various success / failure states of safeguards, to discrete event outcomes		
Consequence Modelling	• Predicting extent of gas/liquid dispersion, fires & explosions	• Size of clouds/pools • Heat from fires • Explosion overpressures • Level of harm to people • Level of damage to plant and buildings		
Fault Tree Assessment (FTA)	• Identifying causes of hazardous events • Identifying hardware and human error causes	• Frequency of hazardous event (the “top event”) • Logic diagram illustrating combinations of events which can lead to the top event	• Component listing and component reliability/failure data	• Isograph Reliability Workbench - FaultTree+
Bowtie Analysis	• Structured analysis of a given hazard	Diagram illustrating: • Potential causes & consequences of accident scenario • Controls specific to each cause/consequence and responsibilities for each control	• HAZID output	• Bowtie XP • THESIS

Technique	Used for	Output	Example Inputs	Specialist Software
Reliability, Availability and Maintainability (RAM)	• Determining the availability and capacity of plants/systems • Optimising equipment redundancy and maintenance strategies	• Capacity • Availability • Number of outages • Production rate	• FMECA output • Failure and downtime data	• Isograph Reliability Workbench • DNV Maros Lite • Relyence
Layers of Protection Analysis (LOPA)	• Deciding how much risk reduction is needed and how many layers of protection should be used	• Recommendations to install or not install safeguards • Basis for functional specification of safety instrumented systems	• HAZOP output, reliability data	• Primatech LOPAWorks
Safety Integrity Level (SIL) study	• Assessing integrity of critical control loops of e.g. shutdown systems	• SIL rating in line with IEC 61511	• HAZOP output • LOPA output • Details of components to be used	• DNV Synergi Plant • Exida exSILentia • ESC SIL Comp

Table 5.1: Summary of safety studies

6. ADDITIONAL TOPICS

In addition to the safety studies described previously in Section 4, there are further topics which are related to pipeline safety and supplement or provide input to the studies detailed within Section 4 and Section 5. The following section provides a brief overview of these topics/ studies, and a reference for where to find more information (if applicable):

6.1 Human Factors and Ergonomics

Human factors is a large subject in itself, and incorporates many different elements relevant to design (including ergonomics in design, and reducing error through design), and to operation (including maintenance inspection and testing errors, human factors in risk assessment and incident investigation, and Human Reliability Analysis (HRA)/ Safety Critical Task Analysis (SCTA)).

- *Where to find more information: The HSE provide a large amount of human factors related information focussed on all the various related topics through their website [15]*

6.2 Maintenance, Inspections and Audits

As part of the lifecycle of a pipeline, there is a requirement for ongoing inspection, maintenance, and audits. For a new project there is a need to ensure that the pipeline project has been built as per the design and operates as expected, and this can be assessed in pre-commissioning and pre-operational acceptance reviews, assessments and inspections. For a more mature pipeline, maintenance, inspections, and audits can determine if the plant is operating within the conditions and parameters that form an input to the safety studies.

- *Where to find more information: Information covering these issues is included in IGEM TD-1 [16] and PD 8010-1 [17]*

6.3 Hazardous Area Classification

Hazardous area classification is used to identify places where, because of the potential for an explosive atmosphere, special precautions regarding sources of ignition are needed to prevent fires and explosions. Hazardous area classification studies identify where controls over ignition sources are needed (hazardous places) and also places where such controls are not necessary (non-hazardous places), with hazardous places further classified in Zones dependent on the chance of an explosive atmosphere occurring.

- *Where to find more information: Explosive atmospheres and area classification is covered in BS EN 60079-10-1 [18] and IGEM/SR/25 [19]*

6.4 Emergency Response Testing

In support of pipeline operations, an Emergency Response Plan (ERP) will be required/ in place to cover the actions to be taken in the event of an emergency. Under the Pipelines Safety Regulations (PSR) there is currently no requirement for testing and exercising pipeline emergency plans, however it is recognised by UKOPA that the testing and exercising of such plans is beneficial. UKOPA has therefore produced a suite of Good Practice Guides (GPGs) to support emergency response testing and exercising:

- *Where to find more information: UKOPA/GPG/010 [20], UKOPA/GPG/011 [21], UKOPA/GPG/012 [22], UKOPA/GPG/016 [23]*

6.5 Environmental Risk Assessment

An environmental risk assessment uses similar risk assessment techniques to those described within this document (e.g. identify hazards, assess the risk, identify and evaluate the controls in place and manage the risk) however the focus is on the environmental impacts associated with the pipeline activities. The environmental impact assessment may make use of some of the outputs from the studies described in Section 4 (for example the hazards identified in the HAZID), however specific documentation and studies (e.g. Best Available Techniques (BAT) reviews) are required as part of any environmental risk assessment.

6.6 Management of Change

Throughout the life of a pipeline there may be the requirement for change or modification to operations, equipment (including IT equipment/software) or people. This is normally managed through the organisation's management of change process, which will differ between operators. Generally though there may be a requirement to utilise some of the tools and techniques from Section 4 to assess the risk associated with the change, both in terms of updating any existing studies (e.g. the overall QRA), and to perform any new assessments to determine the risk associated with the change itself (e.g. utilisation of the risk assessment matrix).

6.7 Hazards During Construction (HAZCON)

For construction and decommissioning phases of a project, a Hazards During Construction (HAZCON) study may be performed as part of the project Construction Design and Management (CDM) requirements. A HAZCON is similar to a HAZID or HAZOP in that a workshop is performed utilising guidewords to identify hazards, risk and controls, however with the focus of the guidewords on the hazards associated with construction activities, design and safe working practices.

6.8 Site Layout and Pipeline Routing

As part of design and modification, it is necessary to consider the layout of the site and the routing of the pipeline in order to minimise the risk presented by the facilities where possible. The overall layout review takes into account the results of safety evaluations and studies, as well as utilising available spacing good practice and guidance.

- *Where to find more information: Information regarding layout and spacing is included in IGEM TD-1 [16] and PD 8010-1 [17]*

7. REFERENCES

[1] Center for Chemical Process Safety (CCPS), *Inherently Safer Chemical Processes: A Life Cycle Approach*, Second Edition, CCPS and John Wiley & Sons, Inc.; 2009

[2] IGEM Technical Gas Standard IGEM/G/7, *Risk assessment techniques*, Communication 1655, 2016

[3] BSI Standard BS EN 61882, *Hazard and operability studies (HAZOP studies) Application guide*, 2016

[4] BSI Standard BS EN IEC 60812, *Failure modes and effects analysis (FMEA and FMECA),* 2018

[5] IGEM Technical Gas Standard IGEM/TD/2, *Assessing the risks from high pressure Natural Gas pipelines*, Communication 1779, Edition 2, 2015

[6] BSI Standard BSI PD 8010-3, *Pipeline systems – Part 3: Steel pipelines on land – Guide to the application of pipeline risk assessment to proposed developments in the vicinity of major accident hazard pipelines containing flammables,* Edition A1, 2013

[7] BSI Standard BS EN 61025, *Fault tree analysis (FTA),* April 2007

[8] CCPS in association with the Energy Institute, *Bow Ties In Risk Management - A Concept Book for Process Safety*, Wiley-American Institute of Chemical Engineers, September 2018

[9] BSI Standard BS EN ISO 20815, *Petroleum, petrochemical and natural gas industries. Production assurance and reliability management*, 2018

[10] BSI Standard BS EN 61511, *Functional safety — Safety instrumented systems for the process industry sector*, 2018

[11] BSI Standard BS EN 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010

[12] UKOPA Good Practice Guide UKOPA/GP/025*, Application of cost benefit analysis to demonstrate ALARP*, Edition 1, December 2018

[13] BSI Standard BS EN IEC 31010*, Risk management – Risk assessment techniques,* 2019

[14] UKOPA Good Practice Guide UKOPA/GP/018, *Remaining Life Assessment,* Edition 1, March 2020

[15] UK Health and Safety Executive, *Human factors and ergonomics* https://www.hse.gov.uk/humanfactors/index.htm

[16] IGEM Technical Gas Standard IGEM/TD/1, *Steel pipelines and associated installations for high pressure gas transmission*, Communication 1789, Edition 5, 2016

[17] BSI PD 8010-1, *Pipeline systems – Part 3: Steel pipelines on land – Code of practice*, second edition, 2015

[18] BSI Standard BS EN 60079-10-1*, Explosive atmospheres. Classification of areas. Explosive gas atmospheres,* 2015

[19] IGEM Technical Gas Standard IGEM/SR/25*, Hazardous Area Classification of Natural Gas Installations,* Communication 1748, Edition 2, 2010

[20] UKOPA Good Practice Guide UKOPA/GPG/010, *Major Accident Hazard Pipeline (MAHP) Emergency Response Plan Guidance on Testing*, Edition 1, April 2017

[21] UKOPA Good Practice Guide UKOPA/GPG/011, *Major Accident Hazard Pipeline (MAHP) Emergency Response Plan: Emergency Plan Template*, Edition 1, April 2017

[22] UKOPA Good Practice Guide UKOPA/GPG/012, *Major Accident Hazard Pipeline (MAHP) Emergency Response Plan: Testing and Exercising Pro-forma*, Edition 1, April 2017

[23] UKOPA Good Practice Guide UKOPA/GPG/016, *Pipeline Hazard Distances*, Edition 1, April 2018