TECHNICAL SPECIFICATION

ISO/TS 16901

First edition
2015-03-01

Guidance on performing risk assessment in the design of onshore LNG installations including the ship/shore interface

Guide pour l'évaluation des risques dans la conception d'installations terrestres pour le GNL en incluant l'interface terre/navire

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

Reference number
ISO/TS 16901:2015(E)

© ISO 2015

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

The committee responsible for this document is ISO/TC 67, *Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries*.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

Guidance on performing risk assessment in the design of onshore LNG installations including the ship/shore interface

1 Scope

This Technical Specification provides a common approach and guidance to those undertaking assessment of the major safety hazards as part of the planning, design, and operation of LNG facilities onshore and at shoreline using risk-based methods and standards, to enable a safe design and operation of LNG facilities. The environmental risks associated with an LNG release are not addressed in this Technical Specification.

This Technical Specification is aimed to be applied both to export and import terminals, but can be applicable to other facilities such as satellite and peak shaving plants.

It applies to all facilities inside the perimeter of the terminal and all hazardous materials including LNG and associated products: LPG, pressurised natural gas, odorizers, and other flammable or hazardous products handled within the terminal.

The navigation risks and LNG tanker intrinsic operation risks are recognised, but they are not in the scope of this Technical Specification. Hazards arising from interfaces between port and facility and ship are addressed and requirements are normally given by port authorities. It is assumed that LNG carriers are designed according to the IGC code, and LNG fuelled vessels receiving bunker is designed according to IMO's regulations.

Border between port operation and LNG facility is when the ship/shore link (SSL) is established.

It is not intended to specify acceptable levels of risk; however, examples of tolerable levels of risk are referenced.

This Technical Specification is not intended to be used retrospectively.

It is recognised that national and/or local laws, regulations, and guidelines take precedence where they are in conflict with this Technical Specification.

Reference is made to ISO 31010 and ISO 17776 with regard to general risk assessment methods, while this Technical Specification focuses on the specific needs scenarios and practices within the LNG industry.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies

ISO/IEC Guide 73:2009, *Risk management — Vocabulary*

ISO 17776:2000, *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment*.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73 and the following apply.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

3.1
as low as reasonably practical
ALARP
reducing a *risk* (3.26) to a level that represents the point, objectively assessed, at which the time, trouble, difficulty, and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained

3.2
boiling liquid expanding vapour explosion
BLEVE
sudden release of the content of a vessel containing a pressurised liquid and for flammables often followed by a fireball

Note 1 to entry: This hazard is not applicable to atmospheric LNG tanks, but to pressurized forms of hydrocarbon storage.

3.3
bow-tie
pictorial representation of how a hazard can be hypothetically released and further developed into a number of *consequences* (3.6)

Note 1 to entry: The left-hand side of the diagram is constructed from the fault tree (causal) analysis and involves those threats associated with the hazard, the controls associated with each threat, and any factors that escalate likelihood. The right-hand side of the diagram is constructed from the hazard event tree (consequence) analysis and involves escalation factors and recovery preparedness measures. The centre of the bow-tie is commonly referred to as the "top event".

3.4
cost to avert a fatality
CAF
value calculated by dividing the costs to install and operate the protection/*mitigation* (3.18) by the reduction in *potential loss* (3.20) of life (PLL)

Note 1 to entry: It is a measure of effectiveness of the protection/mitigation.

3.5
computational fluid dynamics
CFD
numerical methods and algorithms to solve and analyse problems that involve fluid flows

3.6
consequence
outcome of an event

3.7
cost benefit analysis
CBA
means used to assess the relative cost and benefit of a number of *risk* (3.26) reduction alternatives

Note 1 to entry: The ranking of the risk reduction alternatives evaluated is usually shown graphically.

3.8
design accidental load
DAL
most severe accidental load that the function or system shall be able to withstand during a required period of time, in order to meet the defined *risk* (3.26) acceptance criteria

3.9
explosion barrier
structural barrier installed to prevent explosion damage in adjacent areas

Note 1 to entry: A wall is an example of an explosion barrier.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

3.10
F/N curve
FN
plot of cumulative frequency versus N or more persons that sustain a given level of harm from defined sources of hazards

3.11
failure mode and effect analysis
FMEA
analytically derived identification of the conceivable equipment failure modes and the potential adverse effects of those modes on the system and mission

Note 1 to entry: It is primarily used as a design tool for review of critical components.

3.12
fatal accident rate
FAR
number of fatalities per 100 million hours exposure for a certain activity

3.13
harm
physical injury or damage to the health of people or damage to property or the environment

3.14
hazard
potential source of *harm* (3.13)

3.15
hazard identification
HAZID
brainstorming exercise using checklists the hazards in a project are identified and gathered in a *risk register* (3.37) for follow up in the project

3.16
hazard and operability study
HAZOP
systematic approach by an interdisciplinary team to identify hazards and operability problems occurring as a result of deviations from the intended range of process conditions

Note 1 to entry: All four steps are in place and recorded to manage a hazard completely.

3.17
impact assessment
assessment of how *consequences* (3.6) (fires, explosions, etc.) do affect people, structures the environment, etc.

3.18
mitigation
limitation of any negative *consequence* (3.6) of a particular event

3.19
Monte Carlo simulation
simulation having many repeats, each time with a different starting value, to obtain distribution function

3.20
potential loss
product of frequency and *harm* (3.13) summed over all the outcomes of a number of top events

3.21
probability
extent to which an event is likely to occur

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

3.22
probit
inverse cumulative distribution function associated with the standard normal distribution

Note 1 to entry: Probit is used in QRA to describe the relation between exposure, e.g. to radiation or toxics, and fraction fatalities.

3.23
protective measure
means used to reduce risk

3.24
quantitative risk assessment
QRA
techniques which allow the *risk* (3.26) associated with a particular activity to be estimated in absolute quantitative terms rather than in relative terms such as high or low

Note 1 to entry: QRA may be used to determine all risk dimensions, including risk to personnel, risk to the environment, risk to the installation, and/or the assets and financial interests of the company. Reference is made to ISO 17776:2000, B.12.

3.25
residual risk
risk (3.26) remaining after *protective measures* (3.23) have been taken

3.26
risk
combination of the *probability* (3.21) of occurrence of *harm* (3.13) and the severity of that harm

3.27
risk analysis
systematic use of information to identify sources and to estimate the *risk* (3.26)

3.28
risk assessment
overall process of *risk analysis* (3.27) and *risk evaluation* (3.31)

3.29
risk contour
RC
two dimensional representation of *risk* (3.26) on a map

Note 1 to entry: Also called individual risk contours (IRC) or location-specific risk (LSR).

3.30
risk criteria
terms of reference by which the significance of *risk* (3.26) is assessed

3.31
risk evaluation
procedure based on the *risk analysis* (3.27) to determine whether the *tolerable risk* (3.45) has been achieved

3.32
risk management
coordinated activities to direct and control an organization with regard to *risk* (3.26)

3.33
risk management system
set of elements of an organization's management system concerned with managing *risk* (3.26)

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

3.34
risk matrix
matrix portraying *risk* (3.26) as the product of *probability* (3.21) and *consequence* (3.6), used as the basis for risk determination

Note 1 to entry: Considerations for the assessment of probability are shown on the horizontal axis. Considerations for the assessment of consequence are shown on the vertical axis. Multiple consequence categories are included: impact on people, assets, environment and reputation. Plotting the intersection of the two considerations on the matrix provides an estimate of the risk.

3.35
risk perception
way in which a *stakeholder* (3.44) views a *risk* (3.26) based on a set of values or concerns

3.36
risk ranking
outcome of a qualitative *risk analysis* (3.27) with a numerical annotation of *risk* (3.26)

Note 1 to entry: It allows accident scenarios and their risk to be ranked numerically so that the most severe risks are evident and can be addressed.

3.37
risk register
hazard management communication document that demonstrates that hazards have been identified, assessed, are being properly controlled, and that recovery preparedness measures are in place in the event control is ever lost

3.38
risk transect
RT
representation of *risk* (3.26) as a function of distance from the hazard

3.39
rollover
sudden mixing of two layers in a tank resulting to a massive vapour generation

3.40
rapid phase transition
RPT
explosive change from liquid into vapour phase

Note 1 to entry: When two liquids at two different temperatures come into contact, explosive forces can occur, given certain circumstances. This phenomenon, called rapid phase transition (RPT), can occur when LNG and water come into contact. Although no combustion occurs, this phenomenon has all the other characteristics of an explosion. RPTs resulting from an LNG spill on water have been both rare and with relatively limited *consequences* (3.6).

3.41
safety
freedom from unacceptable *risk* (3.26)

3.42
SIMOPS
concatenation of simultaneous operations

Note 1 to entry: SIMOPS often refers to events such as maintenance or construction work in an existing plant when there are more personnel near a live operating plant and who are exposed to a higher level of *risk* (3.26) than normal.

3.43
showstopper
event or *consequence* (3.6) that produces an unacceptable level of *risk* (3.26) such that the project cannot proceed and where the level of risk cannot be mitigated to an acceptable level

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

3.44
stakeholder
any individual, group, or organization that can affect, be affected by, or perceive itself to be affected by a *risk* (3.26)

3.45
tolerable risk
risk (3.26) which is accepted in a given context based on the current values of society

4 Abbreviations

For the purposes of this Technical Specification, the following abbreviations apply:

ALARP	as low as reasonably practical;
BLEVE	boiling liquid expanding vapour explosion;
CAF	cost to avert a fatality;
CFD	computational fluid dynamics;
CBA	cost benefit analysis;
DAL	design accidental load;
EDP	emergency depressuring;
ERC	emergency release coupling;
ESD	emergency shutdown;
ETA	event tree analysis;
FAR	fatal accident rate;
FEED	front-end engineering design;
FEM	finite element method;
FN	frequency vs number (of affected individuals);
FMEA	failure mode and effect analysis;
FMECA	failure, modes, effects, and criticality analysis;
HAZID	hazard identification;
HAZOP	hazard and operability study;
HEMP	hazards and effects management process;
IR	individual risk contour;
LSR	location-specific risk;
LOPA	layers of protection analysis;
MTTF	mean time to failure;
MTTR	mean time to repair;

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

OBE	operating basis earthquake;
PERC	power emergency release coupler;
P&IDs	process and instrument diagrams;
PIMS	pipeline integrity management system;
PLL	potential loss of life;
QRA	quantitative risk assessment;
RC	risk contour;
RPT	rapid phase transition;
RT	risk transect;
SIL	safety integrity level;
SMS	safety management system;
SSE	safe shutdown earthquake;
SSL	ship/shore link.

5 Safety Risk Management

5.1 Decision support framework for risk management

Safety risk management is integrated in the project development and decision making processes and need as consistent support for decisions in all phases of an LNG development but does not include the full operational lifecycle.

The approach to risk management should address the project-specific requirements as agreed between the different parties and stakeholders and also establish an agreed format to communicate risk and ensure that decisions are made in a consistent and agreed format through the life of the project.

The acceptance criteria including the format should be defined in compliance with regulations and company standards. The format of the acceptance criteria prescribes thereby the approach as discussed below.

There is a wide range of tools and approaches that can be used to support decisions related to risk management. UK Offshore Operators Association (UKOOA) presented a framework for decision support reflecting the significance of the decision as well decision context. The framework as shown for information in Figure 1 illustrates the balancing between use of codes and standards, QRA, and decision processes reflecting company and societal values.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

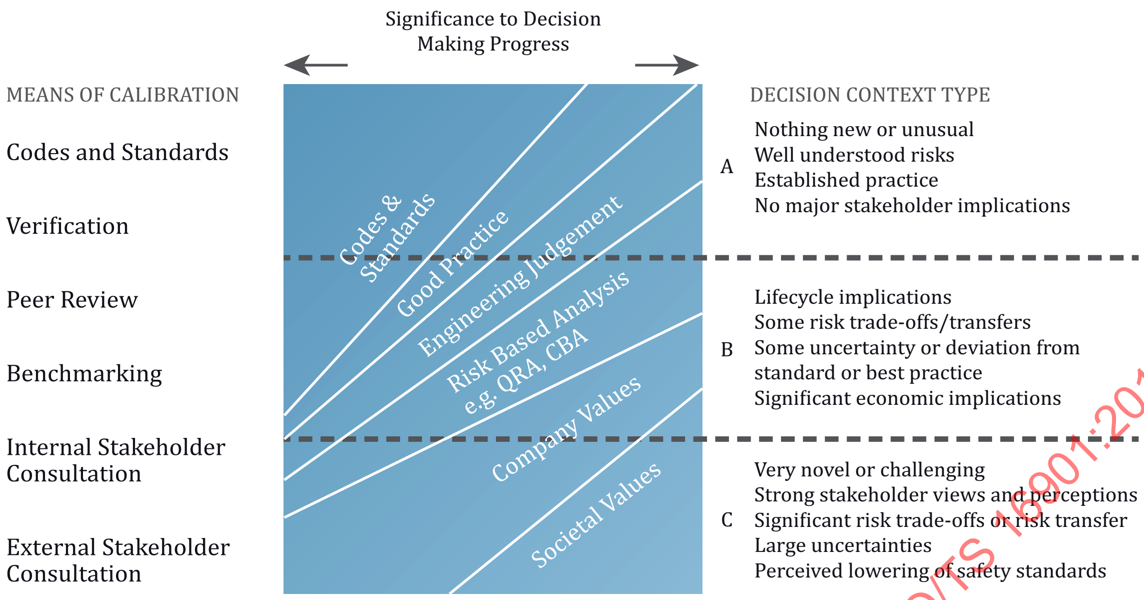

Figure 1 — Decision support framework for major accident risk management

5.2 Prescriptive safety or risk performance

Both prescriptive and risk-based approaches are used in the planning, design, and operation of LNG facilities.

Prescriptive approaches represent industry experience and practices.

The main advantages with prescriptive approaches are predictability and effective decision processes in the design.

The main objections to the use of prescriptive approaches are that they do not accommodate new solutions and thereby can limit novel development and improvement. Further, when the requirements are met, the prescriptive approaches do not encourage a continued effort for further improvements.

Risk-based approaches have developed in the nuclear and offshore industries. Risk-based approaches are used in many parts of the world and are gaining a wider usage.

In essence, risk-based approaches start from first principles aiming at demonstration that the risk acceptance criteria are met with a proper selection of design and operational measures. In principle, no "prescribed solutions" should be given as a starting point (but in reality, good industry experience, practices, and standards are adopted as the starting point).

The main advantage of a risk-based approach is that it does stimulate new and improved solutions; it encourages continuous focus on improved safety, and it focuses efforts on the key areas as formulated in the risk acceptance criteria.

Normally, a risk-based approach starts early and focuses the attention on the key issues that should be addressed in the different project phases. In most cases, a risk-based approach ensures that the correct decisions are made at the right time and thereby avoids costly revisions and adjustments. Further, the site specific conditions and particular stakeholder views are better reflected.

The main criticism to risk-based approaches focuses on the complexity of the process, and the line of responsibility can become unclear. It is essential that risk acceptance criteria are established and derived from national and international regulations and owner's requirements.

It is often found that a risk-based design does not enable all engineering design disciplines to proceed on a firm design basis until the results from the risk analysis is available. This can have a schedule impact.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

Further, the uncertainty involved due to e.g. lack of relevant failure data, model assumptions can make it difficult to relate to the results. A situation where detailed results from sophisticated computational models can generate false confidence in the results can lead to the wrong conclusion. The uncertainty is a particular concern when a risk-based approach is used to demonstrate that sensible safety measures are not needed.

Risk analyses shall not be used to deviate from good engineering practice.

Finally, it is often claimed that the lack of predictability leads to increased cost. But the savings earned by adopting novel solutions can be significant but difficult to quantify.

Successful use of a risk-based approach normally requires an iterative process where the first layouts and decision are based on experience and industry practice (i.e. prescriptive guidelines, standards for process design, etc.) and that this first estimate is qualified and improved using risk-based techniques.

Risk analyses also enable areas and causes of higher risk to be identified so that mitigation measures can be applied in a cost effective manner.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

5.3 Risk assessment in relation to project development

Risk assessment is used for decision support.

The decisions being made in the different phases of a project development vary, and the need for decision support accordingly.

The available information and level of detail as input to any risk assessment increase as the planning progresses. As a result, the requirements to risk assessment techniques and results vary over the project phases, and this can represent a challenge in the communication of the results.

In the early phase of the planning where the key issue is to select business model and technical concept, the main risk activities are to establish risk criteria and safety targets, as well as to demonstrate absence of showstoppers. This requires qualitative approaches.

At this stage of project development, quantitative risk analyses have limited value as no detailed information to describe the facilities are available as input.

In the next phase, the risk assessment should provide quantitative risk information related to the land planning in support of the permitting process.

In later project phases where key issues are the design of mitigation measures, more detailed analyses are appropriate to provide a proper basis for project decisions.

In some jurisdictions, the planning process makes it difficult to modify proposals once they have been submitted to the planning authorities. This makes it difficult to modify the design to reduce risk as detailed engineering develops. This aspect should be considered in project planning.

The requirements, recommendations, and advice given in this Technical Specification reflect this need. Risk assessment and risk results shall always reflect the following:

a) the type of decision that shall be made;

b) effective utilization of available information.

Actions arising from reviews such as HAZID, risk matrix, HAZOP, etc., which are not closed out after the review, should be recorded in a tracking system (for example, a risk register). This should answer that items requiring action at later project stages (i.e. items for operating manuals, etc.) should not be overlooked or forgotten.

This varying level of details in the risk assessment process is illustrated in Table 1 which also is relevant to a wide range of different types of industrial risk assessment

© ISO 2015 – All rights reserved

Table 1 should be used in preference to ISO 13010, Table A.1 to identify risk assessment methods. Further description is given in Clause 7.

Table 1 — Typical requirements to risk-related information in different project phases

Project phase	Needed risk related information	Key decisions based on risk assessment	Method of risk assessment within this guideline
Pre-FEED (i.e. Concept selection and business case development)	— Identify stakeholders — Input to the permitting process (demonstrate absence of showstoppers) — Risk criteria — First estimate of the risk level (when required by regulators) — Basic design options — Go-ahead for the development	— Select site — Select concept — Identify and decide risk criteria — Select design criteria — Select design options — Approve continued development	— HAZID — Consequence analyses of major accident scenarios — Prepare risk criteria — Risk communication to legislation and stakeholders
FEED Development of basic design	— Focus areas for the design process, i.e. results from HAZID and Consequence analysis — Estimate of the risk level of design options — Basis for selection of an optimised basic design	— Optimisation of the design in terms of safety by comparison of options — Select main technologies — Performance standards for safety system — Confirm concept selection — Authority permit — Decide to start detail design	— Qualitative analysis (risk matrix) — HAZOPs and determination of SIL requirements — QRA — Determine DALs — Detailed consequence assessment — Fire/explosion analysis — Risk communication to legislation and stakeholders
Detail design	— Performance standards for components and systems — Issues to be addressed in the design identified in HAZOP findings incl. SIL requirements — Specifications for buildings and equipment	— Selection of equipment, solutions and operational procedures — Detailed design	— Detailed QRA — Detailed HAZOPs — SIL assessment — Vendor HAZOPs — Evacuation analysis
Commissioning and start-up	— Final results from risk assessment — Confirmation of acceptance according to regulations	— Approve the design — Approve decision to start up	— Completion of risk studies and verification schemes — Commissioning of safety systems — Risk communication to legislation and stakeholders

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

6 Risk

6.1 What is risk

Risk is defined in ISO 17776 as combination of the probability of an event and the consequences of the event. To be able to express the risk, the consequences shall be defined and the associated probability determined.

Risk is also often referred to as potential loss. The loss or consequence can be loss of life, money, production, or damage to the environment. The probability term is usually expressed as a frequency. In QRAs, the potential loss in general is not calculated from the product of one event and one consequence, but the sum of a large number of frequency and consequence probability combinations.

Risk or potential loss, combination of the probability of an event, and the consequences of the event cannot be readily used as an indicator to decide the tolerability of the risk. It can be used to compare options when all things different between the two options have been evaluated in terms of probability and consequence and included in the assessment.

To be able to use risk in workable concepts, a number of risk indicators have been developed to express risk. These risk indicators are discussed in 6.5.

6.2 Safety philosophy and risk criteria

LNG developments are often organized as project organizations (e.g. JV) with international participation. It is therefore important for LNG projects to formulate a safety philosophy and risk criteria's based on recognized guidelines/standards in their risk management process, provided that they are not in conflict with national statutory minimum requirements. This aids the project team in gaining a common terminology, understanding of risk, risk philosophy, and ultimately a common risk management system.

The safety philosophy and risk criteria for the project can address the following categories:

— Risk to the population and third-party activities. This has significant impact on the land use and is normally defined by national regulations;

— Risk to personnel in the plant. This is normally defined by the company philosophy but should also be in agreement with national regulation;

— Risk with respect to material damage and loss of production. The criteria should be defined by the company and are often based on a cost benefit assessment;

— Limitations on third-party activity due to hazards arising from the facility.

Examples of the risk criteria required by different authorities are discussed in A.7 and examples of project-specific criteria in A.8.

6.3 Risk control strategy

A widely accepted risk control strategy is the following:

a) adopt inherently safe design;

b) prevent – consider measures that will avoid the hazard;

c) reduce probability of occurrence trough design, inspection, maintenance, and working practices;

d) mitigate consequences – minimise the outcome of an unwanted event;

e) emergency response – enable returning to a controlled situation.

This can be formalized in the bow-tie methodology as described in 7.2.4. The bow-tie is a model that represents how a hazard can be released, escalate, and how it is controlled.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

6.4 ALARP

A common approach is to divide risks into three bands:

a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity can bring, and risk treatment is essential whatever its cost;

b) a middle band (or "grey" area) where costs and benefits are taken into account and opportunities balanced against potential consequences;

c) a lower band where the level of risk is regarded as negligible or so small that no risk treatment measures are needed.

The "as low as reasonably practicable" or "ALARP" criteria system follows this approach and is illustrated in Figure 2.

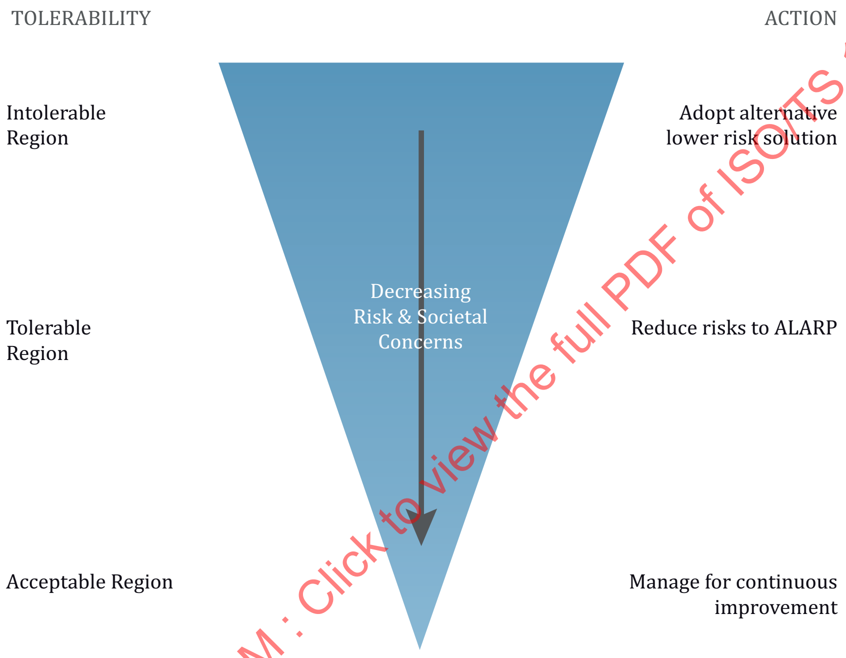

Figure 2 — Risk Reduction Triangle

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

ALARP is the process in which all identified options to reduce the risk have been evaluated. A major part of the ALARP process is the documentation of which options have been evaluated and why they have been included in the design or why they have been discarded. The documentation can be consulted when the circumstances change or when the design is challenged in the future. In general, only full documentation for high risks and complicated medium risk is required as it is not reasonable to insist on full documentation for low risk.

The assessment of risk is not an exact science and the techniques used and the experience of the analyst has been shown to produce widely varying result as discussed in studies on uncertainties in chemical risk assessment using a benchmark exercise in 1992 and a 2002 Risø study about uncertainties in risk analysis of chemical establishments.

The results are evaluated against company or regulatory criteria and there is often a tendency to stop the improvement process when the criteria apparently are satisfied to minimise further capital and manpower expenditure.

The ALARP approach is a conceptual model and there are no boundaries between the three regions. The factors that ultimately decide how a risk is categorized (intolerable, tolerable, ALARP, or acceptable) are dynamic in nature.

 © ISO 2015 – All rights reserved

The addition/deletion or modification of mitigation features to just meet the acceptance criteria is strongly discouraged due to the accuracy of the process.

The ALARP process should be continued until the optimum design without incurring excessive cost is achieved. At the conceptual stage, it is often found that risk can be reduced at very low cost.

It is therefore important to start the risk assessment early in the project.

6.5 Ways to express risk to people

6.5.1 General

Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear (see ISO 31010), and reflect the safety criteria as defined by legislation and operator. An example of ways to express risk to people is given in A.8.

A number of risk indicators are used in the LNG industry for risk assessments when relating risk to people. The more commonly used are discussed in detail in the next sub-clauses.

- risk contours (RC);
- risk transects (RT);
- individual risk (IR);
- potential loss of life (PLL);
- fatal accident rate (FAR);
- cost to avert a fatality (CAF);
- F/N curves (FN).

6.5.2 Risk contours (RC)

The risk contour is an iso-risk line overlaid on the site topography at which a hypothetical individual staying there unprotected and for 24 hours per day 365 days per year is subject to a defined probability of harm due to exposure to hazards induced by an activity.

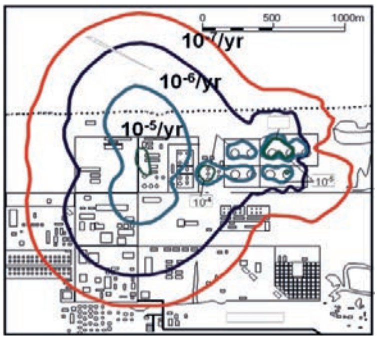

Figure 3 — Examples of risk contours showing predicted risk levels

It is also called location risk and sometimes referred to as individual risk or individual risk contours. An example of a set of risk contours is shown in Figure 3.

Although the hypothetical individual is exposed when the scenario occurs, escape and refuge can be taken into account.

In general, risk contours are calculated by determining the consequences from a number of scenarios. By adapting certain criteria for harm (most often dead) from toxic substances, radiation from fires,

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

and explosion overpressure, effect distances can be determined. Based on incident frequencies and effects from meteorological conditions (wind direction/wind speed/Pasquill stability distribution), the contribution from each scenario to a point at a distance from the activity can now be calculated. By putting a grid over the area surrounding the activity and summing the contribution from all scenarios for each grid point, a three-dimensional (x, y, risk) picture will emerge. Usually, this picture is then reduced to 2D by connecting points of equal risk e.g. 10^{-5}/year, 10^{-6}/year, and 10^{-7}/year.

6.5.3 Risk transects (RT)

Risk transects are similar presentations where the risk contour values or IR/year are plotted versus the lateral distance.

6.5.4 Individual risk (IR)

Individual risk is defined as the probability of being killed (or harmed at certain level) on an annual basis from all hazards. It is risk to an identifiable person or group with similar exposure patterns.

Sometimes it is calculated by dividing the PLL (which can be over the project life or per year) by the number of people exposed. However, it should be realised that this is averaging the people at high risk levels with the people at low risk levels and therefore is not an IR.

IR should be calculated by following someone for a year and add the different risk contributions like transport, small work, major hazards, etc. Most of these contributions can be calculated using the number exposure hours per year and FAR.

6.5.5 Potential loss of life (PLL)

PLL is defined as the expected value of the number of fatalities per year (or over the life time of a project). PLL is a type of risk integral, being a summation of risk as expressed by the product of frequency and consequence (number of fatalities). The integral is summed up over all potential events that can occur. It is mainly used to compare options and enables the inclusion of different risk types like process, transport, workplace hazards, etc. in one number.

6.5.6 Fatal accident rate (FAR)

The number of people killed per 100 million exposure hours. FAR for all kind of activities are available in the open literature and are used to calculate the risk contribution from non-major hazards like transport, small work, etc.

6.5.7 Cost to avert a fatality (CAF)

Cost to avert a fatality is defined as the cost to reduce the hazard divided by the reduction in PLL.

In general, two sets of PLL calculations are done:

— one base-line calculation;

— one with increased protection/mitigation.

CAF is the calculated by dividing the costs to install and operate the protection/mitigation by the reduction in PLL.

6.5.8 F/N curves (FN)

Societal risk is often depicted on a cumulative graph called an F/N curve. The horizontal axis is the number of potential fatalities, N. The vertical axis is the cumulative frequency F per year that N or more fatalities could occur. F/N curves are an indicator used by authorities as a measure for social disruption in case of large accidents.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

It is normal to take account of protection by buildings and response by people. For large toxic release models, alarm and evacuation can be included. The resulting curve is then the residual risk, should the emergency plans not be effective.

Because it is a cumulative curve, the curve always drops away with increasing N. Usually, the curve has a lower frequency cut-off, e.g. at one in a billion.

Regulators often split the graph into different regions, so that different actions can be undertaken depending on where the F/N curve falls. Sometimes a maximum limit is placed on N.

6.6 Uncertainties in QRA

Uncertainties are introduced mainly by the estimation of probabilities and frequencies and, to a lesser degree, by estimating effects and consequences.

When comparing between options, as long as the two options are for a similar operation, the uncertainty is on both sides and tends to cancel it out. On close examination, one often finds that the difference between the two options is in a different exposure caused by, for example, more people.

This often makes marginal differences already significant.

Uncertainty is more of an issue when comparing RC, IR, CAF, and FN with tolerability criteria set by local legislation or by companies for internal use. The calculated RC, IR, CAF, and FN are then compared to absolute values and often the uncertainty is not part of the evaluation.

For this reason, it is advised to do sensitivity calculation by changing the various parameters like failure rates, ignition probabilities, etc.

7 Methodologies

7.1 Main steps of risk assessment

The main steps in a risk assessment can be summarised to identify the following:

— What can go wrong? (hazard identification);

— What is the effect? (consequence and impact assessment);

— What is the likelihood? (frequency assessment);

— Is the risk tolerable, and should risk reducing measures be implemented?

This sequence of steps avoids the requirement to perform a detailed frequency assessment for hazards having insignificant consequences.

The main methodologies used in risk assessment in the different project phases are given in ISO 31010 and ISO 17776 and as listed in Table 1 are described in more detail below.

7.2 Qualitative risk analysis

7.2.1 HAZID

The complexity and diversity of LNG facilities lead to inability to comprehensively identify potential major hazards and operability difficulties within process plant design and operation intuitively. Techniques are therefore required to systematically list these hazards in a detailed, structured, and methodical manner. The HAZID is a technique used for early identification of potential hazards and threats. It is also suited to the identification of non-process related hazards such as ship collision, dropped objects, extreme weather etc. The effect or possible consequence of an untoward incident is itemised and the possible causes determined.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

The HAZID technique is a

— means of identifying and describing occupational HSE hazards and threats at the earliest practicable stage of a development or venture,

— meeting employing a highly experienced multi-discipline team using a structured brainstorming technique, based on a checklist (see A.4) of potential HSE issues, to assess the applicability of potential hazards, and

— rapid identification and description process only, not a forum for trying to solve potential problems.

A common HAZID meeting organisation should involve a facilitator supported by experienced representatives from process design, safety engineering, operations, marine specialist if required, and instrument engineering. Other specialist should be available "on call".

Figure 4 presents the methodology of a HAZID workshop. The structure of the workshop should reflect the purpose of the review, i.e.

— the review of arrangements and safeguards for process facilities will normally be structured according to the process flow (i.e. compression, inlet separation, pretreatment, etc.);

— a review of the operations related to cargo transfer to an LNG carrier should reflect the operational sequence.

Once hazards, consequence, and safeguards are identified, risk ranking is carried out and recommendations are made to overcome or improve the hazards. The process of risk ranking is normally performed using a risk matrix which is further discussed in 7.2.3.

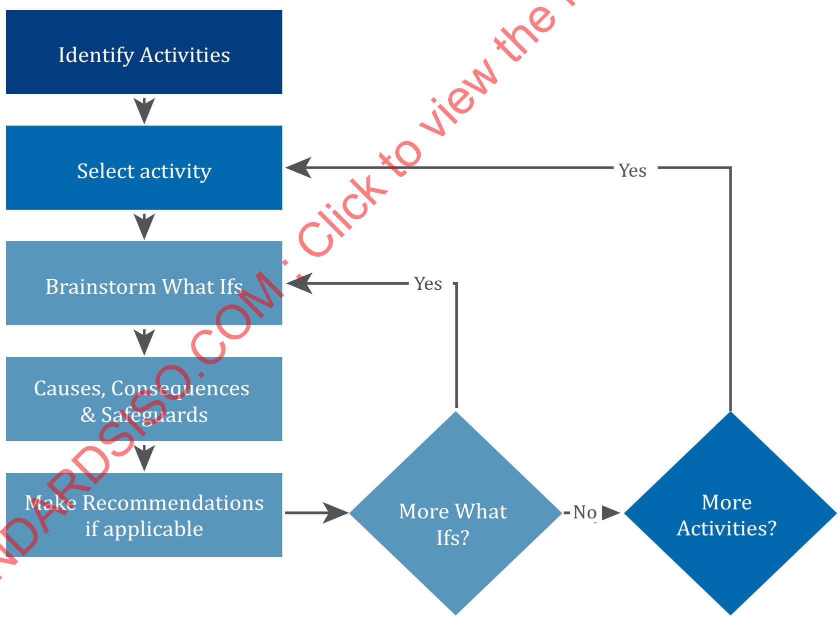

Figure 4 — Process during a HAZID workshop

The HAZID shall produce a list of recommendations and an action plan. This action plan addresses each recommendation developed along the HAZID meeting and shall be tracked (for example, via a risk register) for its assessment and implementation.

A typical HAZID workshop is normally recorded with the following:

— activity ID;

— function;

— failure mode;

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

— failure mechanism/cause;

— system failure effect;

— consequence category (environment, people, cost, reputation);

— consequence (ranked according to risk matrix being used);

— likelihood (ranked according to risk matrix being used);

— criticality (low, medium, or high);

— action items identified;

— comments.

7.2.2 Failure mode and effect analysis (FMEA)

The definition of failure mode and effect analysis is an analytically derived identification of the conceivable equipment failure modes and the potential adverse effects of those modes on the system and mission. It is primarily used as a design tool for review of critical components.

Further details are given in ISO 31010, B.13 and ISO 17776, B.9.

7.2.3 Risk matrix

The risk matrix is an effective tool for qualitative risk assessment and screening. It is normally used in workshops in support of HAZIDs and FMEA. It can be used during the following quantitative analysis (see 7.3 and 7.4). The results from the detailed analysis in terms of frequency and consequences can be reported in the matrix. This enables to track and tune the efficiency of the risk-reducing measures, qualify initial assumptions, and confirm the initial scenario ranking.

An example of a risk matrix from ISO 17776, A.1 is shown in Figure 5.

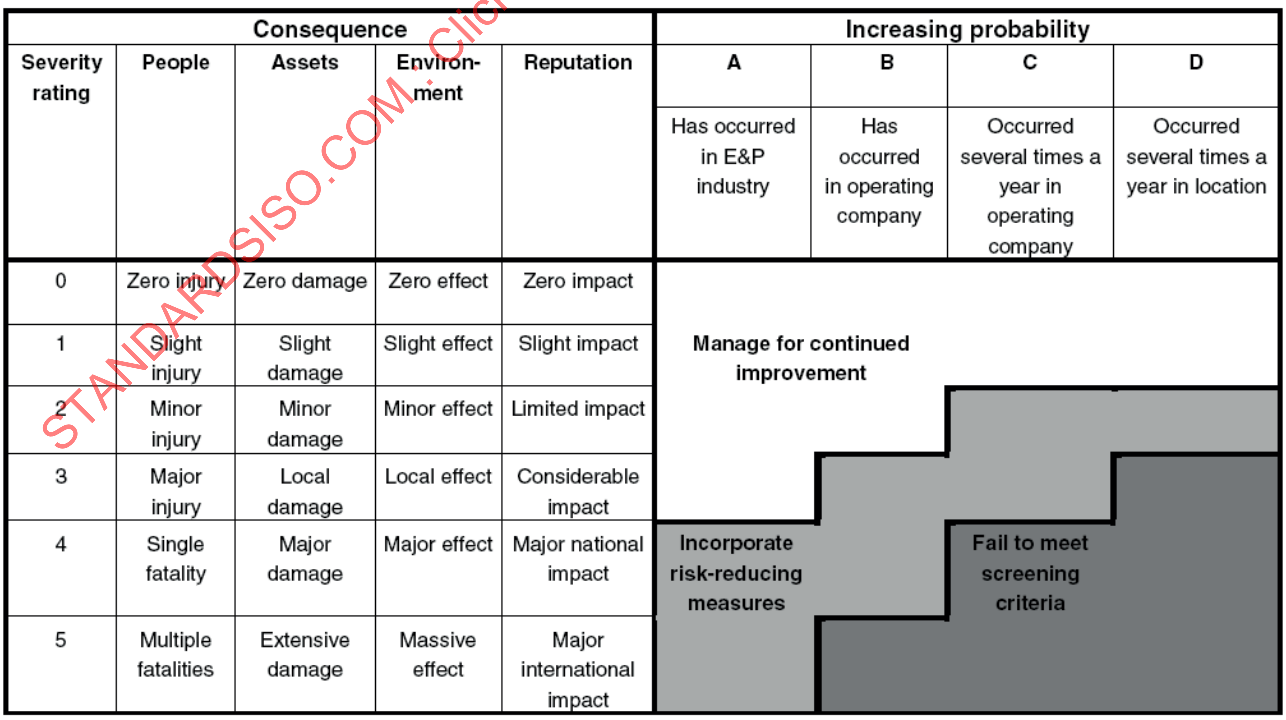

Figure 5 — Example of a risk matrix (source: ISO 17776, A.1)

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

The risk matrix should reflect the company, national and international regulations and practices.

7.2.4 Bow-tie

The bow-tie is a design tool that can be used to assess barriers to prevent occurrence of top events and recovery measures to reduce the consequences. It is based on a model that represents how a hazard can be released, escalate, and how it is controlled. Figure 6 shows the bow-tie diagram.

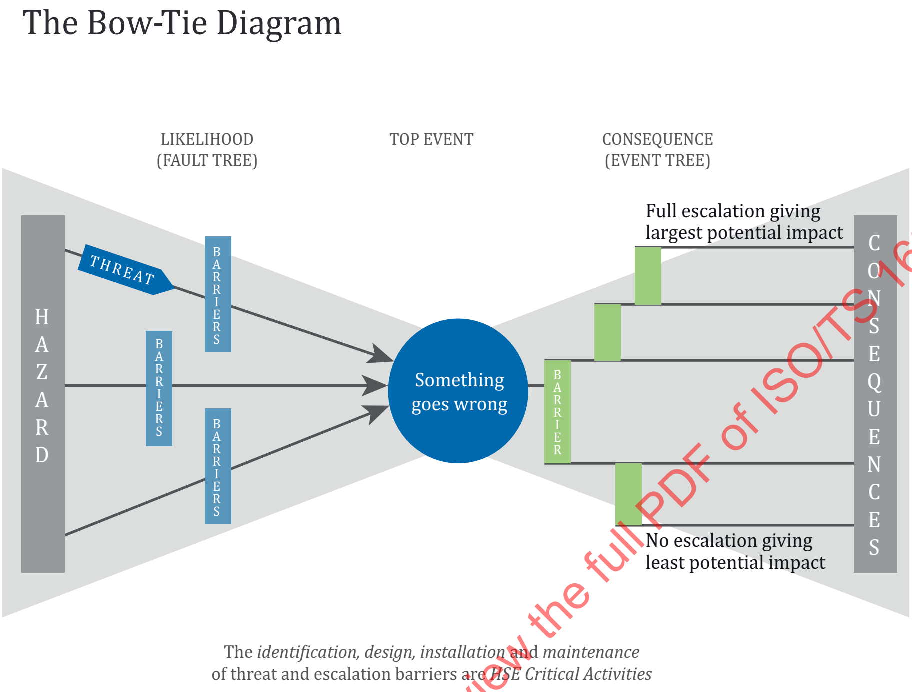

Figure 6 — Bow-tie diagram

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

The bow-tie model provides for the assessment of hazards in order to:

— identify the potential hazard release, escalation, and consequence scenarios;

— identify the controls (i.e. barriers and escalation factor controls) required to effectively manage these hazards, (e.g. the HSE critical elements, HSE critical tasks, and procedures);

— support the ALARP demonstration;

— provide visibility and communicate the above information to those responsible for managing, or who may be affected by the hazards;

— in the event of an incident, have the ability to relate causes of incidents to the controls that failed, thus enabling improved incident learning and prevention.

A barrier is the common term for controls, recovery measures, and escalation factor controls that prevent a threat from being released and then causing the consequences. Barriers prevent or reduce the probability of each threat or prevent, limit the extent of, or provide immediate recovery from the consequences. Barriers to the left of the top-event in the bow-tie are preventive measures. Barriers to the right of the top-event are recovery measures.

© ISO 2015 – All rights reserved

Barriers can be for example:

- — design features (e.g. separation distances);
- — hardware (e.g. pressure relief valve, fire detection);
- — processes (e.g. lock out/tag out);
- — operational intervention tasks (e.g. plant monitoring/shutdown);
- — combination (e.g. alarm plus operator action).

An adequate set of barriers to manage each threat shall be identified. For a barrier to be valid, it shall be:

- — effective in preventing the top-event or consequence;
- — able to prevent a specific threat from releasing the hazard;
- — verifiable (e.g. through audit of the HSE critical activity needed to maintain an effective barrier);
- — independent of the other barriers within the same threat line.

The application of the "bow-tie" depends on company and national regulations representing acceptance criteria and practices.

The barriers are counted from the threat to the consequence. Table 2 contains the required numbers to demonstrate ALARP. If the required number of barriers in Table 2 cannot be met, layers of protection analysis (LOPA, ISO 31010, B.18) shall be used.

Table 2 — Required number of barriers to demonstrate ALARP

Barriers	**High risk hazards**	**Medium risk hazards with potential fatalities**	**Other medium risk hazards**
Total number of barriers from threat to consequence	5 controls + recovery measures	4 controls + recovery measures	3 controls + recovery measures
Controls (threat)	3 controls to be in place for each identified threat. *Alternative:* 4 controls	2 controls to be in place for each identified threat. *Alternative:* 3 controls	2 controls to be in place for each identified threat
Recovery measures (consequence)	2 recovery measures required for each identified consequence. *Alternative:* 1 recovery measure	2 recovery measures required for each identified consequence. *Alternative:* 1 recovery measure	1 recovery measure required for each identified consequence

In most instances, a barrier only is counted as one. An experienced hazard analyst with experience in using LOPA can give a barrier additional credit based on the LOPA tables. For example, for a protective instrument system that is a SIL 2, which gives a probability of failure on demand between 10^{-2} and 10^{-3}, can be counted as two barriers.

7.2.5 HAZOP

The HAZOP is suitable for identifying hazards associated with deviations from the design intent of the LNG terminal. It draws upon the facility process and instrument diagrams (P&IDs) as the basis of the study and is used more as an audit tool once the design is well understood and minor changes to the system can be incorporated easily. HAZOP is a vertical thought process with only one or two simultaneous failures, whereas HAZID is a lateral thought process which can result from a number of simultaneous failures.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

HAZOPs are used to identify both hazards and operability problems. Although hazard identification is the main focus, operability problems are also identified to the extent that they may have the potential to lead to safety or environmental hazards, or have a negative impact on plant profitability. The HAZOP team involves a group typically consisting of operators, designers, technical specialists (both external and internal to the design team), and maintainers focussing on specific portions of the process called "nodes". These sections are defined from the P&IDs prior to the study. A process parameter is identified, e.g. flow and then typical guidewords are then applied to the specified sections to identify possible deviations (e.g. a guideword "no" is combined with the parameter "flow" to create a deviation, "no flow"). The team then lists all the credible causes of a "no flow" deviation beginning with the cause that can result in the worst possible consequence.

HAZOP is applicable during the basic design (FEED), when P&IDs are issued, as well cause-effect matrix has been produced. It is usually carried out during the detail design as well and may even be reapplied during a management of changes.

The typical outputs of a HAZOP analysis include the following:

— identification of possible deviation states;

— identification of the possible causes for deviation;

— probable worst case scenarios;

— documentation of existing safeguards;

— action required to reduce risk;

— allocation of action to an individual or group.

Figure 7 presents the methodology of a HAZOP workshop.

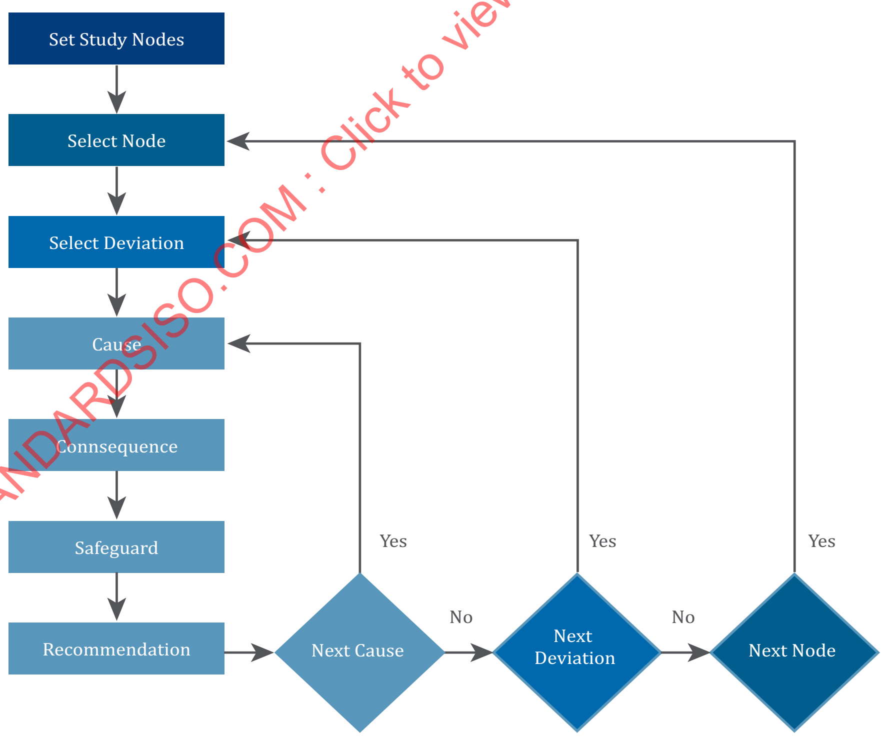

Figure 7 — Process during a HAZOP workshop

Further details are given in ISO 31010, B.6.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

7.2.6 SIL analysis

Safety integrity level (SIL) analysis as described in IEC 61508 complements the HAZOP analysis and the risk assessment study by defining the level of confidence required from the instrumented safety systems including mechanical devices and software, intended to prevent hazardous situations affecting safety of persons and/or the environment or to mitigate their consequences.

IEC 61508 also introduces the notion of safety life cycle that aims to secure the reliability of the implemented safety systems throughout the life of the system.

The SIL assessment should be based on layers of protection analysis (see IEC 61508).

7.3 Quantitative analysis: consequence and impact assessment

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

Quantitative risk analysis requires the use of numerical models. Validated models should be used when available.

7.3.1 Consequence assessment

7.3.1.1 Consequence models

A wide range of computational tools are available to assess the consequences from accidental events comprising both empirical tools and tools developed from the basic physical equations. The burning characteristics depend strongly on the type of fuel (natural gas, LPG) and shall be reflected in the assessment.

The consequence models should be validated by the following:

— taking into account the physical phenomena observed in, and with the data obtained from, available experimental data;

— having been published in an archival, peer-reviewed scientific journal in the related scientific/engineering discipline;

— providing output details of the physics and analysis.

The most important categories are listed below:

	Empirical models	**Models based on solving physical equations**
Liquid spreading and vaporising gas dispersion	Gaussian, plume, and dense gas models	CFD
Fire	Thomas formula, jet fire, or pool fire models	CFD Heat transfer models for fire radiation.
Explosion	A number of commercial packages available, energy correlations	CFD
Structural damage	Engineering tools, Minorsky's energy based correlation for assessment of impact damage	FEM and classical mechanics.

CFD models are gaining acceptance in gas dispersion, fire, and explosion analysis for complex situations. These models offer an accurate representation of the flow mechanics. However, it is important to keep in mind that the quality of the results depends upon model assumptions and inclusiveness of physical/chemical processes more than the number of significant digits or the appearance of the graphical presentations.

© ISO 2015 – All rights reserved

7.3.1.2 Fluid properties

Hazardous material properties used for the calculation should be clearly defined in particular:

— the composition of the release material;

— the thermo-physical properties of the release material;

— the flammability limits of the released material i.e. the proportion of combustible gases in a mixture, between which this mixture is flammable.

For LNG properties, reference is made to EN 1160 or the range of natural gas compositions expected in the plant.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

7.3.1.3 Evaporation of spilled flammable material

The assessment of evaporation of flammable gases from a pool of spilled liquids is based on the following:

— the determination of the pool propagation speed;

— the calculation of the rate of evaporation versus time and, in particular, the maximum evaporation rate.

The factors to be defined are the following:

a) phenomenon of instantaneous vaporisation (flash);

b) nature and temperature of the surface (water, soil, concrete, etc.);

c) ambient conditions (temperature, humidity, wind velocity, stability class).

First evaluation for LNG can be based on evaporation rates. The evaporation rates can be described by theories of the pool spreading and vaporisation models which have been verified with experimental data. These theories are normally imbedded in commercial software tools.

7.3.1.4 Gas dispersion

The assessment of gas dispersion shall determine the zone affected by a cloud extension of flammable material. The extent of the zone is given by the distance from the source to the flammability limit for the gas. Normally, 0.5 LFL is used to account for model uncertainty.

The factors to be defined are the following:

a) Ambient conditions: the ambient conditions are often described by the Pasquill stability classes. The Pasquill method gives a break-down of the amount of atmospheric turbulence present as follows:

   1) A: extremely unstable;

   2) B: moderately unstable;

   3) C: lightly unstable;

   4) D: neutral;

   5) E: lightly stable;

   6) F: moderately stable.

b) Wind speed, direction, and frequency (the wind rose).

c) Relative humidity of the atmosphere.

d) Influence of terrain and obstacles.

Dispersion analysis is normally carried out for selected accident scenarios reflecting local conditions.

© ISO 2015 – All rights reserved

It should be noted that the safety distances as a result of gas dispersion may be different dependent on regional requirements (NFPA 59A and EN 1473).

7.3.1.5 Thermal radiation

The assessment of thermal radiation shall determine the risk due to thermal radiation by calculation of the radiation contours caused by ignition of flammable material from a pool or jet by determination of the radiant heating effects on the exposed targets.

The following factors are to be defined:

a) source configuration (pool dimensions, flame size, and shape, etc.);

b) target configuration versus the radiation source (distance, elevation);

c) target reflectance properties;

d) emissive power of the flammable material;

e) ambient temperature;

f) relative humidity;

g) wind speed, direction, and frequency (the wind rose).

7.3.2 Impact assessment

Impact can be defined as the damage to life, health, or property. Damage can take many forms. Most used are loss of life, irreversible health effects, and loss of money.

According to prescriptive regulations, fixed values are given to which impact to personnel shall be assessed. For example, NFPA recommends 5 kW/m^2 for fire radiation and EN 1473 recommends range of allowable values applicable for areas with different vulnerability (e.g. lower allowable radiation in outside public areas of 1,5 kW/m^2)

For risk-based assessment, impact for personnel has to be evaluated as described in the next sections which give guidance on the impact on human beings and equipment from fire, and explosion. Toxics, in general, do not feature in LNG operations. Main use of the information is guidance for QRA rule sets (which often are referred to as PROBITs).

Fire radiation

The assessment of fire radiation shall determine the radiative heat flux received by different targets (people buildings etc.) in case of fire.

The assessment shall take into account the following:

— position from the source;

— ambient conditions;

— emissivity of the source.

The impact criteria contained in this section relate to the thermal radiation outcome. The physical effects of thermal radiation on humans are most relevant in the immediate vicinity of an incident. The progressive effects resulting are as follows:

— pain;

— first-degree burns;

— second-degree burns;

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

— third-degree burns;

— fatality.

These effects are commonly linked to the intensity of the incident thermal radiation and Table A.1 provides the typical consequences of exposure to various levels of intensity and the expected time to each effect. Values have been approximated to reflect uncertainty in calculation and represent "cautious best estimate" values.

Flash fires

Any people caught in an ignited, dispersing flammable cloud may result in serious injuries or fatalities. In practice, people inside the LFL dispersion cloud zone are assumed to result in causalities.

Explosions

People can survive fairly strong blast waves and in accidents involving explosion there are very few cases in which the blast effect has directly caused fatality. Typical injuries/fatalities following an explosion are caused by burns, flying fragments, buildings, or other structures falling down or being disintegrated and persons falling or "flying" and subsequently hitting a solid object (whole body displacement).

In risk analysis, the most important effects are the following:

— flying fragments hitting personnel;

— whole body displacement resulting in impact damage;

— damage from impact caused by collapsed structures.

7.4 Quantitative analysis: frequency assessment

7.4.1 General

The frequency part of the risk assessment is trying to determine how often things go wrong with the potential to result in damage, injuries, or fatalities. A number of tools are available.

7.4.2 Failure data

Relevant failure data for components exposed to LNG operation is not easily available and there are currently (2013) no publicly available sources for such data.

The relevance of existing failure data is often disputed because the experience does not fully reflect the operational conditions and component design. The lack of relevant data can tempt the assessor to use data that are not applicable to the issue at hand. Typical examples are using general pump leak data for canned pumps or double flushed seal pumps.

However, in spite of the lack of failure data for similar components in similar situations, there are strong arguments for using available failure data as explained below:

— all components shall be fit for purpose;

— design requirements, quality control and maintenance represent the safety net to ensure that the component is "fit for purpose";

— a failure occurs when the control and procedures in place to ensure fit for purpose fails.

Failure data being used in risk assessments should always be referenced and be auditable.

Failure data may be derived from experience database as explained in A.3. These are data gathered all over industry. Based on the number of incidents and the number of equipment items in operation, an incident frequency can be established.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

7.4.3 Consensus data

Consensus data based on discussion and agreement among experienced personnel can be used when no data are available. By interviewing a group of people with relevant experience, meaningful incident frequency data can be developed. However, the methodology can only be used for event frequencies which have an occurrence of at least once every three years to five years. For lower frequencies, the group should be large and it is questionable whether there are that many people at your disposal with the relevant experience.

7.4.4 FAULT tree

A fault tree is an analysis of those events in a process that can result in particular malfunctions or failures, shown in the form of a tree diagram. Fault trees are very useful in simple systems like instrumentation where they are used quite often (see SIL). For complex systems like it is more complicated; e.g. trying to work out the leak frequency of a particular type of tank is riddled with pitfalls. The main problem with fault trees is that it is very difficult to identify all the contributors to the failure and to recognise common mode failures. Errors in both lead in general to a too low a failure frequency. In general, the equipment fails more often than calculated. As they are also very time consuming, their use should not be encouraged.

A fault tree diagram is usually written out using conventional logic gate symbols (“And” and “Or”). The route through a tree between an event and an initiator in the tree is called a cutset. The shortest credible way through the tree from fault to initiating event is called a minimal cutset.

Fault trees can be used to illustrate the contribution from the various part of a system. For example, a fire-fighting system can highlight the contribution from the firewater pumps, deluge valves, and detection. The effectiveness of adding additional detection or fire water pumps can be illustrated using fault trees.

Further fault trees can be used to assess the effects of mitigation measures (redundancy, inspection, maintenance) on failure frequencies of components and systems.

Further details are given in ISO 31010.

7.4.5 Event tree analysis (ETA)

An event tree is a graphical way of showing the possible outcomes of a hazardous event, such as a failure of equipment or hydrocarbon release. An ETA explores the possible outcome of the initial event and determines the resulting frequencies of the different end events which represent different consequences. As such, the event tree is a logical tool to aggregate probabilities and risks.

The branch probabilities determine the distribution of the top events and reflect protective barriers that are enforced to reduce risk. For example, the ignition probability for a hydrocarbon release is lower if the leak has been detected and electrical systems being shut down. And therefore an event tree can be used to assess the efficiency of different mitigating measures by doing comparative studies by variation of the branch probabilities reflecting the different mitigations.

Further description is given in ISO 31010.

7.4.6 Exceedance curves based on probabilistic simulations

The normal approach to risk assessment is to assess the consequences and probabilities for representative accidental scenarios defined by given parameters (e.g. release size, weather and wind conditions, activation of safety systems after a defined delay) resulting in a, because of the limited number of scenarios, few point values. When there are only a few variables this is not a problem. However, when the variables are many like in explosions, then it is difficult to present the results in a meaningful manner.

An alternative approach is to characterise the different parameters as a distribution and use a probabilistic simulation, e.g. by Monte Carlo analysis.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

An example from a Monte Carlo simulation of explosion pressures is shown as an exceedance curve in Figure 8 (exceedance curves are, for example, defined in NORSOK-Z013). The variation in overpressure reflects the variance in important factors:

— size of the releases;

— location of release;

— effects of weather conditions;

— point of ignition.

The results from the simulation are a huge number of frequency/overpressure pairs. These are ordered on overpressure and the frequency plotted versus overpressure as shown in Figure 8.

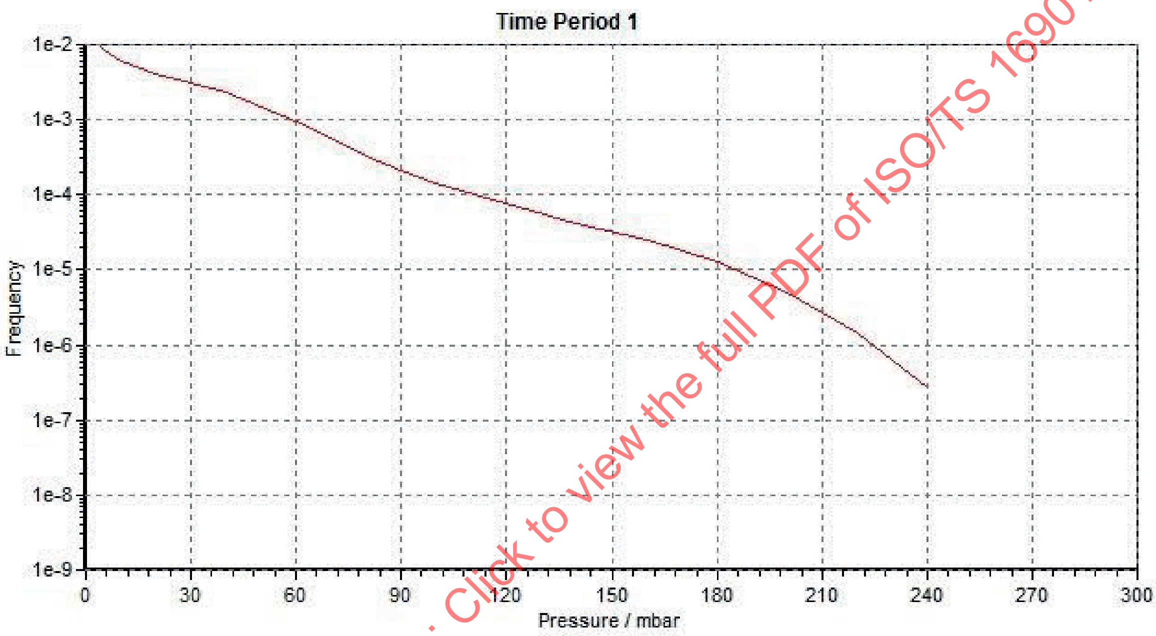

Figure 8 — Sample result of probabilistic explosion modelling

The graph can now be used to estimate how frequently a value is exceeded, e.g. to decide on strength of explosion barriers, buildings, or structures.

7.5 Risk assessments (consequence*frequency)

7.5.1 Risk assessment tools

The aggregation of consequence and frequency into risk can be done simply in a tabular format, but in most cases, a computerised model is used to handle the large number of risk contributors.

Note that the outputs from these risk assessment tools shall be verified, whether by hand calculations, benchmarks, and other test bet verifications.

These risk assessment tools fall generally into two groups: ad hoc developed and proprietary.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

7.5.2 Ad hoc developed risk assessment tools

Ad hoc QRA models are usually based on modelling with multi-layer spreadsheets. These multiple sheets typically contain the following:

— a count of the number and type of components in the plant;

— a table of failure rate data for each component size and type;

— a table of consequence distance (i.e. distance from hazard source at which fatality or injury potentially occurs) for each type and size of failure;

— a sheet with a wind rose with time-based delimitations relevant to vapour cloud dispersion directions;

— a table of occupancy numbers and percentage exposure values for occupied areas of the site.

By multiplying these elements together and summing the results on an area basis, the risk of a fatality in a grid of plant areas can be determined.

Advantages of the spreadsheet method

The calculation methods and steps can be traced from step to step so that the internal working of the model can be reviewed and understood at any given time.

Modifications to the spreadsheet logic can be easily achieved by a skilled risk practitioner.

As the model is transparent, inspection of the model shows quickly the events that contribute most of the risk and whether these “higher risks” are due to the number of hazard sources, the frequency of release the “fatality distances” that the hazards have, and the numbers of people exposed to the risk. The visibility of these factors allows judgement to be applied in how to reduce risk levels if they are too high.

Disadvantages of the spreadsheet method

It requires a QRA Engineer with considerable knowledge of QRA methodology and significant spreadsheet programming ability to build the model.

The models are often large and complex and difficult to check properly.

The control of changes to the model is difficult without a rigorous check and approval procedure.

The maintenance of spreadsheet models can be difficult as original authors move on if the spreadsheet is not fully documented.

Developers of spreadsheet models often prefer not to have integrated consequence models to avoid excessive complexity and often use a curve fit from a range of results from other consequence modelling programs. A change in a plant parameter may need a new set of consequence curves need to be built which is time consuming.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

7.5.3 Proprietary risk assessment tools

Proprietary models have been developed by companies often to assist them with their own consultancy work and subsequently made available to the industry. They are usually the fruits of years of research and have been subject to thorough checking of their modelling methods and internal calculation methods.

They are usually subject to updates by the software support team.

Advantages of proprietary models

Some models include failure rate data based on the company’s own failure rate data base. This can be an advantage as failure rate data have always been difficult to obtain.

Other programs provide a framework in which the user can place their own failure rate data.

© ISO 2015 – All rights reserved

Proprietary risk assessment models often sit above a proprietary consequence modelling program which is often available in its own right. This makes the software sensitive to changes in the design and these can be incorporated quickly.

Disadvantages of proprietary models

The model is a "black box". If it behaves in an unusual or unpredictable way, it is usually difficult to understand what is going on inside the "box".

Some changes can come about as the underlying consequence modelling "engine" moves from one calculation algorithm to another as parameters vary. This characteristic gives the user no support if challenged by a customer over the output from the program or a change in the output as a result of a parameter changing slightly.

8 Accident scenarios

8.1 Overview accident scenarios

Identification of accident scenarios are an essential part of any risk assessment.

The accident scenarios that are studied in a risk assessment are generally identified as part of a hazard identification session.

This clause presents typical accident scenarios that should be considered and that could have an impact on the design and layout of the installation.

The scenarios result in the release of flammable material for which the consequences to be analysed have already been mentioned in 7.3.

Typical scenarios for LNG facilities comprising release of all types of hydrocarbons (including refrigerants and natural gas liquids) and other scenarios that should be considered for detailed assessment are listed in 8.2. There are the general scenarios that apply to all hydrocarbons containing equipment. These have been supplemented with scenarios that are LNG specific and might be overlooked by personnel without in-depth familiarity with LNG plants.

Other accident scenarios that should be considered for export terminals are presented in 8.3.

The development of the accident scenarios for hydrocarbon releases including escalation are shown in 8.4. Possible domino effects should be addressed not only within the terminal but also the impact on the surroundings and impact of the surrounding facilities on the terminal.

In general, QRA are designed to model the operation of the facilities. However, simultaneous operation, major construction/maintenance in or near process areas in operation should be part of the risk assessment.

Security assessment, e.g. vulnerability to terrorist attack, are not considered here and should be the subject of a specific study.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

8.2 LNG import facilities including SIMOPS

Typical possible accidental releases of flammable material for LNG import terminal are listed in Table 3 including the possible source of release scenario and examples of the initiating event.

© ISO 2015 – All rights reserved

Table 3 — Typical accident scenarios for LNG import facilities (1 of 2)

Source of release	Scenario	Possible causes
General process and cargo handling	Accidental release from equipment and piping	Flange tightness
		Defective gasket
		Weld defects
		Corrosion
		Impact
		Supporting structure damage
		External fire
		Overpressure (e.g. pressure tests during commission)
		Embrittlement
		Earthquake
		Other natural hazards
Accidental release from LNG carrier tanks at jetty [a]	Ship collision	Passing ship adrift
	Ship pressure relief valve	Overpressure
		Rollover
Jetty	Damage to piping	Ship colliding with jetty or trestle
	Loading arms leak/rupture	Ship movement, ERC/PERC failure
		List (loss of ballast)
		Extreme weather
		Line failures
		Swivel joint failure
		Pressure surge during transfer
		External fire
		Earthquake
	RPT LNG spills	Spill of LNG into water

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

Table 3 — Typical accident scenarios for LNG import facilities (2 of 2)

Source of release	Scenario	Possible causes
Storage	Tank roof collapse	Tank overfilling
		Tank overpressure
		Rollover
		Flying object
	Tank	Fire damage
	Tank leakage	Dropped in tank pump
		Internal/external leak tank bottom/wall
		Earthquake
	Tank PSV release	Tank overfilling
		Tank overpressure
		Rollover
	BLEVE	Fire impact on pressurized hydrocarbon containers.
	Tank leakage from N_2 tanks	Internal/external leak tank bottom/wall
		Earthquake
	Leaks from tank piping/manifolds	See general
Process	Recondenser leak/rupture	Overpressure
	S&T exchangers/ plate fin exchangers leak/rupture	Pipe rupture
		Overpressure
		Defective gasket
	LNG vaporisers leak/rupture (incl. intermediate fluid: propane, methanol)	Pipe rupture
		Overpressure
	Pipe rupture	Overpressure (LP/HP boundary)
		Pressure surge during unloading
		Pressure surge LP/HP send-out lines
		Cold breakthrough (vaporisers)
		Overpressure export gas line
	Rotating equipment/disk rupture	Surge control
Utilities	Flare and or vent release	Plant upset
LNG trucking	Releases during transfer	Rupture of transfer hoses or piping. Operational errors

[a] Hazards related to ship approach and manoeuvre into the harbour are assumed to be addressed in a specific study.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

8.3 LNG export facilities

Typical possible accidental releases of flammable material for LNG export terminal are given in Table 4 where the possible source of release scenario and the initiating event are also listed.

Table 4 — Typical accident scenarios for LNG export facilities (1 of 2)

Source of release	Scenario	Possible causes
General applicable to all parts of the facilities	Accidental release from equipment and piping	Flange tightness
		Defective gasket
		Weld defects
		Corrosion
		Impact
		Supporting structure damage
		External fire
		Overpressure (e.g. pressure tests during commission)
		Embrittlement
		Earthquake
		Other natural hazards
Slug catcher and receiving	Escalation from fires	Ignited leaks
Conditioning	Spillage of fat solvent	See general
	Pressurized liquid spills in fractionation	See general
Liquefaction	BLEVE of refrigerant	External fire
Storage	BLEVE of refrigerants	External fire
	Tank roof collapses	Tank overfilling
		Tank overpressure
		Rollover
		Flying object
	Tank leakage	Dropped in tank pump
		Internal/external leak tank bottom/wall
		Earthquake
	Tank PSV release	Tank overfilling
		Tank overpressure
		Rollover

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

Table 4 — Typical accident scenarios for LNG export facilities (2 of 2)

Source of release	Scenario	Possible causes
Jetty	Damage to piping	Ship colliding with jetty or trestle
	Loading arms leak/rupture	Ship movement, ERC/PERC failure
		List (loss of ballast)
		Extreme weather
		Line failures
		Swivel joint failure
		Pressure surge during transfer
		External fire
		Earthquake
	RPT LNG spills	Spill of LNG into water
Utilities	Hot oil fires	See general

8.4 Chain of events following release scenarios

The development of the accident scenarios for hydrocarbon releases, including escalation, is illustrated in Figure 9 to Figure 13. The illustrations are informative. For actual installations, installed equipment, operational plans, and safeguards should be reflected.

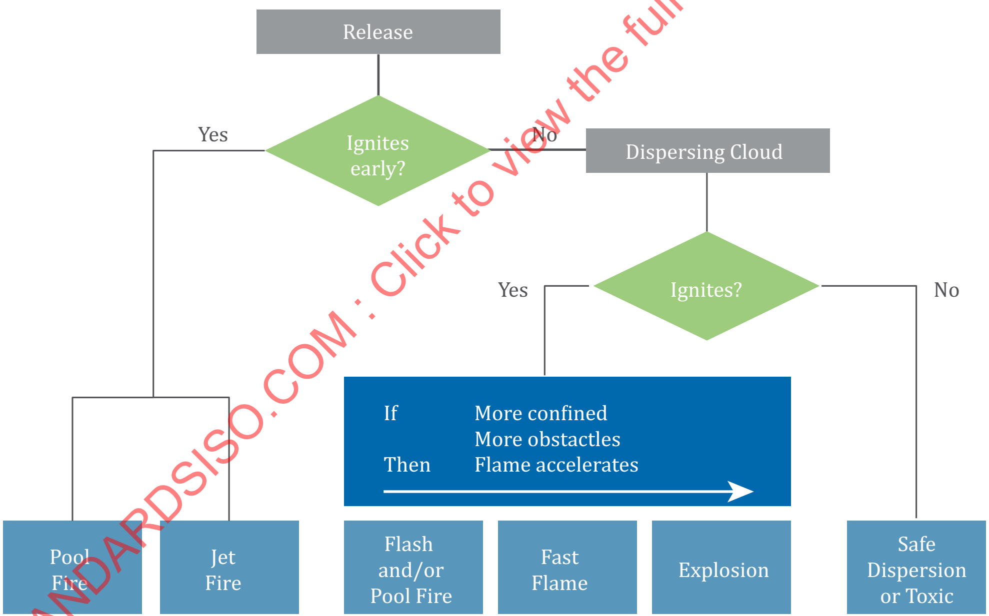

Figure 9 — Possible outcomes of a flammable release

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

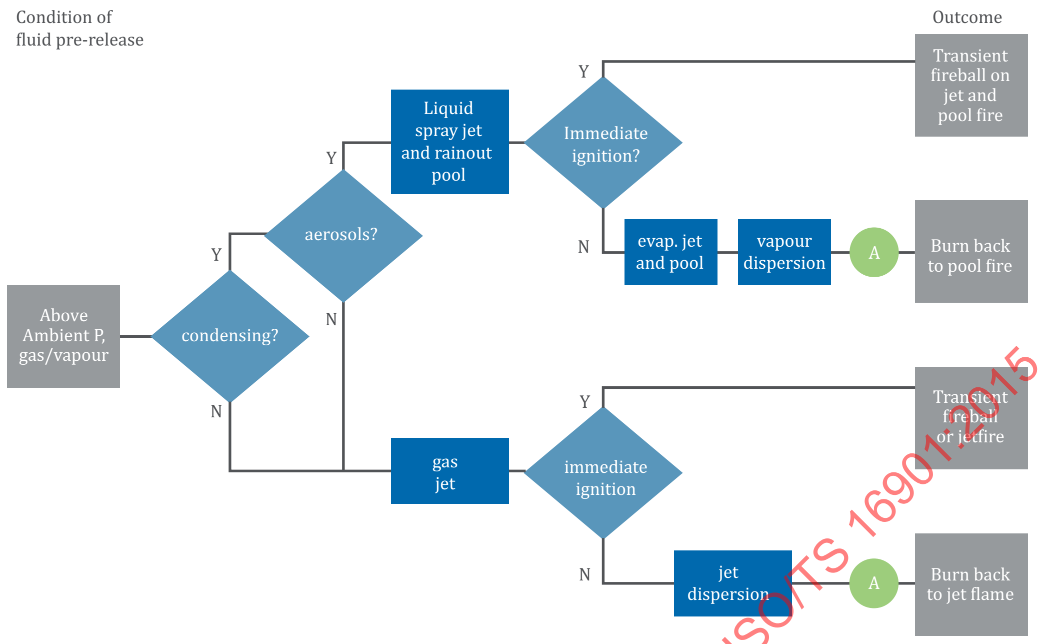

Figure 10 — Outcomes from pressurized vapour releases

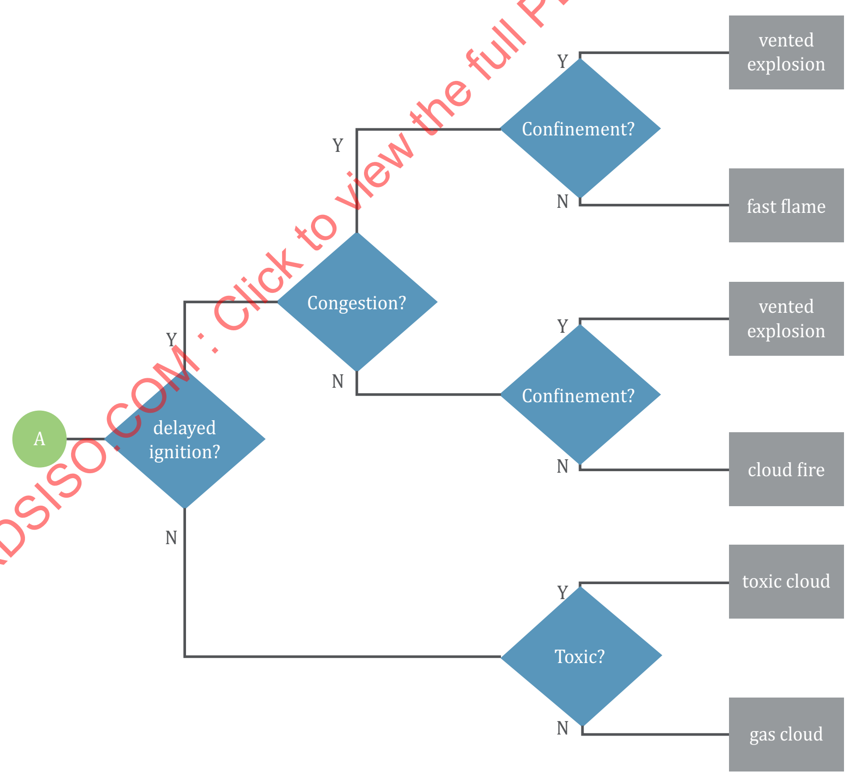

Figure 11 — Continuation of event chain of Figure 10, Figure 12, and Figure 13

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

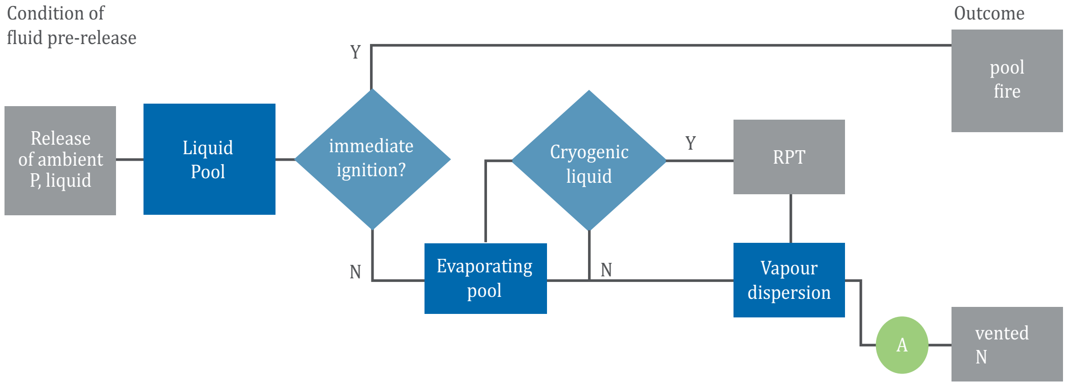

Figure 12 — Outcomes from atmospheric vapour releases

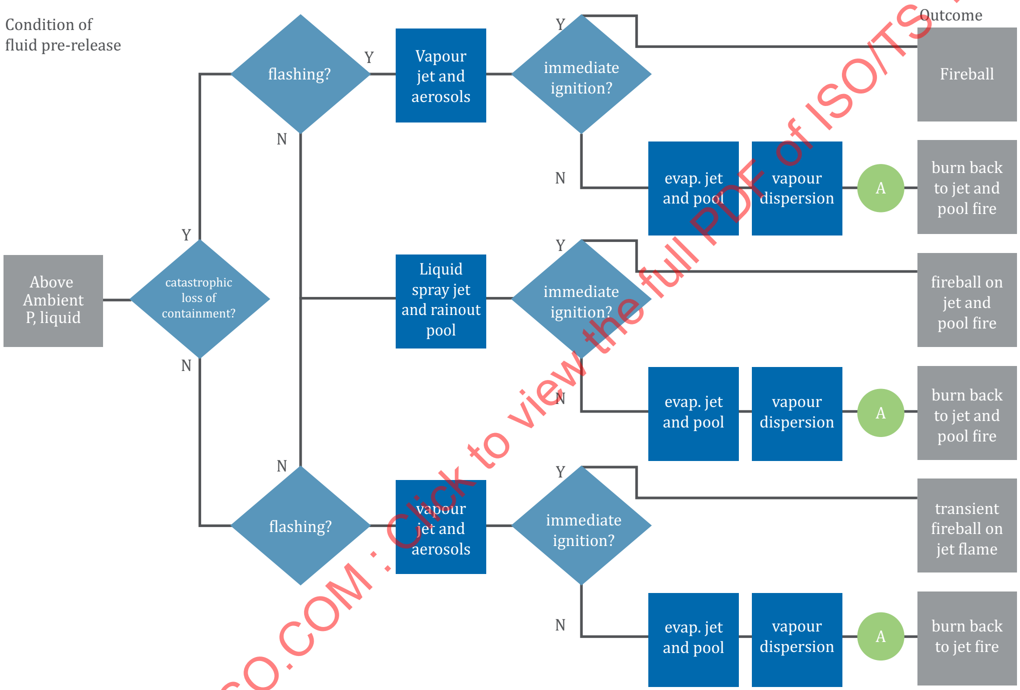

Figure 13 — Outcomes from pressurized liquid releases

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

9 Standard presentation of risk

Risk assessments are being used to support decisions. It is therefore essential that the results from a QRA are presented to ensure the following:

— The risk picture including compliance/noncompliance with acceptance criteria is communicated to and understood by decision makers and other stakeholders.

— That risk-reducing measures and recommendations are clearly presented and understood by decision makers.

— That methodology, assumptions, and data are described in sufficient detail to enable traceability and possible modifications. The study shall be auditable and traceable.

— This requires that the results are presented and communicated in a consistent way reflecting acceptance criteria and legislation, project decision criteria, and company philosophies.

© ISO 2015 – All rights reserved

The minimum content of a QRA report is outlined by the following table of contents:

1. Executive summary
2. Description
3. Study methodology
4. Hazard/Top event ID
5. Flammable and toxic release scenarios
6. Other hazards
   i. Transport
   ii. Structural
7. Risk presentation
8. Sensitivity studies
9. Results and Discussion
10. Conclusions and Recommendations
11. Appendices
    i. System layout
    ii. Assumptions register
    iii. Frequency data
    iv. Consequence modelling results
    v. Action follow-up register

The documentation of input data, model assumptions, and selection of models should enable verification and modifications, such that the results can be reconstructed.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

Annex A
(informative)

Impact criteria

A.1 Accident impact criteria

A.1.1 Thermal radiation

Table A.1 presents the effects of thermal radiation on humans and structures.

Table A.1 — Effects of thermal radiation (Ref: UK HID SPC/Tech/OSD30)

Thermal radiation kW/m^2	**Effect on humans**	**Effect on structures**
1,2	Received from the sun at noon in summer.	
2	Minimum to cause pain after 1 min.	
<5	Will cause pain in 15 s to 20 s and injury after 30 s exposure.	
>6	Pain within approximately 10 s rapid escape only is possible.	
12,5	Significant chance of fatality for medium duration exposure.	Thin steel with insulation on the side away from the fire may reach thermal stress level high enough to cause structural failure.
25	Likely fatality for extended exposure and significant chance of fatality for instantaneous exposure.	Spontaneous ignition of wood after long exposure. Unprotected steel will reach thermal stress temperatures that can cause failure.
35	Significant chance of fatality for people exposed instantaneously.	Cellulosic material will pilot ignite within one minute exposure. Concrete walls will spall.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

A.1.2 Overpressure

People can survive fairly strong blast waves and in accidents involving explosion, there are very few cases in which the blast effect has directly caused fatality. Typical injuries/fatalities following an explosion are caused by burns, flying fragments, buildings, or other structures falling down or being disintegrated and persons falling or “flying” and subsequently hitting a solid object (whole body displacement). In risk analysis, the most important effects are the following:

— flying fragments hitting personnel;

— whole body displacement resulting in impact damage;

— damage from impact caused by collapsed structures

Data for explosion effects on personnel for use in QRAs are given in Ref /14/ (OGP Report 434-14.1 Risk Assessment Data Directory, March 2010) and Ref /15/ [HSE UK, 2010 SPC/Tech/OSD/30, rev 2013—Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment. (http://www.hse.gov.uk/)]

 © ISO 2015 – All rights reserved

A.2 Simple risk calculations

Simple risk calculations are often useful to support decisions, particularly in the early stages of a development when the information required to do a full QRA do not exist. An example of such calculations is given below:

The event tree in Figure A.2 is an element of a single risk analysis. It develops the risk at an occupied target location 100 metres from a single release scenario on the plant.

The intent is to illustrate a possible calculation mechanism that can be used. All the figures are fictional.

The example can be expanded to include other release and hazard scenarios and other target distances and directions and other atmospheric conditions as shown in Figure A.1.

These can then be aggregated to produce levels of risk overlaid on a geographic mesh around the plant.

A risk contour plot can be produced from the mesh of risk values.

When an event tree model such as Figure A.2 is used, the maximum values that dominate aggregates risk levels at particular points can be identified. This allows mitigation measures to be beneficially focused on particular hazards.

Further information and similar event trees are given in ISO 31010.

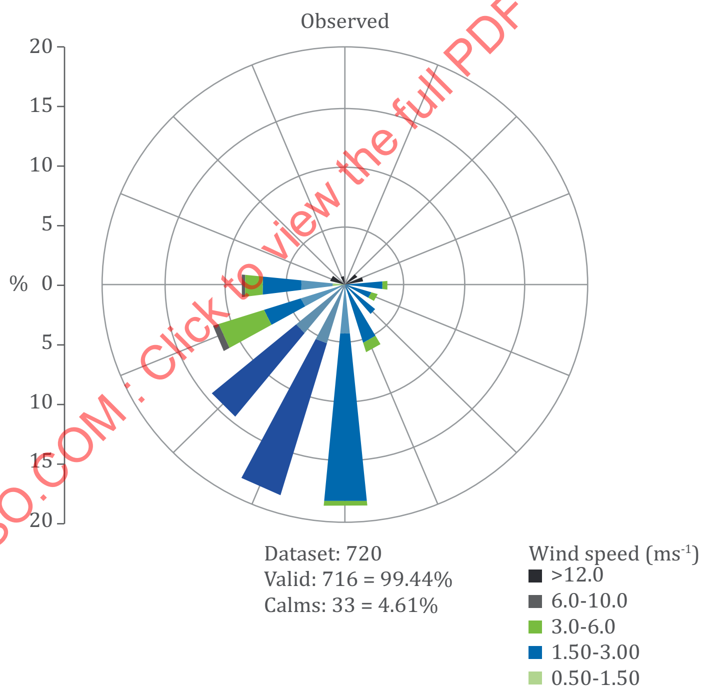

Figure A.1 — Wind rose for simple risk assessment

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

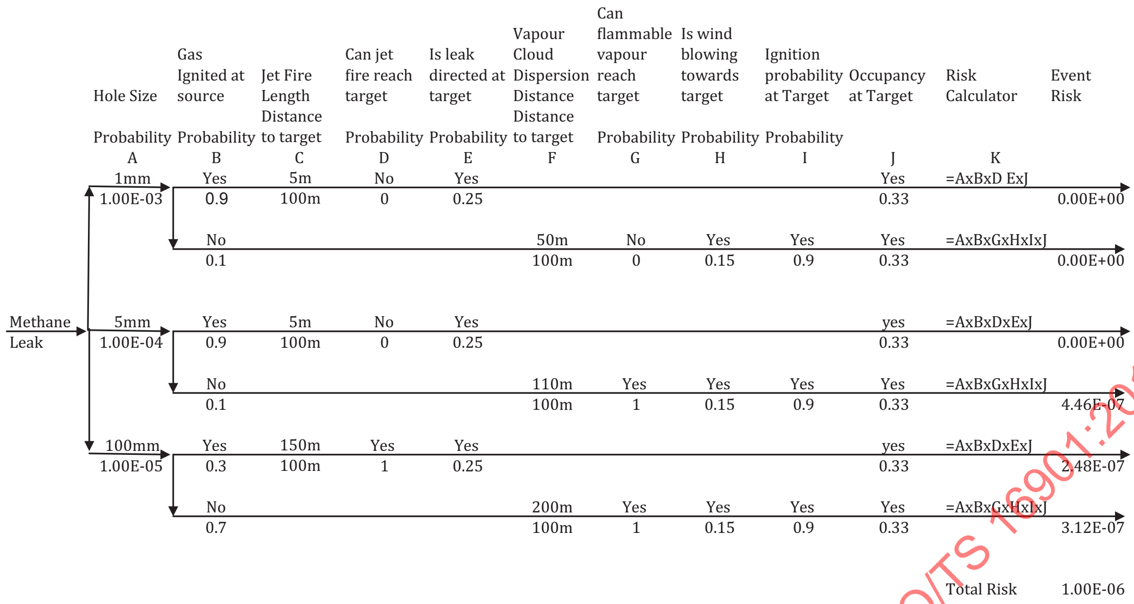

Figure A.2 — Sample event tree for a simple risk assessment

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

A.3 Failure data

The frequency at which failures can occur in a system or equipment item is usually modelled through an exponential failure distribution that can be defined by a unique parameter, called failure rate, that is constant over time. In that case, the failure rate, noted λ, is linked with the mean time to failure (MTTF) of equipment items with the following relationship:

$$MTTF = 1 / \lambda$$

The failure rate is usually given "per year", but other units may also be encountered (ex: "per hour").

How to derive the information within an incident database into failure rates or MTTF is another issue all together as often the confidence of probabilistic failure calculations depends heavily upon the dependability of good failure data. One should use the best available data to estimate the equipment or systems failure and therefore should have data from a large panel of sources in order to ensure the most appropriate data are used. Additionally, a thorough understanding of how information is presented in the incident database is an important factor for obtaining dependable results.

Derivations of incident data into failure rates can include the following:

— a listing of failure modes whose criticality may be broken down into incident groups;

— the cause of failure may also be available and should be listed;

— the observed number of failures for each failure mode is calculated;

— the total population of the equipment item or system and the number of facilities it appears on;

— the total time in service of the equipment item or system in terms of calendar time, operational time, and the total number of demands;

— the uncertainty range of the failure rates of each failure mode;

 © ISO 2015 – All rights reserved

— the mean time to failure (MTTF) estimate;

— the mean time to repair (MTTR) estimate.

Doing this, a number of factors should be taken into account. For instance, reflecting the clean service of a system should incorporate modifying the failure rate to remove the downtime (associated with equipment failures) of certain failure modes. The population should also be taken into account to ensure an adequate range of data are analysed.

Ideally, the equipment failure frequency is estimated using data that has been collected from similar equipment that has been exposed to similar conditions – process, environment, maintenance, etc. In practice, this will usually not be possible. Differences in the history of equipment may limit the applicability of the generic data. In practice, a judgment should be made trading-off the availability and applicability of generic data.

However, when possible and additional resources can be assigned, it is often preferred to determine failure rate data using techniques such as a failure, modes, effects, and criticality analysis (FMECA) especially for novel or improved systems or equipment.

A FMECA study normally takes a group of operational personnel and steps through a system assessing individual equipment items as to the types of failure modes and the overall effect of failure on production. Apart from important reliability data in terms of MTTFs and MTTRs of equipment items, information on the criticality of equipment is determined (i.e. if this valve fails, will it fail safe? Will it cause an impact on production?).

Some references for failure rate data of equipment items are listed below:

— OREDA: Contains data for use in reliability, availability, and maintainability studies - failure rates, failure mode distribution, and repair times for equipment (Reference: OREDA, Offshore Reliability Data Handbook 4th Edition, SINTEF, 2002);

— Reliability Data for Control and Safety Systems, 1998, SINTEF Industrial Management, Trondheim, Norway;

— CCPS Process Equipment Reliability Database. The database is only open to CCPS members but some data are available in the book Guidelines for Process Equipment Reliability Data (CCPS 1989). Guidelines for Process Equipment Reliability Data, CCPS, 1989;

— FMD-97, Failure mode / Mechanism Distributions, 1997, Reliability Analysis Center, Rome, NY;

— NPRD-95, Nonelectronic Parts Reliability Data, 1995, Reliability Analysis Center, Rome, NY;

— IEEE Std. 500, IEEE Guide To The Collection and Presentation Of Electrical, Electronic, Sensing Component, And Mechanical Equipment Reliability Data For Nuclear-Power Generating Stations, 1984, IEEE, New York, NY;

— Johnson, E.M. and Welker, J. R., “Development of an Improved LNG Plant Failure Rate Data Base”, GRI-80/0093, Gas Research Institute, Chicago, IL, USA, 1980.

Some sources of data specific to LNG equipment items exist (cf. last item above) but they are of a limited practical use in a risk assessment. Therefore, the main information mostly comes from the oil and gas industry and the chemical industry.

Failure data also include leak frequency data, which allows to estimate the probability of leaks of various sizes on pipes and equipment items (e.g. valves, pumps). These data can be derived from incident databases or expert judgment as well.

Some references for leak frequency data are listed below:

— Hydrocarbon Releases (HCR) Database, UK Health and Safety Executive, with the following associated documents:

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

- Offshore hydrocarbon releases statistics and analysis, 2002, HID statistics report, HSR 2002 002, February 2003, HSE;
- Revised guidance on reporting of offshore hydrocarbon releases, OTO 96 956, November 1996, HSE;
- Supplementary Guidance for Reporting Hydrocarbon Releases, September 2002, UKOOA;
- UK HSE failure data: "Failure Rate and Event Data for use within Risk Assessments, (28/06/2012)";
- Handleiding Risicoberekeningen BEVI, 3.0 RIVM;
- E&P Forum Hydrocarbon Leak Database (Reference: Quantitative risk assessment datasheet directory, E&P Forum Report N0 11.8/250, October 1996);
- Lees "Loss Prevention in the Process Industry". Loss Prevention in the Process Industry, Frank P Lees, 2nd edition, 1996, ISBN 0750615478 (Note 3rd edition published 2005);
- COVO Study. Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area, Rijnmond Public Authority, 1982;
- Cox Lees & Ang, Classification of Hazardous Locations, 1990.

It should be noted that there are no publicly available incident databases for LNG plants that can be available to derive leak frequencies and therefore should rely on the above more general data.

A.4 List of hazards to be considered (reflecting experience data)

General HAZID checklist as in Table A.2 can be found in many sources, e.g. ISO 17776, Annex B.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

Table A.2 — HAZID checklist external and environmental hazards

External and environmental hazards		
Hazard type	**Guideword**	**Expanders**
Natural hazards	Extreme weather	Temperature extremes
		Waves
		Wind
		Dust
		Flooding
		Sandstorms
		Ice
		Snow
		Blizzards
		Fog
		Fast atmospheric pressure changes
	Lightning	
	Climate change	
	Seismic activity	Earthquake
		Soil liquefaction
	Erosion	Ground slide
		Coastal erosion
		Riverbank erosion
	Subsidence	Ground structure
		Foundations
		Settlement
External and third-party hazards	Third party activities	Farming
		Fishing
		Local industry
	Helicopter/Aircraft crash	
	Ship collision	
	Operator	
Human error	Maintenance	
	Inspection	

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

Table A.3 — HAZID checklist, facility hazards

Facility hazards		
Hazard type	**Guideword**	**Expanders**
Process hazards	Process releases (LNG) — unignited	Gas clouds
		Cryogenic spills
		Gas detection
		Emergency response
	Ignited process releases (natural gas)	Fire
		Explosion
		Heat
		Smoke
		Fire detection
		Emergency response
	Ignited process releases (LPG, refrigerants, and other hydrocarbons with different burning characteristics than natural gas)	BLEVE
		Fire
		Explosion
		Heat
		Smoke
		Fire detection
		Emergency response
	Process releases — toxic	Toxic gas detection
		Emergency response
	Flaring	Heat
		Ignition source
		Location
	Venting	Discharge to atmosphere
		Location
		Dispersion
	Draining	
	Sampling	Operator error
Accommodation and non-process area hazards	Non process fires	Control rooms
		Accommodation
	Smoke ingress	Ingress to safe areas
		HVAC shutdown
	Gas ingress	Ingress to safe areas
		HVAC shutdown
	Stacking and storage	

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

Table A.4 — HAZID checklist, health hazards

Health hazards		
Hazard type	**Guideword**	**Expanders**
Health hazard	Disease hazards	Endemic diseases
		Infection
		Contaminated water/food
		Social, e.g. HIV
Working environment	Physical	Drinking water
		Lighting
		Noise
	Temperature	Extreme hot/cold
		Ventilation
		Guarding
		Cold burns
	Atmospheres	Exhaust fumes
		Confined spaces
NOTE Hazards specific to LNG facilities not addressed in general checklists.		

Table A.5 — HAZID checklist additional LNG and LPG hazards

LNG and LPG hazards		
Hazard type	**Guideword**	**Expanders**
Process Hazard	Storage	Roll-over
	Temperature	Metal embrittlement
		Temperature shock
		High thermal strain gradient
Shipping	Transfer	RPT

A.5 Risk assessment with respect to earthquake

In international LNG plant design codes, two concepts of earthquake design criteria are used. These are the following:

— OBE, operating basis earth-quake. This is the maximum earthquake for which no damage is sustained and restart and safe operation can continue after examination of the plant.

— SSE, safe shutdown earthquake. This is the maximum earthquake event for which the essential fail-safe functions and mechanisms are designed to be preserved. Permanent damage can be expected of this lower probability event, but without loss of overall integrity and containment. The installation will not remain in continuous service without a detailed examination and structural assessment at the ultimate limit state.

When a plant is not designed to the relevant national earthquake requirements incorporating OBE and SSE principles, it may be necessary to include risk arising from earthquake in the risk evaluation.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

A.6 Safety management

A.6.1 General

The risk assessment of any facility is based on the assumption that the plant is operated and maintained in a systematic way by qualified personnel.

As a consequence, a fundamental assumption for the risk assessment is that procedures and programs for training, maintenance, and operation exist and are implemented. This subclause addresses the basic recommendations.

During engineering and construction, safety should be continuously scrutinised to guarantee the appropriate safety level with regard to the hazard assessment.

The safety management, after design and construction, should include design considerations and continuous reviews. Thus, QRA represents a tool to provide identification, priorities, and guidance to develop operational documents and instructions concerning risk management.

For that reason, preparation for plant operation should tackle the following points:

— development of plant operation, maintenance, and inspection procedures (operational procedures);

— personnel training;

— development of safety procedures, which integrate with the overall port emergency procedures [and international ship and port facilities security (ISPS) code, where relevant].

The Code of Practice for LNG Facilities from the Nova Scotia Department of Energy, as well as safety management system (SMS) for gas transmission infrastructure and pipeline integrity management system (PIMS) for gas transmission pipelines from the European Committee for Standardization (CEN), may be referred to.

A.6.2 Operational procedures

After operations and activities associated with hazards are identified, the implementation of documented procedures is necessary to manage the risks and to cover situations where their absence can lead to hazardous situations.

In addition, it is advisable to implement and maintain some controls, such as:

— operational controls, as applicable to the organization and its activities;

— controls related to purchased goods, equipment, and services;

— controls related to contractors and other visitors to the workplace.

The safety management system (SMS) should include documents to ensure the effective planning, operation and control of processes that relate to the management of its OH&S (occupational health and safety) risks (proportional to the level of complexity, hazards and risks concerned, and kept to the minimum required for effectiveness and efficiency).

Regarding the safety control system, it should be designed and operated in accordance with requirements of IEC 61508 or IEC 61511. SIL requirements should be studied and evaluated to be consistent with the required plant safety level.

The ESD signal processor should be SIL 2 or better.

A.6.3 Maintenance procedures

Each LNG terminal operator should have written maintenance procedures based on experience, knowledge of similar facilities, and conditions under which the facilities will be maintained.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

 © ISO 2015 – All rights reserved

Each LNG terminal operator should prepare a written manual that sets out an inspection and maintenance program for each component that is used in the facility.

The maintenance manual for facility components should include the following:

— The manner of carrying out, and the frequency, of the inspections and tests on every component and its support system in service in the facility, to verify that the component is maintained in accordance with the equipment manufacturer recommendations, and in accordance with IEC 61508 for what concerns safety integrity levels.

— A description of any action that is necessary to maintain the facility in safe conditions.

— All procedures to be followed during repairs on operating components while they are being repaired, to ensure safety of people a property at the facility.

Each facility operator should conduct the maintenance program in accordance with the written manual for facility components.

A.6.4 Training

The plant should be operated in a safe efficient manner compliant with national health and safety legislation.

Operating practices and procedures should be compliant with the requirements of the major accident prevention policy and the safety management system.

It should be ensured that any person developing tasks that can impact on health and safety is competent on the basis of appropriate education, training, or experience.

Training needs should be identified in order to provide training or take other actions to meet these needs and evaluate the effectiveness of the training or action taken. Specifically, people engaged in any of the terminal activities should be trained in the hazards and properties of LNG with particular attention to emergency response procedures.

Operation and maintenance staff should be trained in all aspects of their work to ensure that they can work in a safe and competent manner under both normal and emergency condition. Initial training should take into account the background of the individual. Re-training should be undertaken at regular intervals and all records of training be kept.

For management and staff training, schemes should be structured according to the individual experience, duties, and responsibilities within the organisation and should be independently validated.

All people visiting a site for whatever purpose should be instructed in the hazards and properties of LNG; the depth to which this training is undertaken should be appropriate to the level of involvement in site operations.

A.6.5 Emergency for worst case scenarios

The terminal operator is obliged by legislation to take all necessary measures to prevent major accidents and to limit their consequences for people and the environment.

It should be required that the operator draws up a document setting out his major-accident prevention policy and ensures that it is properly implemented. The major-accident prevention policy established by the operator should be designed to guarantee a high level of protection for people and the environment by appropriate means, structures, and management systems.

Prior to starting operation, it should be ensured that the operator draws up an internal emergency plan, including the measures to be taken inside the establishment, to supply to the competent authorities the necessary information to enable them to draw up external emergency plans.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

© ISO 2015 – All rights reserved

The emergency plans shall be established with the objectives of:

— containing and controlling incidents so as to minimize the effects, and to limit damage to people, the environment and property;

— implementing the measures necessary to protect people and the environment from the effects of major accidents;

— communicating the necessary information to the public and to the services or authorities concerned in the area;

— providing for the restoration and clean-up of the environment following a major accident.

A.7 National regulations

National regulations, when available, should be prevailing and decide the framework for project development. This annex (informative) gives basic principles criteria and/or main requirement that are of application for risk assessment studies in varied countries of the world, based on the versions available at the time this framework has been written (2011).

The reported information does not pretend to be exhaustive and only aims at illustrating with examples different requirements in definition of safety philosophy and risk criteria. **The examples listed below are not to be reproduced/considered in an actual project.** For an actual project, the full details of the current regulation should be adopted.

Tables A.6 to A.14 give some information from some regulations, listed in alphabetical order.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 16901:2015

Table A.6 — Regulations in Australia (1 of 2)

Australia New South Wales	Risk-based
ID/Reference	New South Wales Department of Planning
Risk contour for land use planning	Hospitals, schools, child care, and elderly care facilities should be outside the 5×10^{-7}/yr contour Residential developments including hotels and tourist resorts should be outside the 10^{-6}/yr contour. Commercial developments, offices, warehouses, and restaurants should be outside the 5×10^{-6}/yr contour. Sporting complexes and active open areas should be outside the 10^{-5}/yr contour. Industrial sites neighbouring hazardous sites should be outside the 5×10^{-5}/yr contour.
Societal	
Other	
Comments	

© ISO 2015 – All rights reserved