Guide for Risk Analysis

Effective from 15 March 2016

Emirates Classification Society (Tasneef)
Aldar HQ 19th Floor,
Al Raha Beach, Abu Dhabi, UAE
Abu Dhabi, United Arab Emirates

Phone (+971) 2 692 2333
Fax (+971) 2 445 433
P.O. Box. 111155
info@tasneef.ae

GENERAL CONDITIONS

Definitions:

"*Administration*" means the Government of the State whose flag the Ship is entitled to fly or under whose authority the Ship is authorized to operate in the specific case.

"IACS" means the International Association of Classification Societies.

"*Interested Party*" means the party, other than the Society, having an interest in or responsibility for the Ship, product, plant or system subject to classification or certification (such as the owner of the Ship and his representatives, the ship builder, the engine builder or the supplier of parts to be tested) who requests the Services or on whose behalf the Services are requested.

"*Owner*" means the registered owner, the ship owner, the manager or any other party with the responsibility, legally or contractually, to keep the ship seaworthy or in service, having particular regard to the provisions relating to the maintenance of class laid down in Part A, Chapter 2 of the Rules for the Classification of Ships or in the corresponding rules indicated in the specific Rules.

"Rules" in these General Conditions means the documents below issued by the Society:

(i) Rules for the Classification of Ships or other special units;

(ii) Complementary Rules containing the requirements for product, plant, system and other certification or containing the requirements for the assignment of additional class notations;

(iii) Rules for the application of statutory rules, containing the rules to perform the duties delegated by Administrations;

(iv) Guides to carry out particular activities connected with Services;

(v) Any other technical document, as for example rule variations or interpretations.

"*Services*" means the activities described in Article 1 below, rendered by the Society upon request made by or on behalf of the Interested Party.

"Ship" means ships, boats, craft and other special units, as for example offshore structures, floating units and underwater craft.

"*Society*" or *"TASNEEF"* means Tasneef and/or all the companies in the Tasneef Group which provide the Services.

"*Surveyor*" means technical staff acting on behalf of the Society in performing the Services.

Article 1

1.1. The purpose of the Society is, among others, the classification and certification of ships and the certification of their parts and components. In particular, the Society:

(i) sets forth and develops Rules;

(ii) publishes the Register of Ships;

(iii) issues certificates, statements and reports based on its survey activities.

1.2. The Society also takes part in the implementation of national and international rules and standards as delegated by various Governments.

1.3. The Society carries out technical assistance activities on request and provides special services outside the scope of classification, which are regulated by these general conditions, unless expressly excluded in the particular contract.

Article 2

2.1. The Rules developed by the Society reflect the level of its technical knowledge at the time they are published. Therefore, the Society, although committed also through its research and development services to continuous updating of the Rules, does not guarantee the Rules meet state-of-the-art science and technology at the time of publication or that they meet the Society's or others' subsequent technical developments.

2.2. The Interested Party is required to know the Rules on the basis of which the Services are provided. With particular reference to Classification Services, special attention is to be given to the Rules concerning class suspension, withdrawal and reinstatement. In case of doubt or inaccuracy, the Interested Party is to promptly contact the Society for clarification.
The Rules for Classification of Ships are published on the Society's website: www.tasneef.ae.

2.3. The Society exercises due care and skill:

(i) in the selection of its Surveyors

(ii) in the performance of its Services, taking into account the level of its technical knowledge at the time the Services are performed.

2.4. Surveys conducted by the Society include, but are not limited to, visual inspection and non-destructive testing. Unless otherwise required, surveys are conducted through sampling techniques and do not consist of comprehensive verification or monitoring of the Ship or of the items subject to certification. The surveys and checks made by the Society on board ship do not necessarily require the constant and continuous presence of the Surveyor. The Society may also commission laboratory testing, underwater inspection and other checks carried out by and under the responsibility of qualified service suppliers. Survey practices and procedures are selected by the Society based on its experience and knowledge and according to generally accepted technical standards in the sector.

Article 3

3.1. The class assigned to a Ship, like the reports, statements, certificates or any other document or information issued by the Society, reflects the opinion of the Society concerning compliance, at the time the Service is provided, of the Ship or product subject to certification, with the applicable Rules (given the intended use and within the relevant time frame).
The Society is under no obligation to make statements or provide information about elements or facts which are not part of the specific scope of the Service requested by the Interested Party or on its behalf.

3.2. No report, statement, notation on a plan, review, Certificate of Classification, document or information issued or given as part of the Services provided by the Society shall have any legal effect or implication other than a representation that, on the basis of the checks made by the Society, the Ship, structure, materials, equipment, machinery or any other item covered by such document or information meet the Rules. Any such document is issued solely for the use of the Society, its committees and clients or other duly authorised bodies and for no other purpose. Therefore, the Society cannot be held liable for any act made or document issued by other parties on the basis of the statements or information given by the Society. The validity, application, meaning and interpretation of a Certificate of Classification, or any other document or information issued by the Society in connection with its Services, is governed by the Rules of the Society, which is the sole subject entitled to make such interpretation. Any disagreement on technical matters between the Interested Party and the Surveyor in the carrying out of his functions shall be raised in writing as soon as possible with the Society, which will settle any divergence of opinion or dispute.

3.3. The classification of a Ship, or the issuance of a certificate or other document connected with classification or certificate on and in general with the performance of Services by the Society shall have the validity conferred upon it by the Rules of the Society at the time of the assignment of class or issuance of the certificate; in no case shall it amount to a statement or warranty of seaworthiness, structural integrity, quality or fitness for a particular purpose or service of any Ship, structure, material, equipment or machinery inspected or tested by the Society.

3.4. Any document issued by the Society in relation to its activities reflects the condition of the Ship or the subject of certification or other activity at the time of the check.

3.5. The Rules, surveys and activities performed by the Society, reports, certificates and other documents issued by the Society are in no way intended to replace the duties and responsibilities of other parties such as Governments, designers, ship builders, manufacturers, repairers, suppliers, contractors or sub-contractors, Owners, operators, charterers, underwriters, sellers or intended buyers of a Ship or other product or system surveyed.

These documents and activities do not relieve such parties from any fulfilment, warranty, responsibility, duty or obligation (also of a contractual nature) expressed or implied or in any case incumbent on them, nor do they confer on such parties any right, claim or cause of action against the Society. With particular regard to the duties of the ship Owner, the Services undertaken by the Society do not relieve the Owner of his duty to ensure proper maintenance of the Ship and ensure seaworthiness at all times. Likewise, the Rules, surveys performed, reports, certificates and other documents issued by the Society are intended neither to guarantee the buyers of the Ship, its components or any other surveyed or certified item, nor to relieve the seller of the duties arising out of the law or the contract, regarding the quality, commercial value or characteristics of the item which is the subject of transaction.

In no case, therefore, shall the Society assume the obligations incumbent upon the above-mentioned parties, even when it is consulted in connection with matters not covered by its Rules or other documents.

In consideration of the above, the Interested Party undertakes to relieve and hold harmless the Society from any third party claim, as well as from any liability in relation to the latter concerning the Services rendered.

Insofar as they are not expressly provided for in these General Conditions, the duties and responsibilities of the Owner and Interested Parties with respect to the services rendered by the Society are described in the Rules applicable to the specific Service rendered.

Article 4

4.1. Any request for the Society's Services shall be submitted in writing and signed by or on behalf of the Interested Party. Such a request will be considered irrevocable as soon as received by the Society and shall entail acceptance by the applicant of all relevant requirements of the Rules, including these General Conditions. Upon acceptance of the written request by the Society, a contract between the Society and the Interested Party is entered into, which is regulated by the present General Conditions.

4.2. In consideration of the Services rendered by the Society, the Interested Party and the person requesting the service shall be jointly liable for the payment of the relevant fees, even if the service is not concluded for any cause not pertaining to the Society. In the latter case, the Society shall not be held liable for non-fulfilment or partial fulfilment of the Services requested. In the event of late payment, interest at the legal current rate increased by 1.5% may be demanded.

4.3. The contract for the classification of a Ship or for other Services may be terminated and any certificates revoked at the request of one of the parties, subject to at least 30 days' notice to be given in writing. Failure to pay, even in part, the fees due for Services carried out by the Society will entitle the Society to immediately terminate the contract and suspend the Services.

For every termination of the contract, the fees for the activities performed until the time of the termination shall be owed to the Society as well as the expenses incurred in view of activities already programmed; this is without prejudice to the right to compensation due to the Society as a consequence of the termination.

With particular reference to Ship classification and certification, unless decided otherwise by the Society, termination of the contract implies that the assignment of class to a Ship is withheld or, if already assigned, that it is suspended or withdrawn; any statutory certificates issued by the Society will be withdrawn in those cases where provided for by agreements between the Society and the flag State.

Article 5

5.1. In providing the Services, as well as other correlated information or advice, the Society, its Surveyors, servants or agents operate with due diligence for the proper execution of the activity. However, considering the nature of the activities performed (see art. 2.4), it is not possible to guarantee absolute accuracy, correctness and completeness of any information or advice supplied. Express and implied warranties are specifically disclaimed.

Therefore, except as provided for in paragraph 5.2 below, and also in the case of activities carried out by delegation of Governments, neither the Society nor any of its Surveyors will be liable for any loss, damage or expense of whatever nature sustained by any person, in tort or in contract, derived from carrying out the Services.

5.2. Notwithstanding the provisions in paragraph 5.1 above, should any user of the Society's Services prove that he has suffered a loss or damage due to any negligent act or omission of the Society, its Surveyors, servants or agents, then the Society will pay compensation to such person for his proved loss, up to, but not exceeding, five times the amount of the fees charged for the specific services, information or opinions from which the loss or damage derives or, if no fee has been charged, a maximum of AED5,000 (Arab Emirates Dirhams Five Thousand only). Where the fees charged are related to a number of Services, the amount of the fees will be apportioned for the purpose of the calculation of the maximum compensation, by reference to the estimated time involved in the performance of the Service from which the damage or loss derives. Any liability for indirect or consequential loss, damage or expense is specifically excluded. In any case, irrespective of the amount of the fees charged, the maximum damages payable by the Society will not be more than AED5,000,000 (Arab Emirates Dirhams Five Millions only). Payment of compensation under this paragraph will not entail any admission of responsibility and/or liability by the Society and will be made without prejudice to the disclaimer clause contained in paragraph 5.1 above.

5.3. Any claim for loss or damage of whatever nature by virtue of the provisions set forth herein shall be made to the Society in writing, within the shorter of the following periods: (i) THREE (3) MONTHS from the date on which the Services were performed, or (ii) THREE (3) MONTHS from the date on which the damage was discovered. Failure to comply with the above deadline will constitute an absolute bar to the pursuit of such a claim against the Society.

Article 6

6.1. These General Conditions shall be governed by and construed in accordance with United Arab Emirates (UAE) law, and any dispute arising from or in connection with the Rules or with the Services of the Society, including any issues concerning responsibility, liability or limitations of liability of the Society, shall be determined in accordance with UAE law. The courts of the Dubai International Financial Centre (DIFC) shall have exclusive jurisdiction in relation to any claim or dispute which may arise out of or in connection with the Rules or with the Services of the Society.

6.2. However,

(i) In cases where neither the claim nor any counterclaim exceeds the sum of AED300,000 (Arab Emirates Dirhams Three Hundred Thousand) the dispute shall be referred to the jurisdiction of the DIFC Small Claims Tribunal; and

(ii) for disputes concerning non-payment of the fees and/or expenses due to the Society for services, the Society shall have the right to submit any claim to the jurisdiction of the Courts of the place where the registered or operating office of the Interested Party or of the applicant who requested the Service is located.

In the case of actions taken against the Society by a third party before a public Court, the Society shall also have the right to summon the Interested Party or the subject who requested the Service before that Court, in order to be relieved and held harmless according to art. 3.5 above.

Article 7

7.1. All plans, specifications, documents and information provided by, issued by, or made known to the Society, in connection with the performance of its Services, will be treated as confidential and will not be made available to any other party other than the Owner without authorization of the Interested Party, except as provided for or required by any applicable international, European or domestic legislation, Charter or other IACS resolutions, or order from a competent authority. Information about the status and validity of class and statutory certificates, including transfers, changes, suspensions, withdrawals of class, recommendations/conditions of class, operating conditions or restrictions issued against classed ships and other related information, as may be required, may be published on the website or released by other means, without the prior consent of the Interested Party.
Information about the status and validity of other certificates and statements may also be published on the website or released by other means, without the prior consent of the Interested Party.

7.2. Notwithstanding the general duty of confidentiality owed by the Society to its clients in clause 7.1 above, the Society's clients hereby accept that the Society may participate in the IACS Early Warning System which requires each Classification Society to provide other involved Classification Societies with relevant technical information on serious hull structural and engineering systems failures, as defined in the IACS Early Warning System (but not including any drawings relating to the ship which may be the specific property of another party), to enable such useful information to be shared and used to facilitate the proper working of the IACS Early Warning System. The Society will provide its clients with written details of such information sent to the involved Classification Societies.

7.3. In the event of transfer of class, addition of a second class or withdrawal from a double/dual class, the Interested Party undertakes to provide or to permit the Society to provide the other Classification Society with all building plans and drawings, certificates, documents and information relevant to the classed unit, including its history file, as the other Classification Society may require for the purpose of classification in compliance with the applicable legislation and relative IACS Procedure. It is the Owner's duty to ensure that, whenever required, the consent of the builder is obtained with regard to the provision of plans and drawings to the new Society, either by way of appropriate stipulation in the building contract or by other agreement.
In the event that the ownership of the ship, product or system subject to certification is transferred to a new subject, the latter shall have the right to access all pertinent drawings, specifications, documents or information issued by the Society or which has come to the knowledge of the Society while carrying out its Services, even if related to a period prior to transfer of ownership.

Article 8

8.1. Should any part of these General Conditions be declared invalid, this will not affect the validity of the remaining provisions.

INDEX

1 GENERAL AND APPLICATION

Risk assessment is a tool that can be used to demonstrate that a proposed design achieves an equivalent safety level to a standard design (when safety rules apply), or that the risks of the design has been made ALARP (if no applicable rules are available, due to the novelty of the design).

This guide applies to risk analysis of industrial system.

2 RISK ASSESSMENT PROCESS

2.1 GENERAL

2.1.1

This item covers the basics of the risk assessment approach. For its very nature, there is no unique methodology to be applied in any context. Every case has to be evaluated separately and the most cost-effective approach has to be selected. In particular, once decided the acceptance criteria, the appropriate scoping of the work and the level of detail are instrumental to the success of the activity: the proper way to proceed must take into account factors like the magnitude of the risks involved, the uncertainties, and the complexity of the problem. Further guidance can be found in the “Guidelines for alternative design and arrangements for fire safety”, IMO MSC/Circ. 1002, and “Guidelines for alternative design and arrangements for SOLAS Chapters II-1 and III”, IMO MSC/Circ. 1212.

2.2 MAIN APPROACHES

2.2.1

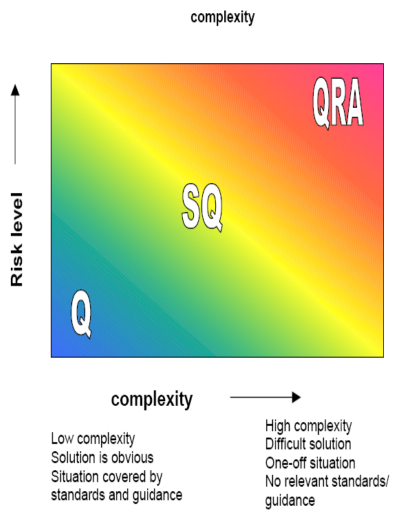
All or some of the following stages of the risk assessment activity may be followed:

- Qualitative, where frequency and severity are estimated according to attributes expressing quality or kind (e.g. high, low, medium etc.)
- Semi-quantitative, where frequency and severity are estimated approximately within numerical ranges
- Quantitative, where full quantification of frequencies and consequences is carried out.

The three approaches require an increasing order of detail, complexity, resources and background information/data to be retrieved. In turn, the choice of the depth of the analysis depends on the design phase. A broad, qualitative risk assessment should be carried out at the initial design stages: it is possible that the design under study is characterized by a low level of novelty, or represents a simple alternative to a certain prescription. In such cases, a simple qualitative method like FMECA, HAZOP, What-if (detailed in the following sections) may be adequate to compare the risks of the new versus traditional design, and may be apt to suggest alternatives for risk reduction. As the design progresses, becomes more complex and shows multi-faceted aspects, the need of more in-depth and accurate assessments may arise.

Figure 1: Proportionate risk assessment

Figure 2: Alternative description of the approach to risk assessment as a function of risk level and complexity



2.3 RISK RANKING

2.3.1

If a qualitative or semi-qualitative risk assessment technique is employed, the results are to be presented and ranked according to a risk matrix: in fully quantitative studies, the results are numeric and their ranking is manifest. No standard risk matrix can be defined because it has to be set up according to the specific study, but it is important that it is capable of discriminating between the risks of the different hazardous events, but on the other hand an excessive number of categories would make the matrix difficult to handle.

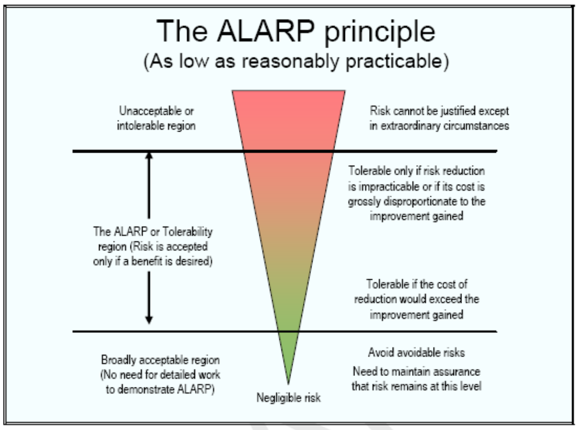
Table 1: Example of risk matrix

Likelihood	Severity levels			
	1 Insignificant	**2 Marginal**	**3 Critical**	**4 Catastrophic**
5: Frequent	Undesirable	Intolerable	Intolerable	Intolerable
4: Probable	Tolerable	Undesirable	Intolerable	Intolerable
3: Occasional	Tolerable	Undesirable	Undesirable	Intolerable
2: Remote	Negligible	Tolerable	Undesirable	Undesirable
1: Improbable	Negligible	Negligible	Tolerable	Tolerable

2.3.2 ALARP Principle

ALARP principle is that the residual risk, due to the hazard, is to be "as low as reasonably practicable". The ALARP risk region is to be defined within the risk matrix.
The ALARP concept is illustrated in the following Fig 3.

Figure 3



2.3.3 Severity classification

Severity is an assessment of the significance of the hazard effects.
The classification of the severity effects is highly dependent on the HAZID application and is developed in consideration of several factors such as:

- the nature of the system in relation to possible effects on users or the environment resulting from hazard
- the functional performance of the system
- any contractual requirements imposed by the customer
- government or industry safety requirements.

The following table illustrates an example of severity classification:

Table 2: Example of severity classification

Class	Severity Level	Consequence to person, property or environment
IV	Catastrophic	A Hazard which could potentially result in the failure of the system's primary functions and therefore causes serious damage to the system and its environment and/or personal injury
III	Critical	A Hazard which could potentially result in the failure of the system's primary functions and therefore causes considerable damage to the system and its environment, but which does not constitute a serious threat to life or injury
II	Marginal	A Hazard, which could potentially degrade system performance function(s) without appreciable damage to system or threat to life or injury
I	Insignificant	A Hazard which could potentially degrade the system's functions but will cause no damage to the system and does not constitute a threat to life or injury

2.3.4 Organization of Risk Assessment

Whatever the scope, the approach and the level of detail, a risk assessment requires multi-disciplinary expertise. When a company undertakes a risk assessment, common practice requires a team to be established to follow the risk assessment process through to completion. In turn, the company may perform the whole activity in-house or outsource some particular tasks to external specialists. The actual organization depends very much on the problem under study, but it is suggested that Tasneef be early involved in the process: this would be beneficial to streamline the subsequent process of review and feedback that is required for the classification of new or alternative designs.

Any risk assessment is expected to go through the following basic steps:

a) Preliminary phase – identification of the applicable normative aspects, the goals (alternative or novel design), the equivalency criteria, the acceptance criteria and the scope of work

b) Collection of background information – retrieval of the necessary documentation (e.g. drawings, technical specifications, operating/test/maintenance procedures, properties of materials involved, etc.) and of the field experience on comparable situations from experienced personnel (lessons learnt, practical issues, operating requirements, etc.)

c) Conducting the HAZID – collecting the analysis team with the necessary multidisciplinary knowledge and the team leaders (usually, a qualified facilitator and a scribe), preparing the worksheets (in paper and /or electronic form), organizing the meeting, evaluating the results against the acceptance criteria, considering the recommendations, determining the need of more sophisticated tools, documenting the study

Conducting more detailed studies (if required) – scoping the activities, collecting the team(s), deciding the tools to be employed, performing the assessment(s), evaluating the results against the acceptance criteria, considering the recommendations, documenting the study.

d) Rank the risks and collect the recommendations for risk reduction to be followed up in the design and/or in the operating lifecycle.

The success of a study requires:

- management support
- necessary expertise in the various topics addressed
- availability of adequate and up-to-date information
- tools to perform the various steps of the studies
- definition of the level of resolution necessary and sufficient for the problem.

1 GENERAL

This section summarizes the most commonly used hazard evaluation techniques. Depending on the purpose and scope of the assessment, they may provide sufficient conclusions in terms of risk prioritization, or may provide intermediate results that constitute proper inputs to more sophisticated analyses like QRA.

2 HAZARD IDENTIFICATION (HAZID) TECHNIQUE

HAZID is a general term used to describe an activity with the purpose to identify hazards and associated events that have the potential to significantly affect personnel (e.g., injuries and fatalities), environment (oil spills and pollution) and financial assets (e.g., production loss/delay). The HAZID technique can be applied to technical systems (e.g. all or part of a facility or vessel), operational procedures or even project management. There is no standard HAZID methodology, and the techniques will depend on the characteristics of the problem under study. Typically, a multidisciplinary team (whose composition and size are proportional to the extent and complexity of the issues to be analyzed) will conduct a brainstorming meeting through the following tasks.

a) Basic Information
During this part, background information about the system to be analysed is given, mainly how the subject under consideration (system, function, operation) works is explained.

b) Hazard Identification
A complex problem is normally subdivided into functions, subsystems, operations, etc. as far as applicable, and a fixed amount of time for discussions for each of these areas should be assigned a priori. Hazard identification may be carried out through brainstorming or by means of more structured techniques such as What-If, HAZOP, FMECA, etc.

c) Ranking
During this part of the meeting, frequency and consequence estimates are elicited from the team members, based on an established scale of frequency and consequence indexes. The risks associated to every hazard are then ranked accordingly.

3 WHAT-IF ANALYSIS

3.1 GENERAL

What-if analysis is a brainstorming examination normally used for a process or operation, but is flexible enough to be employed in other fields of application. The brainstorming is carried out by a team of experts (of appropriate expertise and number). Each member is then encouraged to address questions that, typically, begin with 'What-if? to which the team is supposed to find an answer in terms of potential consequences, available safeguards and recommendations for preventing problems. Or, the questions can be divided into specific areas of investigation, to be subsequently addressed by the appropriate specialists.

For example:

- What if the crew leaves the door open?
- What if the operator opens valve B instead of valve A?
- What if a given mistake is made?
- What if a certain piece of equipment fails?

The method can also be enhanced by the use of pre-determined checklists based on past experience, constituted by written lists of items that help to identify known types of hazards, design deficiencies, and potential accident situations associated with the system, equipment or operation.

3.2 CHARACTERISTICS

The What-If Analysis method is a flexible technique, not as structured as other techniques (i.e. FMECA, HAZOP), which allows easy adaptations to specific applications. It is a powerful method if the team members are experienced, and it is useful to give a first assessment of hazards. It is heavily reliant on the experience of the team members carrying out the review and therefore the results are prone to be incomplete depending on the experience of the team members. Also, there is no assurance that the questions asked are sufficient in either breadth (coverage) or depth (detail) to identify all the hazards.

3.3 TYPES OF RESULTS

The What-if Analysis technique generates a list of questions and answers about the problem. It may also produce a tabular listing of hazardous situations, their consequences, safeguards, and possible recommendations for risk reduction. It is possible to associate a qualitative risk estimate to each question.

Table 1: What-if Evaluation Example

What if …?	Immediate System Condition	Ultimate Consequences	Safeguards	Risk Ranking (Consequence, Likelihood)	Recommendations
Loss of level signal from process vessel level transmitter	Process vessel level rises uncontrollably	Oil flows into gas outlet to flare allowing oil to escape from top of flare	Regular checking of vessel gauge glass	High Risk (Consequence: High, Likelihood: Medium)	Separate independent level switches in vessel to activate shut down of process

4 CHECKLIST ANALYSIS

4.1 GENERAL

Checklist analysis uses a written list of items or procedural steps to verify the status of a system or a procedure. Traditionally, checklists are mainly used to ensure that organizations are complying with standard practices, and to provide a framework for interviews, reviews and inspections. Checklists should be developed by authors with various background and experience relevant to the context to be analyzed.

Checklist analysis is frequently used in conjunction with another method (especially what-if analysis) to address specific requirements.

4.2 CHARACTERISTICS

A checklist analysis is based on experience and knowledge of the rules, codes and standards applicable to the system or operation under study. The approach is easy to use and flexible enough to be employed at any stage of a design or operation, and can be extended as necessary to satisfy the specific situation. On the other hand, it relies heavily on the degree of expertise injected therein.

4.3 TYPES OF RESULTS

In the HAZID application, the analysts, assisted by the necessary skilled personnel, defines standard design or operating practice, then uses them to generate a list of questions based on deficiencies or differences. The technique generates qualitative lists of ‘yes’, ‘no’, ‘not applicable’ or ‘needs more information’ answers to each question, highlighting the hazards as deviations (non-conformities) from the standard. A qualitative estimation of the risk can be associated to each deviation.

5 HAZARD AND OPERABILITY (HAZOP) ANALYSIS

5.1 GENERAL

The HAZOP technique originates from the chemical industry and it is best suited to identify safety hazards and operability problems of continuous process systems (especially fluid and thermal systems) or sequential procedures or operations.

5.2 CHARACTERISTICS

The HAZOP analysis focuses on specific points of the system or operation (e.g., process sections, operating steps etc.). One at a time, a multidisciplinary team examines each section or step for potentially hazardous process deviations that are derived from a set of established guide words. Guide words are simple words (e.g. no, more, less, as well as, reverse, etc.) that, coupled with a series of significant process parameter defined up front, highlight a possible deviation, as in the following example:

Guide word		Parameter		Deviation
NO	+	FLOW	=	NO FLOW
MORE	+	PRESSURE	=	EXCESSIVE PRESSURE

While it is possible to have more deviations of the same parameter (e.g. ‘no flow’, ‘reverse flow’), there are also meaningless combinations (e.g. ‘as well as’ coupled with ‘pressure’) that the team has to discard during the process.

The group is then called to identify potential causes of these deviations (including human errors) and the appropriate safeguards to help prevent the causes from occurring.

5.3 TYPES OF RESULTS

The HAZOP Analysis technique produces a tabular listing of hazardous situations (i.e., the deviations identified by the team), their consequences, safeguards, and possible recommendations for risk reduction. A qualitative risk estimate can be associated to each deviation.

Table 2: Checklist Analysis Example

Questions	Responses	Risk Ranking (Consequence, Likelihood)	Recommendations
Instrumentation Are separate independent level switches provided in vessel to activate shut down of process? • • •	*Instrumentation* Yes, to enhance reliability of safeguard • • •	*Instrumentation* Medium Risk (Consequence: High, Likelihood: Low) • • •	*Instrumentation* — • • •

Table 3: Example of a HAZOP Analysis

Item	Deviation	Causes	Consequences	Safeguards	Risk Ranking (Consequence, Likelihood)	Recommendations
More+Level	Process vessel level rises uncontrollably	Failure of control system	Oil flows into gas outlet to flare allowing oil to escape from top of flare	Regular checking of vessel gauge glass	High Risk (Consequence: High, Likelihood: Medium)	Separate independent level switches in vessel to activate shut down of process

Table 4: FMECA Evaluation Example

Failure mode	Causes	Local Effects	End Effects	Indications/ Safeguards	Risk Ranking	Recommendations /remarks
Failure of level switch	Internal faults	Oil flows into gas outlet to flare allowing oil to escape from top of flare	Process vessel level rises uncontrollably	Regular checking of vessel gauge glass	High Risk (Consequence: High, Likelihood: Medium)	Separate independent level switches in vessel to activate shut down of process

6 FAILURE MODES AND EFFECTS AND CRITICALITY ANALYSIS (FMECA)

6.1 GENERAL

The primary objective of FMECA is to provide a comprehensive, systematic and documented investigation which establishes the most significant failure conditions of the installation systems, and assesses their significance. FMECA is based on a single failure concept, under which each considered system at various levels of a system's functional hierarchy is assumed to fail by one realistic cause at a time (including human errors). The postulated failures are analyzed and classified according to the severity of their local effect (i.e. impact on a specific equipment or subsystem under study) and end effect (i.e. impact on the system function, taking into account the effects on the whole installation). Such effects may include secondary failures (or multiple failures) at other level(s).

6.2 CHARACTERISTICS

Generally, FMECA is used for reviews of mechanical and electrical hardware systems. It requires multi-disciplinary knowledge of typical failure modes of the components of equipment or systems. In FMECA, each individual failure is considered as an independent occurrence, with no relation to other failures in the system, except for the subsequent effects that it might produce (cascade effects). This technique can be applied to well-defined systems, and is not appropriate to more general issues such overall vessel safety, or to accident scenarios involving chain of multiple events.

6.3 TYPES OF RESULTS

The FMECA technique produces a tabular listing of items to which the team associates its failure modes, their consequences (local and end effects), safeguards, and possible recommendations for risk reduction. A qualitative risk estimate can be associated to each failure mode.

7 FAULT TREE ANALYSIS (FTA)

7.1 GENERAL

A fault tree is a graphical model that illustrates combinations of events (usually failures) that will cause one specific failure of interest, denominated ‘Top Event’. Fault Tree analysis (FTA) is a deductive technique that uses Boolean logic symbols like AND, OR, NOT etc. to break down the causes of a Top Event into basic equipment/subsystem failures, human errors and special conditions (called ‘basic events’). The analyst starts with an undesirable event (failure, accident scenario etc.) that is to be avoided and identifies the immediate causes of that event (including human errors). In turn, each of the immediate causes is further examined in the same way until the basic causes are identified, at the appropriate level of detail according to the scope of the analysis. The resulting fault tree model displays the logical relationships between basic events and the Top Event.

A HAZID technique like those described in the previous sections normally generates a list of hazardous situations, each of which can constitute a Top event and can be studied by FTA to obtain the list of necessary and sufficient combination of its causes (denominated ‘minimal cut sets’ or MCS).

7.2 CHARACTERISTICS

This methodology can also be applied to many types of applications, but is most effectively used to analyze system failures caused by relatively complex combinations of events. For example, the verification that a system is single-failure-proof, where the combinations of multiple failure events are not of interest, does not require a FTA, an FMECA being generally sufficient (but the use of FTA is not precluded).

The resources required by FTA are heavily dependent on various aspects:

- number of top events to be studied
- complexity of the systems
- physical system boundaries
- level of detail of the failure events
- logic boundary conditions (not allowed events, equipment configurations etc.).

An FTA requires a level of basic information and expertise superior to the coarser HAZID techniques.

Since a fault tree tends to become rapidly complex as the level of detail increases, enhancing the difficulties of the minimization of the cut sets, ad-hoc commercial software tools are normally required to conduct an FTA except for very simple cases.

7.3 TYPES OF RESULTS

FTA produces a graphical representation of the fault tree, with a list of minimal cut sets having probability and/or number of events higher than a cut-off defined by the analyst, an evaluation of the significance of every cut set and the probability/frequency of the top event (in case the analysis is quantitative, otherwise, the fault tree can be used in logical form). The single point failures (i.e., MCS of order 1) are to be highlighted and recommendations should be given for their reduction.

8 EVENT TREE ANALYSIS (ETA)

8.1 GENERAL

Event tree analysis (ETA) evaluates the potential for an accident that is the result of a general type of an initiating event (e.g., equipment failure, accident scenario etc.). Unlike FTA (a deductive reasoning process), ETA is an inductive reasoning process where the analyst begins with the initiating event and develops the possible sequences of events that lead to potential accidents, accounting for both the successes and the failures of any associated safety functions as the accident escalates, usually denominated ‘nodes’ of the event tree. Each node is characterized by at least two outcomes (success and failure), but it is possible to have more according to the type of function that is described. A node may represent the success or failure of operators’ interventions other than safety systems.

8.2 CHARACTERISTICS

ETA is suited for analyzing initiating events that could result in a variety of outcomes. An event tree emphasizes the initial cause of potential accidents and works from the initiating event to the final effects. Each branch of the event tree represents a separate accident sequence. ETA may be used to analyze almost any sequence of events, but is most effectively used to address possible outcomes of initiating events for which multiple safeguards are in line as protective features. However, since the event tree is a static representation of phenomena in series, the model of the sequences must be consistent with the time order of the succession of the nodes. If the intervention of two or more functions, described by the nodes, is competitive in time, the sequence of the nodes cannot be uniquely defined. In this case, the event tree may become inadequate.

8.3 TYPES OF RESULTS

ETA produces a number of sequences, and each sequence can be analysed in the same way of fault trees to determine their minimal cut sets. Each accident sequence represents a logical 'AND' of the initiating event and subsequent occurrences (successes of failures of the nodes). Thus, each sequence can be thought of as a separate fault tree with the accident sequence as the Top event, followed by an AND gate containing the initiating event and all the events representing the status of safety systems. The main difference with respect to the fault tree is that usually fault trees are 'coherent' (i.e., containing only AND and OR gates and failure events), whilst event trees must contain sequences of successes and failures of each node: this allows defining fully consistent separate sequences. Normally, the quantification takes place by assigning a frequency to the initiating event, and a probability to the nodes: this way, each sequence is characterized by a frequency. It is commonplace to construct and quantify complex event trees by software suites that often can build also fault trees: it is also possible to quantify the probability of failure of each node by means of a dedicated fault tree and quantify each sequence as a combination of the fault trees representing the node failures ('fault tree linking' technique). The result of ETA is a graphical representation of the event tree, with the list of sequences and their associated frequency (in case the analysis is quantitative, otherwise, the event tree can be used in logical form).

Figure 1: Example Fault Tree Analysis

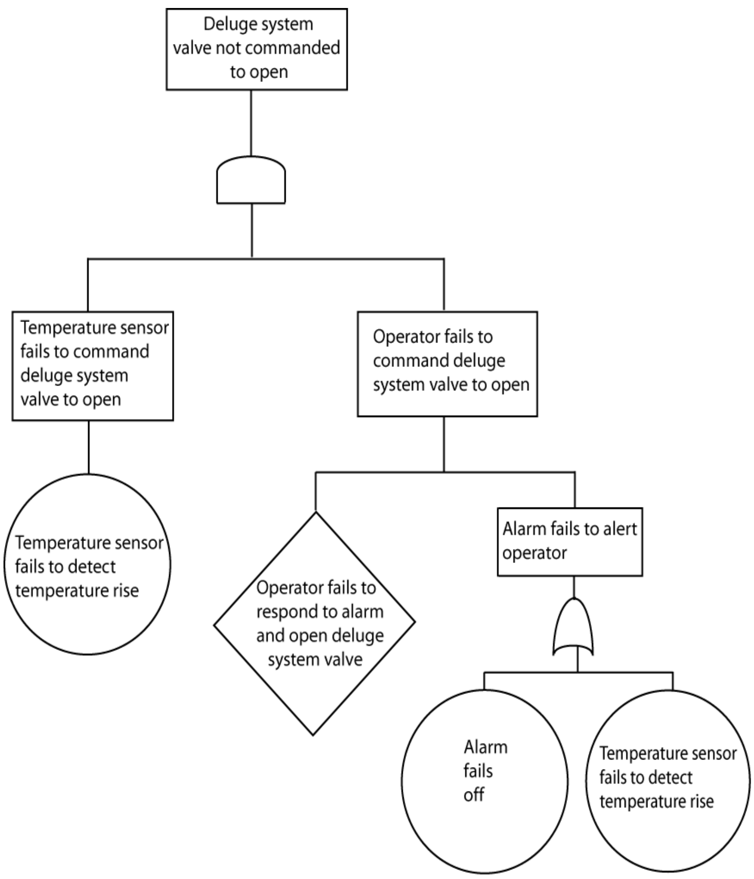
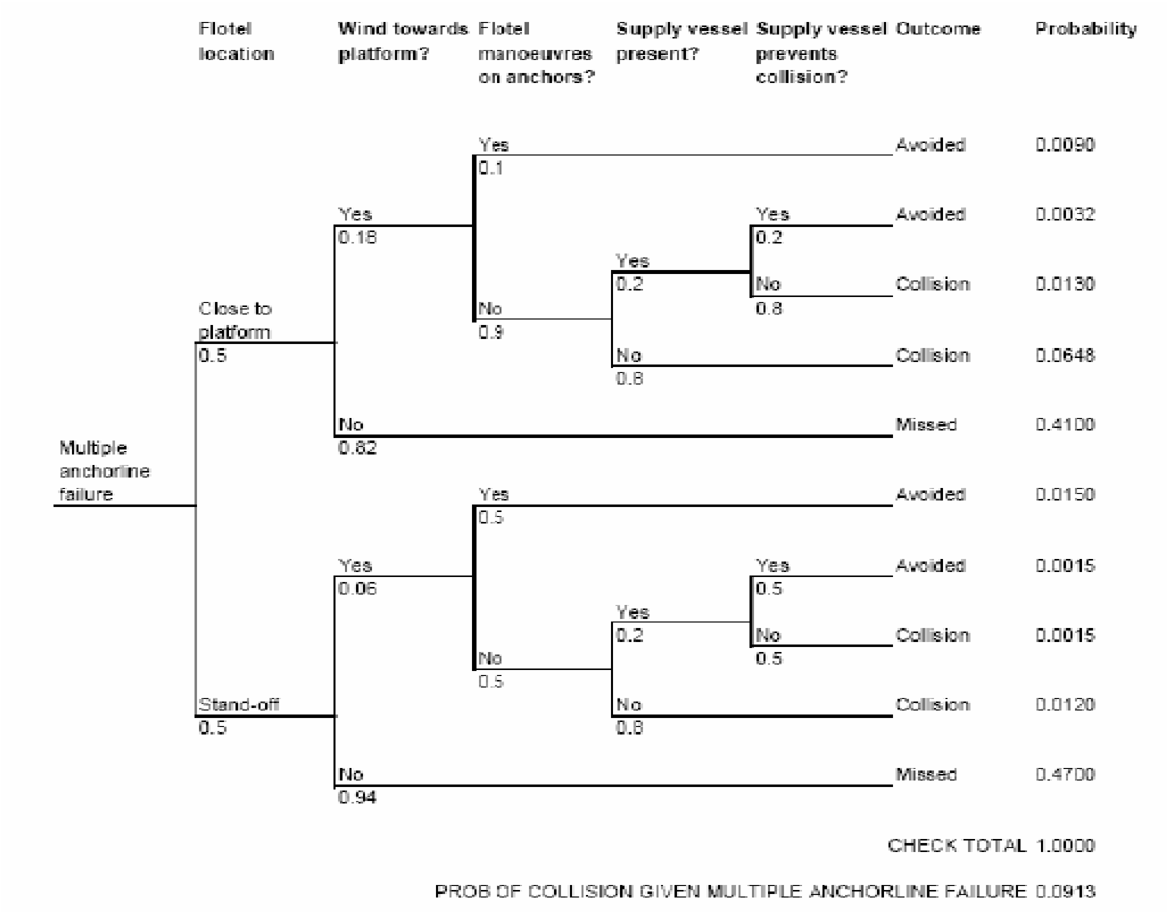


Figure 2: Example Event Tree Analysis



9 COMPARISON OF COMMONLY USED HAZARD EVALUATION TECHNIQUES

9.1 SELECTION OF HAZARD EVALUATION TECHNIQUES

Many factors can influence the decision-making process in the selection of the proper technique. The most significant aspects are:

- motivation for the study
- type of results needed
- type of information available to perform the study
- characteristics of the analysis problem: complexity, size, type of process/operations
- perceived risk associated with the process or activity
- resource availability
- analysis' background.

Appendix 1 - Overview of Hazard Evaluation Techniques

Table 5

Hazard Evaluation Tool	Summary of Method	More Common Uses
What-if Analysis		• Useful for any type of system, process or activity • Most often used when the use of other, more precise, methods (e.g., FMECA and HAZOP analysis) are not possible or practical • What-if analysis is frequently combined with checklist analysis
Failure Modes and Effects Analysis (FMECA)		• Best suited for reviews of mechanical and electrical systems • Can be used to improve planned maintenance and equipment inspection plans • Can be used to support incident investigation • Can be used to support fault tree analysis. • Operator errors can be included.
Hazard and Operability (HAZOP) Analysis		• Used for finding safety hazards and operability problems in continuous process systems, especially fluid and thermal systems. Operator errors can be included.
Fault Tree Analysis (FTA)		• Suited to almost every type of risk assessment, but best used to focus on the basic causes of specific system failures of relatively complex combinations of events • Operator errors can be included. • Can be used for probability quantification.
Event Tree Analysis (ETA)		• Suited to almost every type of risk assessment, but best used to focus on possible results of events for which many safeguards are in place as protective features • Often used for analysis of escalating scenarios like spread of fires or explosions or toxic releases • Operator errors can be included. • Can be used for probability quantification.

Table 6: Summary of Key Features of Risk Assessment Techniques

Risk Assessment Tools	Type of result				Types of activities or systems	Level of effort/ complexity	Level of expertise required for analysis teams
	Qualitative accident description	Quantitative Risk Characterizations	Relative importance of accident contributors	Recommendations			
What if analysis	√	√	√	√	All	Low to medium	Low to medium
FMEA	√			√	All, especially mechanical and electrical systems	Medium	Medium
HAZOP analysis	√			√	Cargo loading and unloading systems, especially fluid and thermal systems Sequential operations and procedures	Medium to high	Medium
FTA	√	√	√	√	All	Medium to high	Medium to high
ETA	√	√	√	√	All	Medium to high	Medium to high

9.2 OVERVIEW OF CONSEQUENCE EVALUATION TECHNIQUES

9.2.1

For the purpose of a qualitative or semi-qualitative analysis, usually a hazard evaluation is sufficient. A more detailed study like a QRA requires the quantitative estimation of likelihood and consequences of the accident scenarios. As mentioned in the previous section, hazard evaluation techniques like FTA or ETA can be used for the quantification of the likelihood. Conversely, the quantification of the magnitude of the consequences requires ad-hoc simulation tools for the physical phenomena of the abnormal events likely to be originated in the accident scenarios, and their impact on personnel, plant and environment.

In most process systems, the abnormal events to be studied fall in three main categories:

- fires
- explosions
- release of hazardous materials.

In turn, each category includes different types of abnormal events, which have to be evaluated by specific prediction models that must include meteorological (wind and stability) and topographic features.

The final quantification of the risk requires the definition of the damage criteria to personnel and structures due to the incident heat flux.

There are a number of empirical limits of thermal radiation which have traditionally been used in land-based plant design. Some sources are listed in the following:

- API RP 510
- BS 5908
- Frank P. Lees, ‘Loss Prevention in the Process Industries’, 1996
- NFPA standards
- NORSOK standards.

Damage criteria are to be established up front and approved by Tasneef.

9.2.2 Definitions

This item provides a list of the most common consequence models.

a) Source Terms
Characteristics of a release in terms of flow rate, duration, physical and hazardous properties of the substances released.

b) Jet fire
A jet fire can occur when a high speed release of flammable gas finds an ignition source close to the point of release. The heat radiation can damage the nearby structures and personnel around the likely points of release.

c) Fireball
A fireball can occur if a vessel of a pressurized flammable liquefied gas fails causing a flash evaporation of a portion of the liquid and the sudden formation of a vapour cloud. If the vapour is ignited immediately, it can originate a burning sphere.

d) Pool Fire
A pool fire can occur from the ignition of a pool of vaporizing hydrocarbon fuel, where the fuel vapour has negligible initial momentum.

e) Tank Fire
A fire burning the contents of an oil storage tanks.

f) Flash Fires
A flash fire can occur from the ignition of a gas or vapour cloud, where a delay between the release of flammable material and subsequent ignition has allowed a cloud of flammable material to build up and spread out from its release point.

g) Boiling Liquid Expanding Vapour Explosion (BLEVE)
A BLEVE can occur when a vessel containing pressure-liquefied gas fails catastrophically with the release of the entire inventory, due to a fire (such as a pool or jet fire) that impinges on the vessel, raises its internal pressure and weakens its containment.

h) Confined Gas Explosion
A confined gas explosion can occur when a flammable cloud of vapour or gas finds an ignition source within a confined space, which may be e.g. a structure, a vessel or a duct.

i) Unconfined Vapour Cloud Explosion (UVCE)
An unconfined vapour cloud explosion can occur when a massive release of flammable vapours finds a delayed ignition source.

j) Rapid Phase Transition Explosion (RPT)
A rapid phase transition explosion can occur if a hot and relatively non volatile liquid contacts a colder and more volatile liquid (like in case of release of LNG on water). In certain circumstances the vaporization of the cold liquid occurs in such a brief time to resemble an explosion.

k) Toxic Release
The release of toxic substances usually consists of:
   - emission
   - dispersion

l) Emission
Emission is usually due to a failure of plant integrity, or to other circumstances such as valves deliberately opened or forced venting in emergencies. Emission situations may be classified as follows:
   1) Fluid
      - Gas/vapour
      - Liquid
      - Vapour-liquid mixture

2) Plant
   - vessel
   - other equipment
   - pipe work
3) Aperture
   - Complete rapture
   - Limited aperture
4) Enclosure
   - Within structures
   - In open air
5) Height
   - Below deck level
   - At deck level
   - Above deck level
6) Fluid momentum
   - Low momentum
   - High momentum

m) Dispersion

Emission and vaporization are followed by dispersion of the relevant gas or vapour.

Dispersion situations may be classified as follows:

1) Fluid buoyancy
   - Neutral buoyancy
   - Positive buoyancy
   - Negative buoyancy
2) Momentum
   - Low momentum
   - High momentum
3) Source geometry
   - Point source
   - Line source
   - Area source
4) Source duration
   - instantaneous
   - continuous
   - intermediate
5) Source elevation
   - deck level
   - elevated source

The following figures illustrate the most typical scenarios that can be involved in a QRA.

Figure 3: Types of fire

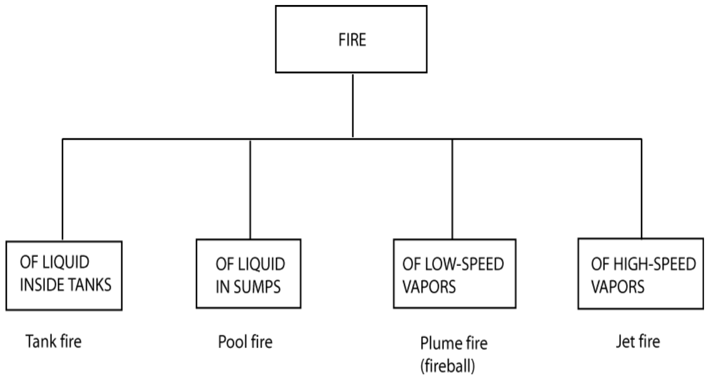


Figure 4: Types of explosions

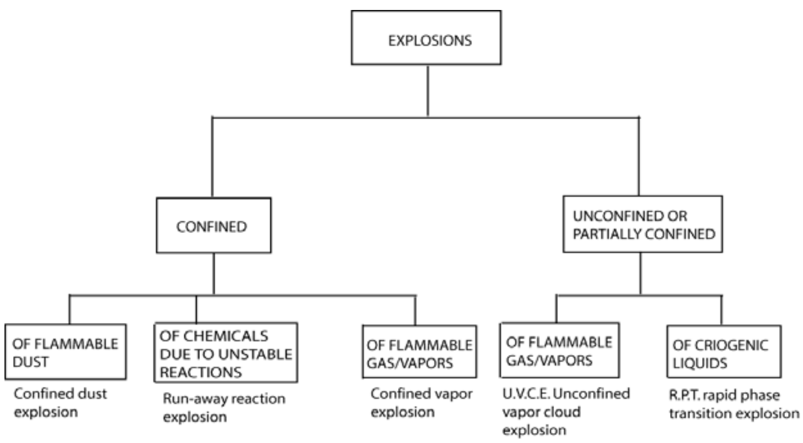


Figure 5: Types of release

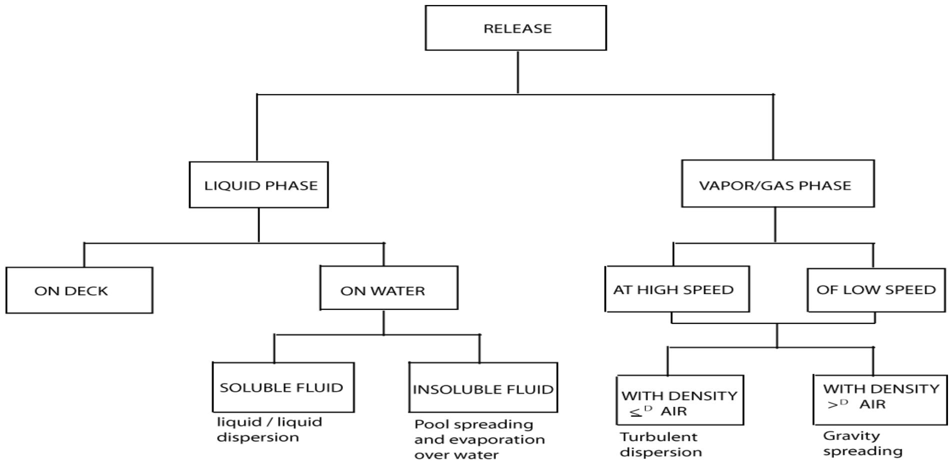


Table 7

Main mathematical models necessary for the evaluation of the likely consequences of abnormal occurrences in the process industries.	
1. Thermal radiation	1.1. From tank fires 1.2. “ pool fires 1.3. “ fireballs 1.4. “ jet fires
2. Overpressure	2.1. Confined dust explosions 2.2. Confined vapor explosions 2.3. Run-away reactions 2.4. Unconfined vapor cloud explosion 2.5. Rapid phase transition explosion
3. Dispersion	3.1. Liquid spreading and evaporation on deck 3.2. Liquid spreading and evaporation over water 3.3. Soluble liquid mixing and dilution 3.4. Turbulent jet dilution 3.5. Turbulent plume dispersion 3.6. Gravity spreading