1. OBJECTIVE

Establish the different techniques and tools for the identification, analysis, and assessment of risks, which may be used within the framework of the application of the guidelines of the Contractual Risk Manual.

2. SCOPE

This guide summarizes and indicates some risk assessment techniques and tools based on the contents of the standard NTC-IEC/ISO 31010:2013 Risk Management, Risk Assessment Techniques, which will be useful when performing the steps of risk identification, analysis, and evaluation.

3. TERMS DEFINITIONS

3.1. Possibility: Potential for something to happen.

3.2. Opportunity: Combination of circumstances that are expected to be favorable to the objectives.

3.3. Risk factor: Factor that has an important influence on risk.

3.4. Threat: Potential source of danger, harm, or other undesirable outcomes.

4. DEVELOPMENT OF ACTIVITIES

4.1. TECHNIQUES AND TOOLS FOR RISK IDENTIFICATION, ANALYSIS, AND ASSESSMENT

A combination of several techniques could result in an adequate risk study with less uncertainty in the characterization of each assessed risk.

The list developed here is not an exhaustive list of the available instruments that can be applied. It includes some summarized techniques and tools used when performing risk management exercises.

4.2. APPLICATION

4.2.1. Types of Techniques

This classification shows how the techniques are applied to each step of the risk assessment process.

For each corresponding step, the applicability of the tools and techniques is described as follows:

a) Resoundingly Applicable (RA).
b) Applicable (A) or
c) Not applicable (NA).

Table 1. Applicability of risk assessment tools.

Tools and Techniques	Risk Assessment Process				
	Risk Identification	Risk Analysis			Risk Assessment
		Consequence	Probability	Level of Risk	
Brainstorming	RA	NA	NA	NA	NA
Expert Panel (EP)	NA	RA	RA	RA	RA
Delphi Technique	RA	NA	NA	NA	NA
Structured or semi-structured interviews	RA	NA	NA	NA	NA
Checklist	RA	NA	NA	NA	NA
Structured "What If" Technique (SWIFT)	RA	RA	RA	RA	RA
Scenarios analysis	RA	RA	A	A	A
Preliminary Hazard Analysis (PHA)	RA	NA	NA	NA	NA
Hazard and Operability Studies (HAZOP)	RA	RA	A	A	A
Fault tree analysis	A	RA	A	A	NA
Monte Carlo simulation	NA	NA	NA	NA	RA
Matrix of consequences and probabilities	RA	RA	RA	RA	A

4.2.2. Factors influencing the selection of risk assessment techniques

The attributes of the methods are described below in terms of:

a) Complexity of the problem and the methods needed to analyze it.
b) The nature and degree of uncertainty of the risk assessment based on the amount of information available and what is required to meet the objectives.
c) The extent of resources required in terms of time and level of expertise, data needs, or whether the method can provide a quantitative result.

Table 2. Attributes of a selection of risk assessment tools

Examples of Types of risk assessment techniques and methods	Description	Is a quantitative result possible?
RESEARCH METHODS		
Checklist	A simple way of risk identification. A technique that provides a list of typical uncertainties to be considered. Users refer to a list, codes, or standards previously developed.	No
Preliminary analysis of hazards (PHA)	A simple method of inductive analysis aimed at identifying hazards and hazardous situations and events that may cause damage to a given activity, facility, or system.	No
SUPPORT METHODS		
Brainstorming and Structured or semi-structured interviews	A means of compiling a broad set of ideas and evaluations, ranked by a team. Brainstorming can be stimulated by guidelines or by one-on-one or group interview techniques.	No
Delphi Technique	A means of combining expert opinions that can support source and influence identification, probability estimation, consequence, and risk assessment. It is a collaborative technique to generate consensus among experts. Involve independent analysis and expert voting.	No
Structured "What If" Technique (SWIFT)	A system to induce a team to identify risks. Normally used within a facilitated workshop. Regularly linked to a risk analysis and assessment technique.	No
SCENARIOS ANALYSIS		
Scenarios analysis	Possible future scenarios are identified through imagination or extrapolation from the present, and different risks are considered, assuming that each scenario could occur. This can be done formally or informally, qualitatively or quantitatively.	No

Fault tree analysis	A technique that starts with the undesired event (maximum event) and determines all the ways in which it could occur. These are shown graphically in a logic tree diagram. Once the fault tree has been developed, ways to reduce or eliminate potential causes/sources should be considered.	Yes
FUNCTION ANALYSIS		
Hazard and Operability Studies (HAZOP)	A general risk identification process to define possible deviations from expected or planned performance. It uses a system based on the guide word. The criticalities of the deviations are evaluated.	No
Examples of Types of risk assessment techniques and methods	Description	Is a quantitative result possible?
STATISTICAL METHODS		
Monte Carlo simulation	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system for a number of inputs, where each input has a defined distribution, and these are related to the output through defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be defined mathematically. Such inputs may be based on various distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used.	Yes

4.3. TECHNIQUES AND THEIR DESCRIPTION

4.3.1. Brainstorming

Brainstorming involves stimulating and encouraging fluid conversation among a group of knowledgeable people to identify possible failure modes and associated hazards, risks, and criteria for decisions, or treatment options. The term "brainstorming" is often used loosely to refer to any type of group discussion. However, true brainstorming involves particular techniques to spark people's imaginations through the group's thoughts and statements.

Effective facilitation is very important in this technique and includes stimulating discussion at the outset, periodic group guidelines in other relevant areas, and capturing issues that arise from the discussion.

4.3.1.1. Usage

Brainstorming can be used in conjunction with other risk assessment methods described below, or it can stand alone as a technique to encourage imaginative thinking at any stage of the risk management process. It can be used for high-level discussions where difficulties are identified for a detailed review of particular problems.

Brainstorming places a strong emphasis on imagination, so it is particularly useful when identifying risks of new technologies because there is no data or when new solutions to emerging problems are needed.

4.3.1.2. Inputs

A multidisciplinary team of people with knowledge of the organization, system, process, or subject being evaluated.

4.3.1.3. Process

Brainstorming can be formal or informal. The former is more structured, requiring participants to be prepared in advance as the session has a clearly defined purpose and outcome, which is to evaluate the ideas presented. Informal brainstorming is less structured and often more ad-hoc[1].

In a formal process, the following characteristics are observed:

- **a)** The facilitator prepares thought messages that incite cognitive activity on the specific topic and context-appropriate triggers before the session;
- **b)** The objectives of the session are defined and the rules are explained to the participants;
- **c)** The facilitator starts a line of thought, and everyone explores ideas identifying as many problems as possible. There is no discussion at this time about whether or not things should be on a list or what particular statements mean because this tends to inhibit free thought.
- **d)** All entries are accepted, and none are criticized. The idea is to move the group forward quickly to allow ideas to activate lateral thinking[2];
- **e)** The facilitator can pull people away on a new line when one direction of thought is exhausted or the discussion gets too sidetracked. The idea, however, is to collect as many diverse ideas as possible for further analysis.

4.3.1.4. Outputs

The outputs depend on the stage of the risk management process at which it is applied. For example, at the identification stage, the outputs may be a list of current risks and controls.

4.3.2. <u>Expert Panel (EP)</u>

This technique consists of bringing together a group of independent and qualified specialists in at least one of the subjects or fields concerned by the issue to be evaluated. The purpose is to issue a collective and consensual judgment on said matter.

4.3.2.1. Inputs

[1] It is used as an adjective phrase in the sense of 'suitable, appropriate, specially arranged for a purpose'.

[2] Edward De Bono, El uso del pensamiento lateral, 1967.

Prior to the EP, all members of its members shall be informed of the background, objectives, and topics to be discussed, and the documentation required by them for analysis shall be submitted. It should be verified that the experts have the minimum necessary knowledge of the project.

4.3.2.2. Process

There must be a previous stage of validation, by the experts, of identifying project risks or causes of risk under previous analysis. If the panel's purpose is to identify the contract risks or causes of the risk under analysis, the panelists must first meet with the contract structurer team. For this stage it is recommended:

a) To establish scales of probabilities and consequences: To analyze risks it is necessary to create qualitative scales that reflect the different levels of probability of occurrence of each risk and, in addition, allow quantifying the impact within the project in case of its materialization. The ranges should correspond to the experts' experiences and be consistent with the risk assessment.

It is important to avoid constructing wide ranges which make most of the risks concentrated in a certain position. This is to eliminate possible answers in the intermediate valuation range, which do not suggest a neutral position on the part of the experts.

b) Assessment of probabilities and consequences per risk: For each risk identified or its causes, the experts will assess its probability and impact. At a minimum, they should establish ranges with a minimum, average, and maximum value based on the particular information of the contract under analysis. How this information will be used will depend on the valuation methodology used by the panel.

c) Assessment of possible cost overruns and longer terms for risks where applicable.

4.3.2.3. Outputs

Once all panel members have assessed the probabilities and impacts of the risks, their cost overruns, and schedule overruns, or the causes of the risk under analysis, the workshop leader will proceed to apply the selected methodology to aggregate these assessments and make a projection of the estimated cost overruns and schedule overruns for the project.

4.3.3. <u>Delphi Technique</u>

The Delphi Technique is a procedure for obtaining a reliable consensus of opinion from a group of experts. An essential feature of this technique is that the experts can express their opinions individually and anonymously while having access to each other's opinions as the process progresses.

4.3.3.1. Usage

The Delphi technique can be applied at any stage of the risk management process or at any stage of a system's life cycle as long as a consensus of expert opinions is required.

4.3.3.2. Inputs

A set of options for which consensus is needed.

4.3.3.3. Process

A group of experts is questioned by means of a semi-structured questionnaire.

Experts are not assembled so that their opinions are independent.

The procedure is as follows:

- **a)** Formation of a team to undertake and monitor the Delphi process;
- **b)** Selection of a group of experts (it may be one or more panels of experts);
- **c)** Implementing the first-round questionnaire. The number of rounds to be carried out will depend on the need and results achieved from round 1 to round n.
- **d)** Test the questionnaire, determining whether the questions correctly fit the reality of the issue and whether the eventual answers can lead to consensus;
- **e)** Send the questionnaire individually to the panelists;
- **f)** The information from the first round of responses is analyzed, combined, and re-distributed to the panelists;
- **g)** Panelists respond, and the process is repeated in n number of rounds until a consensus is reached.

4.3.3.4. Outputs

Convergence towards consensus on the issue in question.

4.3.4. <u>Structured or semi-structured interviews</u>

In a structured interview, individual interviewees are asked a set of questions prepared from a questionnaire that encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar but allows more freedom in a conversation to explore issues that arise.

4.3.4.1. Usage

Structured and semi-structured interviews are useful when it is difficult to bring people together for a brainstorming session, or when free-flowing group discussion is not appropriate for the situation or the people involved. They are most often used to identify risks or to evaluate the effectiveness of existing controls as part of risk analysis. They can be applied at any stage of a project or process, as they are a means of providing stakeholder input to the risk assessment.

4.3.4.2. Inputs

Inputs include:

- **a)** A clear definition of the objectives of the interviews;
- **b)** A list of interviewees selected from relevant stakeholders; **c)** A questionnaire.

4.3.4.3. Process

A set of relevant questions is created to guide the interviewer. They should be open-ended whenever possible, simple, in an appropriate language for the interviewee, and they should seek to cover only one topic. Similarly, possible follow-up questions are prepared to seek clarification. Then, the interviewee is asked questions, taking care of guiding his or her response.
Responses should be considered with a degree of flexibility to provide the opportunity to explore areas where the respondent may wish to go.

4.3.4.4. Outputs

The results are the stakeholders' views on the issues that prompted the interviews.

4.3.5. <u>Checklist</u>

Checklists are lists of events, risks, or control failures that have generally been developed from experience, either due to previous risk assessment or past failures.

4.3.5.1. Usage

A checklist can be used to identify hazards and risks or to evaluate the effectiveness of controls. They can be used at any stage in the life cycle of a product, process, or system or as part of other risk assessment techniques, but they are most useful when applied to verify that everything has been covered after using a more imaginative technique that identifies new problems.

4.3.5.2. Inputs

It is essential to have prior information and experience on the subject so that a relevant and preferably validated checklist can be selected or developed.

4.3.5.3. Process

The procedure is as follows:

- **a)** Define the scope of the activity;
- **b)** Select a checklist that adequately covers the scope. Checklists should be carefully selected for the purpose. For example, a standard controls checklist cannot be used to identify new hazards or risks;
- **c)** The person or team using the checklist steps, through each element of the process or system, reviews whether the items on the checklist are present.

4.3.5.4. Outputs

The results depend on the stage of the risk management process in which they are applied. For example, the result may be a list of controls that are inadequate or a list of risks.

4.3.6. Structured "What If" Technique (SWIFT)

It is a systematic study based on teamwork, using a set of "quick" words or phrases that the facilitator uses to stimulate participants to identify risks within a workshop. The facilitator and team use "*what if*" statements in combination with the instructions to investigate how a system, process, plant element, organization, or procedure will be affected by deviations from normal operations and behavior.

4.3.6.1. Usage

While SWIFT was originally designed to study chemical and petrochemical plant hazards, the technique is now widely applied to systems, plant elements, procedures, and organizations in general. In particular, it is used to examine the consequences of changes and altered or created risks.

4.3.6.2. Inputs

The system, process, procedure, plant element, and/or change must be carefully defined before the study begins. The external and internal contexts are established through interviews and the facilitator's study of documents, plans, and drawings. Normally, the element, situation, or system under study is divided into nodes or key elements to facilitate the analysis process, but this rarely occurs at the level of definition required.

Other key information is the expertise and experience of the study team, whose members should be carefully selected. All interested parties should be represented, if possible, along with those with experience in similar elements, systems, changes, or situations.

4.3.6.3. Process

The general process is as follows:

- **a)** Before the study begins, the facilitator prepares a quick and appropriate list of words or phrases that can be based on a standard set or created to allow a thorough review of the hazards or risks.
- **b)** In the workshop, the external and internal contexts of the item, system, change, or situation and the scope of the study are discussed and agreed upon.
- **c)** The facilitator asks participants to raise and discuss known risks and hazards, previous experience and incidents, known and existing controls and safeguards, regulatory requirements, and restrictions.
- **d)** Discussion is facilitated by creating a question using a "what if" phrase and a cue word or topic. Phrases that can be used are, "what if...?", "what would happen if...?", "could someone or something...?", and "would someone or something ever...?". The intention is to encourage the study team to explore potential scenarios, their causes, consequences, and impacts.
- **e)** Risks are summarized, and the team considers existing controls. The description of the risk, its causes, consequences, and expected controls are confirmed with the team and recorded.
- **f)** The team considers whether the controls are adequate and effective and agrees on a risk control effectiveness statement. If this is not satisfactory, the team further considers risk treatment tasks, and possible controls are defined.

g) During this discussion, more "what if" questions are posed to identify other risks.
h) The facilitator uses the list of suggestions to monitor the discussion and suggest additional problems and scenarios for the team to discuss.
i) It is normal to use a qualitative or semi-quantitative risk assessment method to rank the actions created in terms of priority. This risk assessment is normally performed taking into account existing controls and their effectiveness.

4.3.6.4. Outputs

The outputs include a risk record with actions or tasks classified by risk, which can become the basis of a treatment plan.

4.3.7. SCENARIOS ANALYSIS

Scenarios analysis, created to develop descriptive models of what the future might look like, can be used to identify risks when considering possible future developments and to explore

its implications. Sets of scenarios reflecting, for example, "best case", "worst case", and "expected case" can be used to analyze the possible consequences and their probabilities, as a form of sensitivity analysis when analyzing risk.
Scenarios analysis cannot predict the likelihood of change, but it can consider consequences and help organizations develop the strengths and resilience needed to adapt to foreseeable changes.

Scenarios analysis can be used to help make policy decisions and plan future strategies, as well as to consider existing activities. It can play a role in all three components of risk assessment.
For identification and analysis, sets of scenarios reflecting, for example, "best-case", "worst-case", and "expected" scenarios can be used to identify what might happen under particular circumstances and to analyze the possible consequences and their probabilities for each scenario.

Scenarios analysis can anticipate how both threats and opportunities will develop and can be used for all types of risks with short- and long-term time frames. With short time frames and good data, likely scenarios can be extrapolated from the present. For longer time frames, or with weak data, scenario analysis becomes more imaginative and could be said to be future analysis.

Scenarios analysis can be useful when there are strong distributional differences between positive and negative outcomes across space, time, and groups in the community or an organization.

4.3.7.1. Inputs

The prerequisite for scenarios analysis is a team of people who understand the nature of the relevant changes (e.g., possible advances in technology) and the imagination to think about the future without necessarily extrapolating from the past. Access to literature and data on changes that are already occurring is also helpful.

4.3.7.2. Process

The structure for scenario analysis can be informal or formal.

Having established a team, the relevant communication channels, and defined the context of the problem(s) to be considered, the next step is to identify the nature of the changes that may occur. This will require research on major trends and the likely time of changes in trends, as well as imaginative thinking about the future.

Changes to be considered may include:

- **a)** External changes (such as technological changes);
- **b)** Decisions to be made in the near future but which may have a variety of outcomes;
- **c)** Stakeholder needs and how they might change;
- **d)** Changes in the macro environment (regulatory, demographic, etc.). Some will be inevitable and others will be uncertain.

Sometimes a change may be due to the consequences of another risk. For example, the risk of climate change is driving changes in consumer demand related to large quantities of food. This will influence which foods can be exported profitably and which can be grown locally.
Local and macro factors or trends can now be listed and classified according to (1) their uncertainty and (2) their importance. Special attention is given to the most important and uncertain factors. Key factors or trends are mapped against each other to show areas where scenarios can develop. For

the above, a series of scenarios are proposed, each focusing on a plausible change in the parameters.

A "story" is then written for each scenario which indicates how to move from here to the target scenario, and it can include precise details that add value to the scenarios.

Similarly, scenarios can be used to test or evaluate the original question by taking into account any significant but predictable factors (e.g., usage patterns) and then exploring how successful the policy (activity) would be in this new scenario and the results of previous tests using "what if" questions in model assumptions.

When the question or proposal has been evaluated concerning each scenario, it may be obvious that it needs to be modified to make it more robust or less risky. It should also be possible to identify some leading indicators that show when change is occurring. Monitoring and responding to leading indicators can provide the opportunity to change planned strategies.

As scenarios are only defined as "segments" of possible futures, it is important to ensure that the probability of a particular outcome (scenario) occurring is taken into account, i.e., that a risk framework is adopted. For example, in the best-case, worst-case and expected cases, an attempt should be made to qualify or express the probability of occurrence of each case.

4.3.8. Preliminary Hazard Analysis (PHA)

The PHA is a simple and inductive analysis method that aims to identify hazards, hazardous situations, and events that can cause damage to a given activity, facility, or system.

4.3.8.1. Usage

It is most commonly carried out early in the development of a project, when there is little information on design details or operating procedures, and can often be a precursor to new studies or provide input to the specification of a system design. It can also be useful when analyzing existing systems, to prioritize hazards and risks through further analysis, or when circumstances prevent using a more extensive technique.

4.3.8.2. Inputs

Inputs include:

a) Information on the system to be evaluated;
b) Details of the system design according to its availability and relevance.

4.3.8.3. Process

A list of hazards, situations, and generic hazardous risks is formulated by considering characteristics such as:

a) Materials used or produced and their reactivity;
b) Equipment used;
c) Operating environment;
d) Design;

e) Interfaces between system components, etc.

Qualitative analysis of the consequences of an undesirable event and its probabilities can be carried out to identify risks for further assessment.

The PHA should be updated during the design, construction, and testing phases to detect new hazards and make corrections, if necessary. The results can be presented in different ways, such as through tables and trees.

4.3.8.4. Outputs

Results include:

a) A list of hazards and risks;
b) Recommendations in the form of acceptance, recommended controls, design specifications, or requests for more detailed evaluations.

4.3.9. <u>HAZOP</u>

HAZOP is the acronym for Hazard and Operability study. It is a structured and systematic examination of a planned or existing product, process, procedure, or system. It is a technique for identifying risks to people, equipment, the environment, and/or the organization's objectives. The study team is also expected, whenever possible, to provide a solution to address the risk.

The HAZOP process is a qualitative technique based on using guide words that question how the design intent or operating conditions might not be achieved at each step of the design, process, procedure, or system. It is used to identify risks to people, equipment, environment, and/or organizational objectives and sometimes it can provide a solution to address risk. In general, it is carried out by a multidisciplinary team during a series of meetings designed for this purpose.

4.3.9.1. Usage

The HAZOP technique was initially developed to analyze chemical process systems but has been extended to other types of complex systems and operations. These include mechanical and electronic systems, procedures and software systems, organizational changes, and design and legal review of contracts. It can address all deviations from design intent due to design deficiencies, components, planned procedures, and human actions.

It is widely used for software design review. When applied to the control of safety-critical instruments and computer systems, it may be referred to as CHAZOP (Control Hazards and Operability Analysis) or computer hazards and operability analysis.

A HAZOP study is generally conducted at the detail design stage when a complete diagram of the intended process is available, and design changes are still feasible. However, it can be carried out in a phased approach with different guide words for each stage as the design develops in detail. A HAZOP study can also be carried out during operation, but the changes required may be costly at that stage.

4.3.9.2. Inputs

Essential inputs to a HAZOP study include current information about the system, the process, or procedure to be reviewed, and the design intent and performance specifications.

Inputs may include drawings, specification sheets, flow sheets, process control and logic diagrams, layout plans, operating and maintenance procedures, and emergency response procedures. For non-hardware HAZOP, inputs can be any document describing functions and elements of the system or procedures under study. For example, inputs can be organizational diagrams and job descriptions, a draft contract, or even a draft procedure.

4.3.9.3. Process

HAZOP takes the "design" and specification of the process, procedure, or system under study and reviews each part of it to discover what deviations from expected performance may occur, what the potential causes are, and what the likely consequences of a deviation are. This is achieved by systematically examining how each part of the system, process, or procedure will respond to changes in key parameters through the use of appropriate guide words.

Guide words can be customized for a particular system, process, or procedure, or generic words can be used to cover all types of deviations.

The normal steps in a HAZOP study include:

- **a)** Appointment of a person with the necessary responsibility and authority to carry out the HAZOP study and to ensure that all actions arising from the study are completed;
- **b)** Definition of the objectives and scope of the study;
- **c)** Establish a set of key or guide words for the study;
- **d)** Define a HAZOP study team; this team is usually multidisciplinary and should include design and operations personnel with appropriate technical expertise to assess the effects of deviations from the planned or current design. It is recommended that the team include persons not directly involved in the design or the system, process, or procedure under review;
- **e)** Compilation of the required documentation;
- **f)** Divide the system, process, or procedure into smaller elements or subsystems or sub-processes or sub-elements to make the review tangible;
- **g)** Agree on the design intent for each subsystem, sub-process, or sub-element, and then for each element in that subsystem or element applying the guide words one after the other to postulate possible deviations that will have undesirable results;
- **h)** Where an undesirable outcome is identified, agree on the cause and consequences in each case and suggest how they might be addressed to prevent them from occurring, or mitigate the consequences if they do;
- **i)** Document the discussion and agree on specific actions to address the identified risks.

4.3.9.4. Outputs

Record of HAZOP meetings with items for each review point recorded. This should include the guide word used, the deviation(s), possible causes, actions to address the identified problems, and the person responsible for the action. For any deviation that cannot be corrected, the risk of the deviation must be assessed.

4.3.10. Fault Tree Analysis (FTA)

FTA is a technique for identifying and analyzing factors that may contribute to a specific undesirable event called the "top event". The causal factors are identified deductively, organized logically, and represented graphically in a tree diagram depicting the causal factors and their logical relationship to the top event.

The factors identified in the tree can be events associated with component hardware failures, human error, or any other relevant event that leads to the undesired event.

4.3.10.1. Usage

A fault tree can be used qualitatively to identify potential causes and paths to failure (the top event) or to quantitatively calculate the probability of the top event, given knowledge of the probabilities of causal events.

It can be used in the design stage of a system to identify possible causes of failure and, therefore, select between different design options. It can be used in the operational phase to identify how major failures may occur and the relative importance of different pathways to the top event. A fault tree can also be used to analyze a failure that has occurred to show in a diagram how the different events came together to cause the failure.

4.3.10.2. Inputs

For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to assist in the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state are required for all basic events in the fault tree.

4.3.10.3. Process

The steps to develop a fault tree are as follows:

- **a)** The top event to be analyzed is defined. This may be a failure or perhaps a broader result of that failure. When the result is analyzed, the tree may contain a section related to the actual failure mitigation.
- **b)** Starting with the top event, the possible immediate causes or failure modes leading to the main event are identified.
- **c)** Each of these cause/failure modes is analyzed to identify how its failure could be caused.
- **d)** Step-by-step identification of undesirable system performance is followed to successively reduce system levels until further analysis becomes unproductive. In a hardware system, this may be the failure level of the component. The events and causal factors at the lowest level of the system under analysis are known as basic events.
- **e)** When probabilities can be assigned to basic events, the probability of the top event can be calculated. For quantification to be valid, it must be possible to demonstrate that, for each gate, all inputs are necessary and sufficient to produce the output event. If this is not the

case, the fault tree is not valid for probability analysis, but it can be a useful tool to show causal relationships.

Except for single fault trees, a software package is needed to properly handle the calculations when there are repeated events at various locations in the fault tree and to calculate the minimum cut sets. Software tools help ensure consistency, correctness, and verifiability.

4.3.10.4. Outputs

The outputs of the fault tree analysis are as follows:

a) A graphical representation of how the main event may occur showing interactive pathways where two or more simultaneous events must occur;
b) A list of minimum failure sets (individual paths) with the probability of occurrence of each when data are available;
c) The probability of the maximum event.

4.3.11. Monte Carlo Simulation

Many systems are too complex to model the effects of uncertainty using analytical techniques, but they can be evaluated by considering the inputs as random variables and running an "N" number of calculations (so-called simulations), sampling the input to obtain "N" possible outcomes of the desired result.
This method can address complex situations that would be very difficult to understand and solve using an analytical method. Systems can be developed using spreadsheets and other conventional tools, but more sophisticated tools are available to assist with more complex requirements, including Crystal Ball, @RISK, Risk Simulator, and MathWorks, among others.

4.3.11.1. Usage

Monte Carlo simulation provides a means to evaluate the effect of uncertainty in systems in various situations. It is typically used to assess the range of possible outcomes and the relative frequency of values in that range for quantitative measures of a system such as cost, duration, performance, demand, and similar measures. Monte Carlo simulation can be used for two different purposes:

a) Uncertainty propagation in conventional analytical models;
b) Probabilistic calculations when analytical techniques do not work.

4.3.11.2. Inputs

The input to a Monte Carlo simulation is a good mathematical model that represents as closely as possible the project, budget, process, or risk issue under study, with types of inputs, the sources of uncertainty to be represented, and the required output. Input data with uncertainty are represented as random variables with distributions that are more or less dispersed according to the level of uncertainty.

4.3.11.3. Process

The process is as follows:

a) Define a mathematical model or algorithm that represents, as precisely as possible, the behavior of the system under study.
b) The model is run several times using random numbers to produce model outputs (system simulations); where the application is to model the effects of uncertainty, the model is in the form of an equation that provides the relationship between input parameters and output. The values selected for the inputs are taken from appropriate probability distributions that represent the nature of the uncertainty in these parameters.
c) In either case, a computer runs the model multiple times with different inputs and produces multiple outputs. These can be processed using conventional statistics to provide information such as mean values, standard deviation, and confidence intervals.

4.3.11.4. Output

The result could be a single value, or it could be a result expressed as the probability or frequency distribution, or it could be the identification of the main functions within the model that have the greatest impact on the output.

In general, a Monte Carlo simulation will be used to evaluate the full distribution of outcomes that could arise or key measures of a distribution such as:

a) The probability that a definite outcome will occur;
b) The value of an outcome in which the owners of the problem have a certain level of confidence that it will not be exceeded or hit, a cost that has less than a 10% probability of being exceeded, or a duration that is 80% certain to be exceeded.

An analysis of the relationships between inputs and outputs can illustrate the relative importance of factors in the work and identify useful targets for efforts to influence the uncertainty of the outcome.

4.3.12. <u>Matrix of consequences and probabilities</u>

The consequence/probability matrix is a means of combining qualitative or semi-quantitative consequence and probability ratings to produce a risk level or risk rating.

The format of the matrix and the definitions applied to it depend on the context in which it is used, and it is important that a circumstances-appropriate design is used.

4.3.12.1. Usage

A consequence/probability matrix is used to classify risks, their sources, and their treatments according to their level. It is commonly used as a screening tool when many risks are identified, for example, to define which require additional or more detailed analysis, which need treatment first, or which should be referred to a higher level of management. It can also be used to select, at the moment, which risks should not be considered further.

This type of risk matrix is also used widely to determine whether a given risk is broadly acceptable or unacceptable depending on the zone where it is located in the matrix. Similarly, it can be used to help communicate a common understanding of qualitative risk levels throughout the organization.

The way in which risk levels are established and the decision rules assigned must be aligned with the organization's risk appetite. A form of consequence/probability matrix is also used for criticality analysis or prioritization after HAZOP. It can also be used in situations where there is insufficient data for a detailed analysis of the situation and does not warrant the time and effort for a more quantitative analysis.

4.3.12.2. Inputs

The inputs to the process are custom scales for consequence and probability and a matrix combining the two.

The consequence scale (or scales) should cover the range of different consequences to be considered, e.g., financial loss, safety, environmental, or other parameters, depending on the context, and should range from the maximum credible consequence to the lowest consequence of concern. The scale can have any number of points. Scales of 3, 4 or 5 steps are the most common.

The probability scale can also have any number of points. Probability definitions should be selected to be as unambiguous as possible. If numerical guidelines are used to define different probabilities, then units must be given. The probability scale should cover the range relevant to the study in question, remembering that the lowest probability must be acceptable for the highest defined consequence. Otherwise, all activities with the highest consequence are defined as intolerable.

A matrix is drawn with consequence on one axis and probability on the other.

The risk levels assigned to the cells will depend on the definitions of the probability/consequence scales. The matrix can be configured to give additional weight to consequences or probability, or it can be symmetrical, depending on the application. Risk levels may be linked to decision rules, such as the level of management attention or the time scale by which a response is needed.

Rating scales and a matrix can be configured with quantitative scales. For example, in a reliability context, the probability scale might represent indicative failure rates, and the consequence scale cost of failure in dollars.

The use of the tool needs people (ideally a team) with the relevant expertise and data available to assist in consequence and probability judgments.

4.3.12.3. Process

To rank risks, the user first finds the consequence descriptor that best fits the situation and then defines the probability with which those consequences will occur. The risk level is then read from the matrix.

Many risk events can have a range of outcomes with different probabilities associated with them. Generally, minor problems are more common than catastrophes, which is why there is the option of ranking the most common or the most serious outcome or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as they pose the greatest threat and are often of greatest concern, and in others, it may be appropriate to classify common problems and unlikely catastrophes as separate risks. In any case, it is important to use the probability relevant to the selected consequence and not the probability of the event as a whole.

The risk level defined by the matrix may be associated with a decision rule, such as to treat or not to treat the risk.

4.3.12.4. Output

The result is a rating for each risk or a ranked list of risks with defined levels of importance.