Swiss Virtual Campus

« Dealing with Natural Hazards »

Module 5

Learning Unit: **Integral Natural Risk Management**

Detailed Table of Contents

Objectives

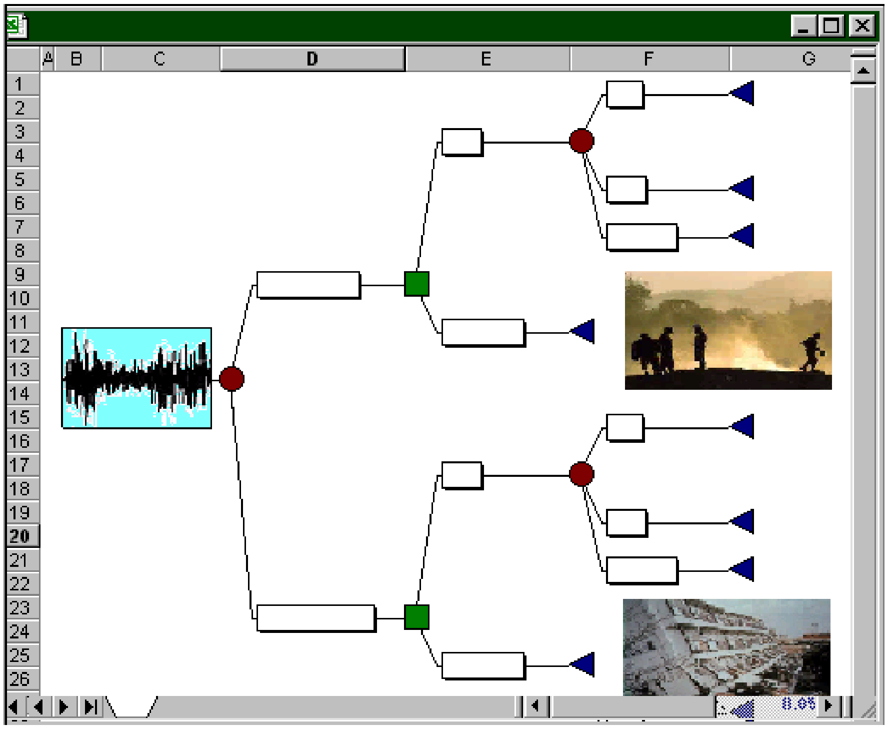


Figure 1
Risk Analysis relies on numerous well-tried dedicated methods and tools

The targets of this learning unit are to understand:

- the basic foundations, motivations and historical development of the science of risk analysis·
- the general principles and application fields of the risk analysis methods
- the characteristics of natural risk analyses ·
- the available approaches to conduct a qualitative, semi-quantitative or quantitative risk analysis

Introduction: Definition of Risk Analysis/Assessment

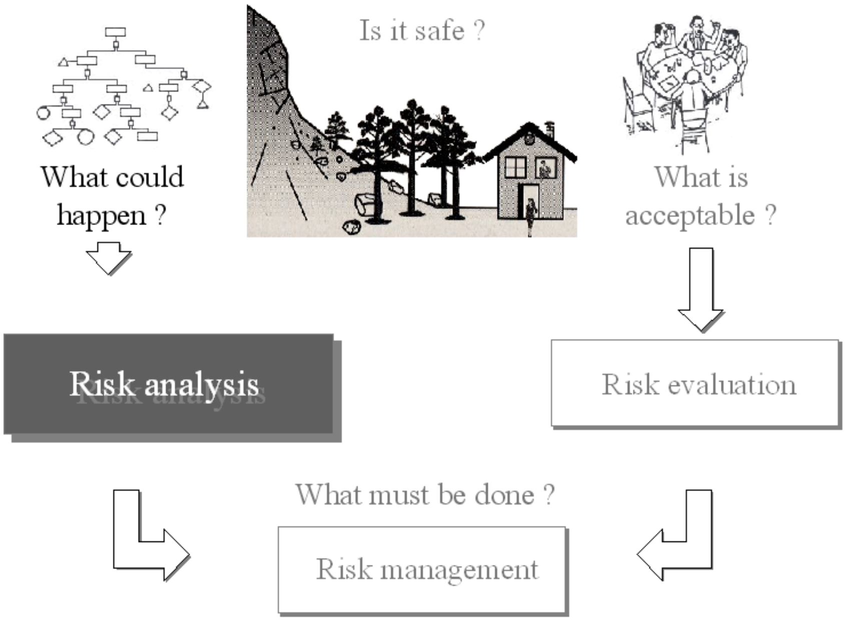


Figure 2
Risk analysis in the general risk management process
(source: [BUWAL, 107/I, 1999])

Risk analysis deals with the scientific determination and, when feasible, quantification of risks from hazard-related data and understanding of the processes involved.

Risk analysis aims at providing an answer to the question “what could happen ?” (see Fig. 2). This involves investigating the risk as a function of the probability of occurrence of a disaster and the possible consequences of resulting events in a given area.

When the process of risk analysis is more specifically focused on quantitative aspects (evaluation of damages or injuries, probability of occurrence) it is rather called *risk assessment*. Risk assessments provide a basis to judge whether the corresponding consequences/ probabilities are great enough to justify increased management or regulation.

Introduction: Risk Analysis, why?

Figure 3
A necessary balance of interests for efficient resource use

At many places, natural events such as flooding, debris flows, avalanches, rock falls and landslides represent a danger to persons and material assets. Protection measures, as well as measures for spatial planning and emergencies, can offer protection against these natural hazards, but they are costly. The objective is to achieve maximum safety for a minimum of investments; in other words, to aim at optimal efficiency. [BUWAL, 107/I, 1999]. Awareness of the natural risks by the public in general and percep-tion of how they compare to other risks determine society's attitudes about diminishing them (Fig. 3). Risk analysis is a primary step in achieving the objectives of better risk knowledge and more efficient resource utilisation.

Introduction: Short History of the Development of the Science of Risk Analysis

Figure 4
A very old human *concern*,
… but a (relatively) young *science*

The concern of preserving humankind from the negative consequences of its own creations or of natural events is certainly as old as the discovery of the fire, … or of the wheel (see Fig. 4)..If risk analysis, risk assessment and risk management are relatively new terms in public debate, they are practices with lengthy histories. According to historians, the first professional risk assessors were from ancient Babylon (3200 B.C.); these were consultants offering advices on risky, uncertain, or difficult decisions in life – such as marriage proposals or selecting building sites [American Chemical Society, 1998].The science of risk analysis is however much younger. It can be dated back to the infancy of the probabilistic "reliability" assessment of the German V-1 flying-bomb during World War II followed, immediately after the end of this one, by the progressive development of a whole arsenal of methods and tools for reliability and safety assessment purposes in the aircraft (later in the spacecraft) and nuclear industries in particular. Risk analysis, risk assessment and risk management are today everyday activities of industrial, banking, insurances, and business operations throughout the world. Important applications in human health and safety have been around for decades; research on natural hazard risks and disasters followed more recently.Let us recall here that a science is characterised by the fact that it relies on models (always an approximation of the reality), developed on the basis of the experience, able to deliver qualitative and quantitative forecasts when feed with appropriate data. The results thus obtained can in their turn be compared with measurements of real parameters, leading in case of discre-pancies to possible improvements of the model or input data (iterative process).

Introduction: Natural vs. Technological Risk Analyses

Figure 5
Natural vs. industrial risks: similar, … while different

Natural risks are related to events caused by natural forces (storms, flooding, avalanches, rock falls, volcanic eruptions, earthquakes, etc.). Such events generally result in a large number of individual losses. The extend of these losses depends not only on the severity of the natural forces concerned, but also on human factors like construction methods or the efficiency of disaster protection measures in the affected region.Technological – or, more generally, man-made risks – arise in direct conjunction with human activities (power generation, transport, production of goods, etc.). Generally a large object in a very limited space is affected. Natural disasters often greatly exceed technological disasters caused by industry or transportation in their capability to cause massive loss of life. Indeed the scale of energy release that is possible in nature – in cyclone, flood, volcano or large earthquake (which may be equivalent to hundreds of atomic bombs) – still far outstrips any human-made source of energy. Drought and related famine have been the greatest killers of the 20th century. Among the so-called rapid onset disasters, floods and earthquakes are the world's severest hazards, both in frequency and lethality. Storms, including cyclones and tornados come close [UNDP, 1994].One particular problem with natural systems is the scarcity and uncertainty of the input data due to the unique character and non-repeatability of most natural disasters.In spite of these different characters, basically the same procedure can be used to analyse the risks of both technical and natural systems. In principle, all the methods developed for technical applications can also be used for the analysis of natural risks. However, because of the scarcity and uncertainty of the input data about natural disastrous events, it is of special importance for the analysis of natural risks to have suitable technique available for the enlargement of the databases, for the utilisation of fuzzy information and for pooling and calibrating data.

Introduction: General Principles of Risk Analysis

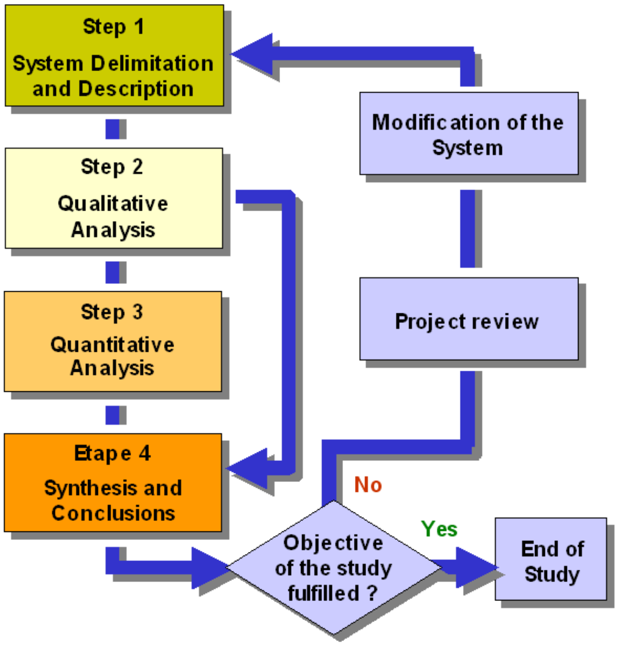

Step 1
System Delimitation and Description
Step 2
Qualitative Analysis
Step 3
Quantitative Analysis
Etape 4
Synthesis and Conclusions
Modification of the System
Project review
No
Yes
Objective of the study fulfilled ?
End of Study

Figure 6
General iterative scheme of a risk analysis study

As a general rule, a risk analysis study should more or less follow the iterative scheme presented on Fig. 6, which comprises four main steps:

- System delimitation and description (system definition):
  - collection of information
  - definition of the system and of its environment
  - breaking down of the system (components)
- Qualitative analysis:
  - definition of the objectives of the analysis
  - definition of the limits of the analysis
  - choice of analysis method(s)
  - analysis of the causal, functional and spatial relationships between the different components of the system
  - modeling of the system and its behavior
  - determination of the pertinent safety flaws (system & components vulnerability)
  - first lessons learnt
- Quantitative analysis:
  - quantitative assessment of the risks incurred by the system and its components (using appropriate input data)
  - sensitivity study (data uncertainties)
  - lessons learnt
- Synthesis and conclusions

Introduction: System definition

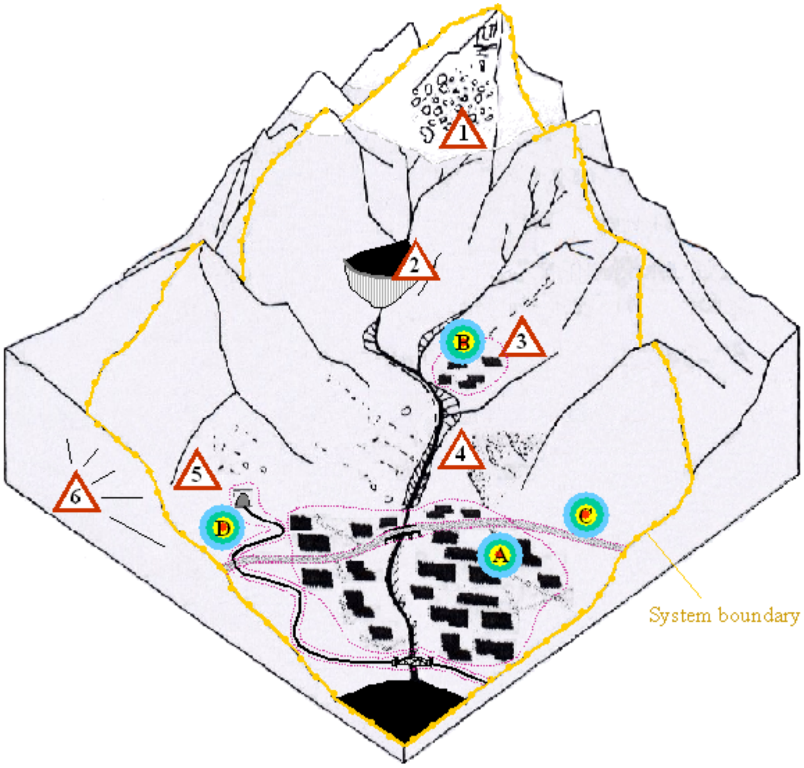


Figure 7
Example (imaginary): "*Cindynia Valley*" *
* from the Greek word « *kindynos* » (*kindynos*) meaning "danger"

1. Avalanche	2. Flooding	3. Debris flow
4. Landslide	5. Rock fall	6. Earthqauke

As it is generally the case in every scientific investigation, the first step in a risk study is to precisely delimitate and describe the system under scrutiny.

This operation aims at:

a/ well defining the physical limits of the system (boundaries, what belongs to it and what belongs to its environment)

b/ defining the same way the conditional (e.g. precipitation level) and thematic (e.g. type of damages) limits considered in the study

c/ allowing to disaggregate the global system in more elementary - and thus more easily manageable - elements (elementary systems, subsystems, components) and to precise their functionalities, characteristics and relationships

In the Fig. 7 example, such elements could be:

- the mountain
- the runnel
- the dam
- the lake
- the build-up area (A)
- the hamlet (B)
- the road (C)
- the railway (D)

The way of carrying out this breaking down task depends on the purpose and type of the analysis; there is no unique disaggregating scheme for a given system

Introduction: System definition (cont.)

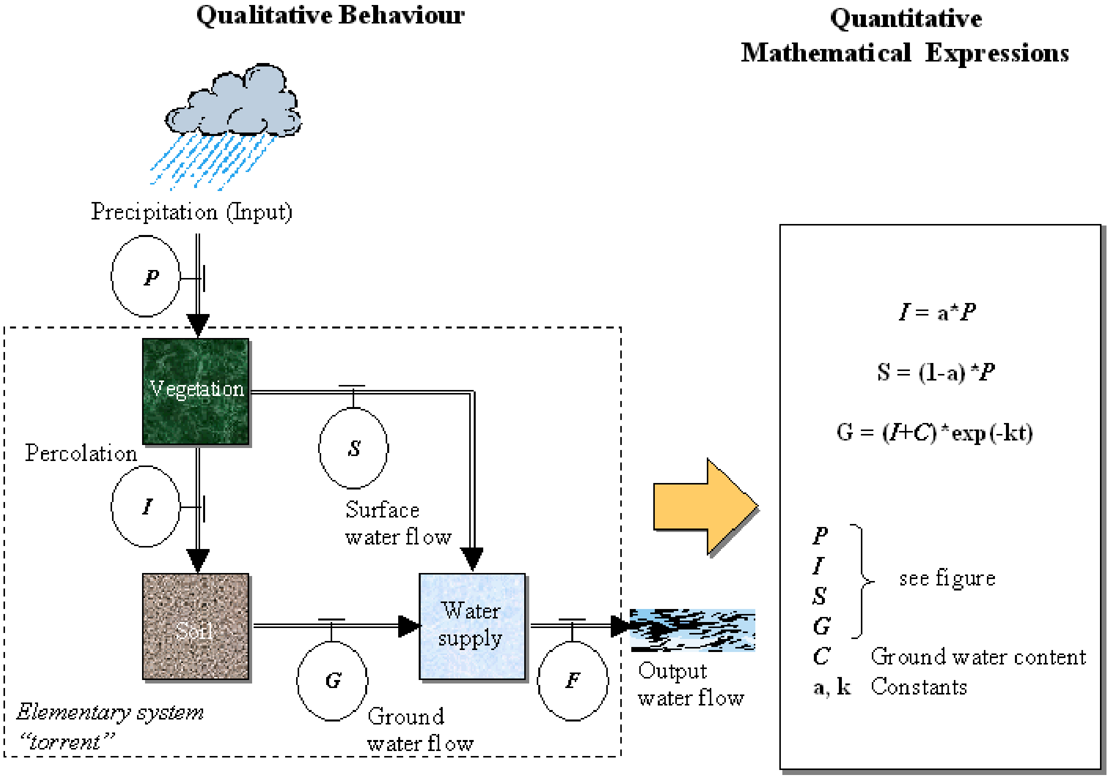


Figure 8 (adapted from [Hollenstein, 1997])Example of a simplified model for an elementary system ("torrent") drawing on the conclusion of the system definition task. In a first step, only a qualitative description of the behaviour of the elementary system is considered. In a second step, mathematical expressions are established to allow a more quantitative description of the behaviour of the system.

The system definition is the necessary foundation for further modelling of the system components (see example in Fig. 8). To avoid subsequent errors and reduce uncertainties, this initial task should be carried out with great care.

The description of the system doesn't consist solely in the delimitation of the "investigation perimeter"; it has as more central objective to make explicit the functionalities of the different part of the system and the reciprocal influences of the ones to the others.

The description of the system in the form of an object-attribute structure can additionally help to better organise the data for the next steps of the risk analysis. It is worth noting however that deterministic modelling and clear-cut delimitation of system and components are generally more difficult to achieve in the case of natural processes than in the case of industrial complexes. Models relative to natural processes are often of a very empirical and highly integrated form (so-called blackboxes). The description of the system must take this fact into account, in the sense that it would be useless to push it too far in the details if input data are anyhow not available to feed accor-dingly precise models. That’s why natural systems are rather defined in terms of elementary systems or subsys-tems than in components or pieces of components like it is the case for industrial systems.

Qualitative Methods:
Checklists, Preliminary Hazard List (PHL)

Figure 9 (sources: PLANAT, CREALP) PHL: identifying potential hazard sources

Qualitative methods aim at carrying out a first and rapid screening of the hazards that can threaten people or assets (Fig. 9). They are broad in scope and give only relatively rough information; the absolute intensity, or the relative contribution to the global risk, of the hazards thus identified cannot be obtained this way. On the other hand, they can be carried out without too great an analytical effort and without precise and detailed knowledge of the system under study.

In qualitative methods, the hazards identification usually draws on lists of keywords that describe possible dysfunction states of the concerned system. This is of course not really relevant for natural systems, but the hazards inventory can nevertheless be based on tables of the kind given below (adapted to the case of the “Cindynia Valley”, see Fig. 7):

General Hazards	*Sources*
Avalanche	Held snow masses
Flooding	Held water masses
Debris flow	Running waters
Landslide	Instable ground
Rock fall	Loose rock masses
Earthquake	Colliding tectonic plates

The result of such checklist consultation is an enumeration as exhaustive as possible of potentially dangerous events. The advantages of this approach are its easiness of execution, its large domain of application and its fast carrying out. Its drawbacks are its susceptibility to omissions, its dependence on prior system knowledge from the analyst and other involved people, and the lack of quantification of its results

Qualitative Methods:
Preliminary Hazard Assessment (PHA)

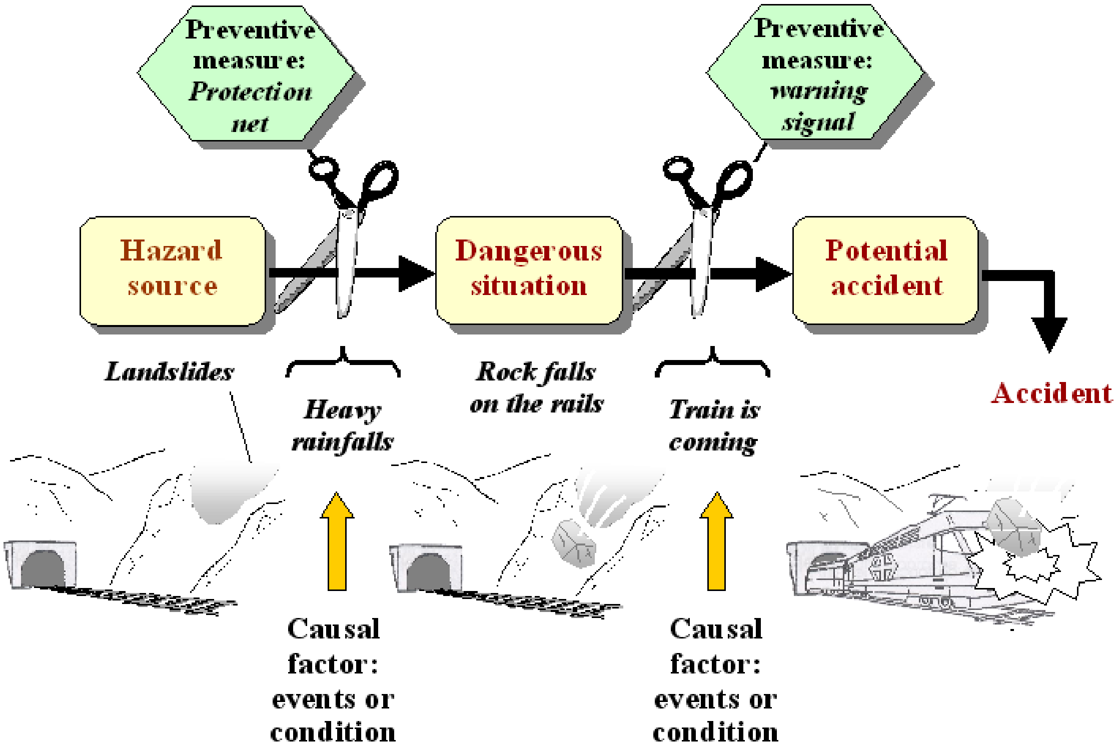

Preventive measure: *Protection net*
Preventive measure: *warning signal*
Hazard source
Dangerous situation
Potential accident
Landslides
Heavy rainfalls
Rock falls on the rails
Train is coming
Accident
Causal factor: events or condition
Causal factor: events or condition

Figure 10 PHA principle and example (railway in the “Cindynia Valley”)

The Preliminary Hazard Assessment method is an inductive approach that broadens to some extent the scope of the checklist process.

The results of a PHA are presented in a table form, with typical headings such as:

Hazardous Source: A description of the hazard and/or undesired or unacceptable occurrence

Causal Factor 1: A description of why or how the hazard may result in a mishap (events or condition leading to a dangerous situation)

Dangerous situation: A description of the situation that may lead to a potential accident when a hazard source exists

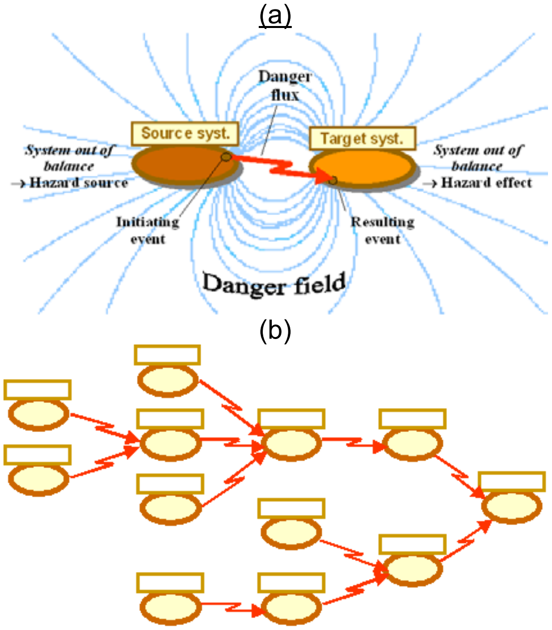
Causal Factor 2: A description of why or how the dangerous situation may degenerate in a potential accident

Potential accident: How the system, subsystem, environment, community or persons could be hurt

Comments: Preventive measures recommendation, applicable codes, standards, or regulations

- Contrary to the checklist approach, the PHA is not only interested in the constituent parts of the system but also in its potentially dangerous states and corresponding possible correcting measures (Fig. 10). The anticipating character of the PHA is interesting for natural systems when for example possible future land uses have to be analyzed. The susceptibility to omissions, the main drawback of the checklist approach, is however by no means improved with the PHA method.

Qualitative Methods: Danger “Source ▸ Flux ▸ Target” Model (MOSAR)



(a) (b) Figure 11 Danger “Source ▸ Flux ▸ Target” reference model (a) and chaining principle (b) (inspired from [Périlhon, 1999])

The use of a reasoning scheme based on the chaining of events structured as danger “source ▸ flux ▸ target” triplets (MOSAR-type model, [Périlhon, 1999]) can greatly help identifying the risks incurred by different objects at risk in a given geographical area (the “system”) presenting multiple potential hazards (Fig. 11).

To establish this type of model, one considers as danger flux any undesirable “transaction” of a system or subsystem with its environment and as danger field the active environment showing fluctuations susceptible to put the system or subsys-tem out of balance.

The origin of a danger is called the source system and the part influenced by the danger flux, the target system (object at risk, which represent people, buildings or other elements that could be affected by the hazard should this last one occur).

It should be noted that the element thus put out of balance (hazard effect) can in its turn become a source of danger for another part of the system (transforming this way the target system into a source system); this gives rise to the chaining phenomena of undesirable events called a danger scenario.

In the Cindynia Valley, such a chain could for example originate with a landslide as source of danger giving rise to a fall of rock material (danger flux) in the lake behind the dam (target system). The resulting overtopping of the dam will transform this one into a new source of danger possibly leading to a downstream flooding affecting the built area (new target system).

Semi-Quantitative Methods: Failure Mode Effect and Criticality Analysis (FMECA)

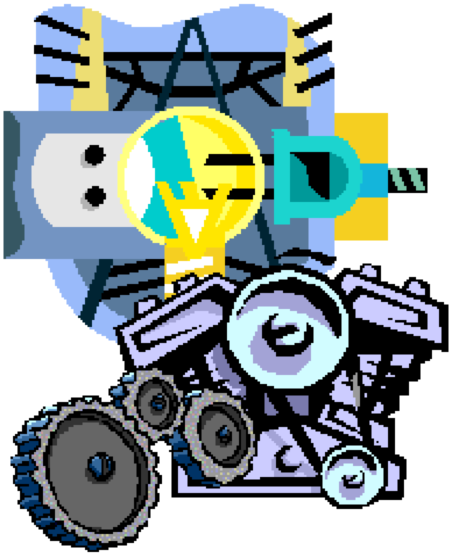


Figure 12 FMEA or FMECA, a component-oriented approach

A Failure Mode Effect Analysis (FMEA) is an inductive analytical technique used to assure that, to the possible extent, all potential failure modes and their associated causes/mechanisms have been considered and addressed. A failure mode is the particular way a given failure manifests itself (e.g. failure to open, failure to close, failure to continue to operate, etc.). In the industrial domain, the FMEA is a systematic process conducted at the component or subsystem level (Fig. 12) for evaluating how a design process or service may fail and identifying the actions to proactively eliminate or minimize the probability of failure or the effects of (inescapable) failures. It is an ongoing process that should start as part of the first Design Review and continue throughout the life of the product.

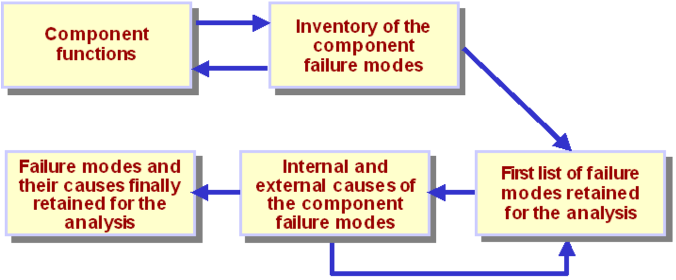
The FMEA is basically of a qualitative nature, but it becomes a semi-quantitative method (FMECA) when in addition some rough criticality assessment (evaluation of the frequency of occurrence and of the severity of the failure) is carried out. Such rough criticality assessment is often made according to the following grid scheme:

Severity/Occurrence	Very rare	Rare	Average	Frequent
IV Catastrophic				
III Critic				
II Significant				
I Minor				

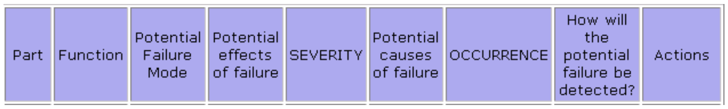
NASA invented the FMEA method early in the US Apollo space program. NASA created the tool to alleviate the stress between two conflicting mottos; "failure is not an option" and "perfect is the enemy of good". The first meant successfully completing the mission and returning the crew. The second meant that failure of at least some components was recognized unavoidable; the job was to predict them, prevent them when possible, plan for them, and build in the ability to overcome failures. FMEA is today largely used by design engineers. It is a simple concept although demanding in application. This method is frequently selected whenever a detailed analysis involving fault trees (see section 5.2) or event trees (see section 5.3) is not required.

Semi-Quantitative Methods: Failure Mode Effect and Criticality Analysis (cont.)

a)


Component functions
Inventory of the component failure modes
First list of failure modes retained for the analysis
Internal and external causes of the component failure modes
Failure modes and their causes finally retained for the analysis

(b)



Part	Function	Potential Failure Mode	Potential effects of failure	SEVERITY	Potential causes of failure	OCCURRENCE	How will the potential failure be detected?	Actions

(a) (b) Figure 13 FMEA-process block flow diagram (a) and typical table of results headings (b)

In essence, in a FMEA (or FMECA) every function and every component of the system under consideration is subjected to investigation (and where feasible testing) to discover potential failure modes (see Fig. 13 a).

The failure modes are function of the considered component. Every component has generally numerous potential failure modes and, theoretically, there is no limit as to the depth one could go in the analysis. Practically, there is a point of diminishing returns where the added cost exceeds the benefits derived. It is OK to combine similar failure modes if they have the same effect, they can always be later separated for finer resolution if necessary.

The advantage of the FMEA or FMECA lies in its explicit and systematic consideration of the effects of potential failure modes. It is not only looked for the circumstances in which the system will continue to be able to fulfill its function(s) but also for the various consequences of possible malfunctions of its components. When dealing with natural risks, an obvious drawback of this approach is the difficulty in such context to assign a clear signification of the concept of failure modes. A FMEA analysis can be carried out with spreadsheets and flow charts. Results are generally given under the form of a table with appropriate headings (see example in Fig. 13 b). A short example of a FMEA results table for a water-flow regulating device is given below [Hollenstein, 1997].

Part	Function	Failure mode	Danger. situation	Cause of failure	Potential effcts	Potential conseq.	Actions
Regul. Device	Power supply	Power cut off	Regul. imposs.	High water	No water retention	Village flooding	Install battery
	Software	Oper. error	Inacurr. regul.	Code error	Too high water flow	Village flooding	Test the software

Semi-Quantitative Methods: Hazard and Operability Study (HAZOP)

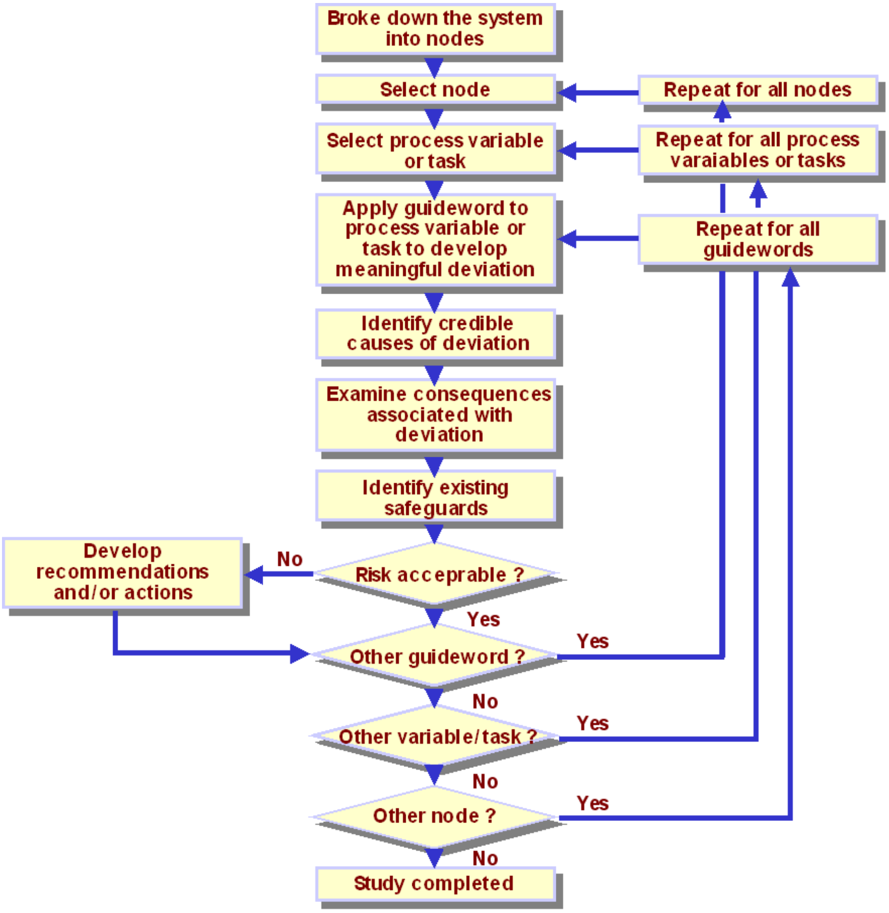

Broke down the system into nodes
Select node
Repeat for all nodes
Select process variable or task
Repeat for all process varaiables or tasks
Apply guideword to process variable or task to develop meaningful deviation
Repeat for all guidewords
Identify credible causes of deviation
Examine consequences associated with deviation
Identify existing safeguards
Develop recommendations and/or actions
No
Risk acceprable ?
Yes
Other guideword ?
Yes
No
Other variable/task ?
Yes
No
Other node ?
Yes
No
Study completed

Figure 14 HAZOP-process block flow diagram Example:GuidewordPossible deviation

Guideword	Possible deviation
No	No discharge available
Less	Less snow cohesion
More	More rainfalls
Too much	Too much sediment deposition
Too little	Too little retention capacity
Reverse	Reverse order

The HAZOP method was initially developed for the particular needs of the chemical process industry; it is a widely used technique for identifying unsafe deviations from design intent and assessing their potential consequences, and is fully recommended by legislators, regulators, insurance companies and other professional institutions.

The analysis should be carried out by a team having a broad knowledge of the system and its operation; it aims at establishing the hazardous states or conditions and their effects by means of a methodical examination of the system and its elements. To this end, an agreed checklist containing guidewords relevant to the system should be compiled prior to the analysis. The purpose of the guidewords list is to help identifying how deviations from the design intent can occur in the system, and whether the conse-quences of these deviations can result in hazard. The guidewords are simple expressions such as : “No”, “More”, “Less”, “As well as”, “Reverse”, “Other than”. They are applied to parameters (process variables) – e.g. Flow, Temperature, Pressure, Composition, etc. - that will depend on the type of process being considered, the equipment in the process and the process intent.

HAZOP focuses on specific portions of the process called “nodes”. A process parameter is identified, say “flow” and then combined with a guideword, e.g. “no”, to give a possible devia-tion (in this example: “no flow”). One looks then for the credible causes and consequences of the identified possible deviation. This process is repeated for all nodes, parameters and guidewords (see Fig. 14). Final recommendations include design, operating, or maintenance changes that will reduce or eliminate unsafe deviations, causes and/or consequences. The method can be made semi-quantitative by using a Risk Ranking Matrix, with estimated severity and likelihood rankings for each identified hazards.

Contrary to the FMEA, the HAZOP method does not require the systematic study of all the failure modes of the system but rather focuses on “failure events”. It is however not always straight-forward to attribute a well delimited part of the system to each couple “guideword-parameter”, which could lead to errors in the analysis or to the risk of overlooking complex events chains.

Quantitative Methods: Success Path Analysis (SPA)

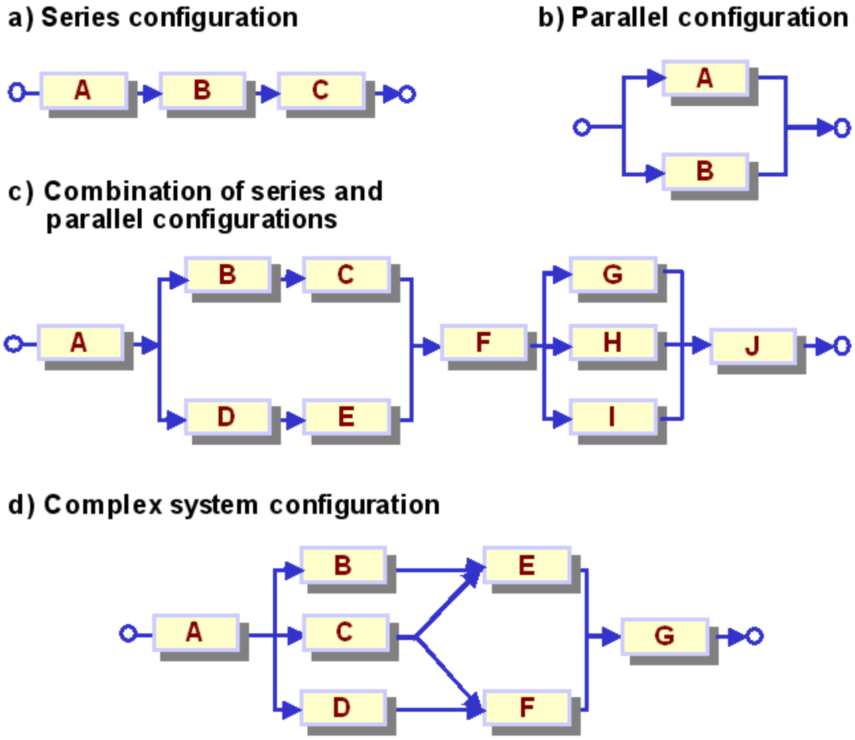

a) Series configuration
A
B
C
b) Parallel configuration
A
B
c) Combination of series and parallel configurations
B
C
A
F
G
H
J
D
E
I
d) Complex system configuration
B
E
A
C
G
D
F

Figure 15 SPA, basic reliability blocks configurations

The SPA method is a drawing and calculation tool used to model relatively complex systems. To this end, the different components of a system are symbolized as individual graphic and functional elements, called “reliability blocks” (for this reason, in its industrial applications this method is also known under the name of “Reliability Block Diagram”, or RBD, method). These blocks are reliability-wise arranged and related, often, but not necessarily, in the same way that the corresponding components are physically connected. Once the blocks are properly configured, and reliability data for these blocks is provided, calculations can be performed in order to calculate the failure rate, the “mean time between failure” (MTBF), reliability and availability of the system.

The simplest and most elementary types of reliability blocks configurations are the series and active-parallel configurations. Items connected in series must all work for the system to fulfil its function (“success path”). In the example of figure 15 a, the system will fail if either A, B or C fails. Items placed in parallel are considered to be redundant, because the good working of only one of them is enough for the system to function. In the example of figure 15 b, either A or B (but not A and B simultaneously) can fail and the system will continue to function.

The reliability of a system of N independent components, all in series or all in active-parallel, can respectively be calculated from the following mathematical expressions (Ri: reliability of component i, assumed to be known) [McCormick, 1981]:

$$R_{sys}(t)=\prod_{i=1}^{N} R_i(t) \qquad \text{(series)}$$

$$1-R_{sys}(t)=\prod_{i=1}^{N}\left[1-R_i(t)\right] \quad \text{(active-parallel)}$$

These two elementary configurations form the basis of the reliability block diagram construct and success path analysis.

Quantitative Methods: Success Path Analysis (cont.)

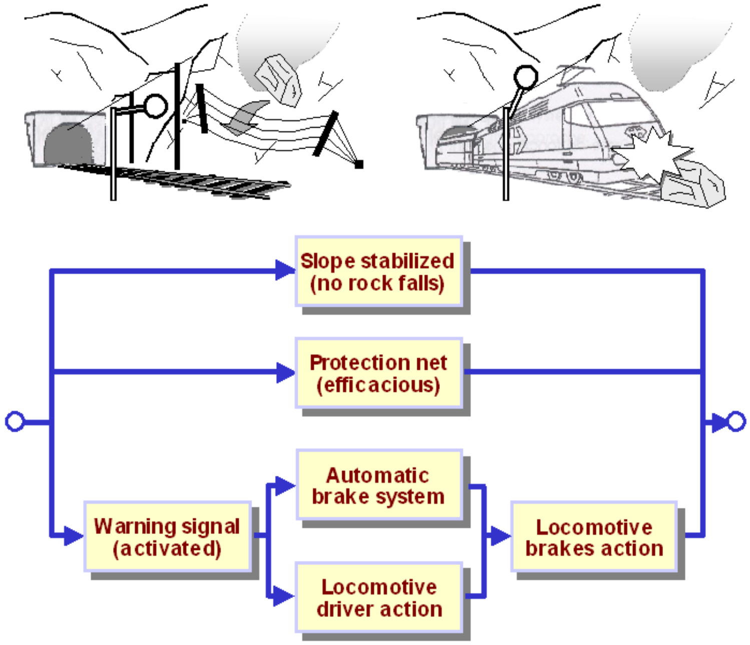

Slope stabilized (no rock falls)
Protection net (efficacious)
Automatic brake system
Warning signal (activated)
Locomotive brakes action
Locomotive driver action

Figure 16 SPA example (“Cindynia Valley” Railway)

The above construction and calculation scheme can be expanded further, as shown in figure 15 c, with various combinations of series and parallel configurations in the same diagram.

Not all systems however can be represented by simple combinations of blocks connected in series or active-parallel. “Complex” block diagrams of the type shown in figure 15 d require more advanced analytical treatment. A method for determining the reliability of such systems is the “decomposition method”, which is an application of the law of total probability. It involves choosing a “key” component and then calculating the reliability of the system in two steps: assuming first that the key component fails, and then that it succeeds. These two probabilities are then combined (multiplied by the respective probabilities of failure or success of the key component, and then summed) to obtain the reliability of the system, since at any given time the key component can only fails or operates properly (mutually exclusive states).

It is also possible to introduce alternative forms of redundancy such as the redundancy known as k-out-of-n redundancy for example. A k-out-of-n redundancy requires that k out of the n possible parallel success paths must work for the system to function.

Figure 16 shows a very simple example of a block diagram (series/parallel) in a natural risk analysis context.

Quantitative Methods: Fault Tree Analysis (FTA), basic principles

Figure 17 FTA first applications (1960s / 1970s): reliability studies of the “Minuteman” missile launching system and probabilistic safety assessment (PSA) studies of light-water nuclear power plants (“Rasmussen report”, WASH-1400)

Fault tree analysis is a top-down approach to the identification of process hazards. It is acknowledged as one of the best methods in complex system design, development, and operation for systematically identifying and graphically displaying the many ways something can go wrong.

The FTA method was originally developed in the U.S.A. in the early 1960s to evaluate and improve the reliability of the “Minuteman” missile launching system. It has since then largely been used in the aerospace, nuclear, and transportation industries for reliability or safety studies.

FTA is a deductive analysis method that begins with the consideration of an undesirable event. This undesirable event at the system level is referred to as the top event. It generally represents a system failure mode or hazard for which the occurrence probability is not directly available, but required. Based on a set of rules and logic symbols from probability theory and Boolean algebra, FTA then uses a top-down approach to generate a logic model that provides for both a qualitative description of the failure paths and a quantitative evaluation of the top event occurrence probability. The approach consists in defining successive levels of subordinate failure events (intermediate events), each level going a step deeper in the explanation of the possible causes of the failures identified at the preceding level. The intermediate events at a given level are linked to the events at the immediately superior level by logical connective functions. This let us construct in a very systematic way a complete event tree structure representing the various possible failure paths leading to the occurrence of the top event. When a contributing failure event does not need to be divided further, because its failure rate is known or readily available, or it is decided to limit further analysis of a subsystem for practical reasons, the corresponding branch of the tree structure is terminated with a basic event.

The basic event for a branch is termed a primary fault event if the corresponding subsystem failed because of a basic mode such as a structural fault, or failure to open or close, etc. It is a secondary fault if the subsystem is out of tolerance so that it fails because of excessive operational or environmental stress placed on it.

Quantitative Methods: Fault Tree Analysis (FTA), logical gates and symbols

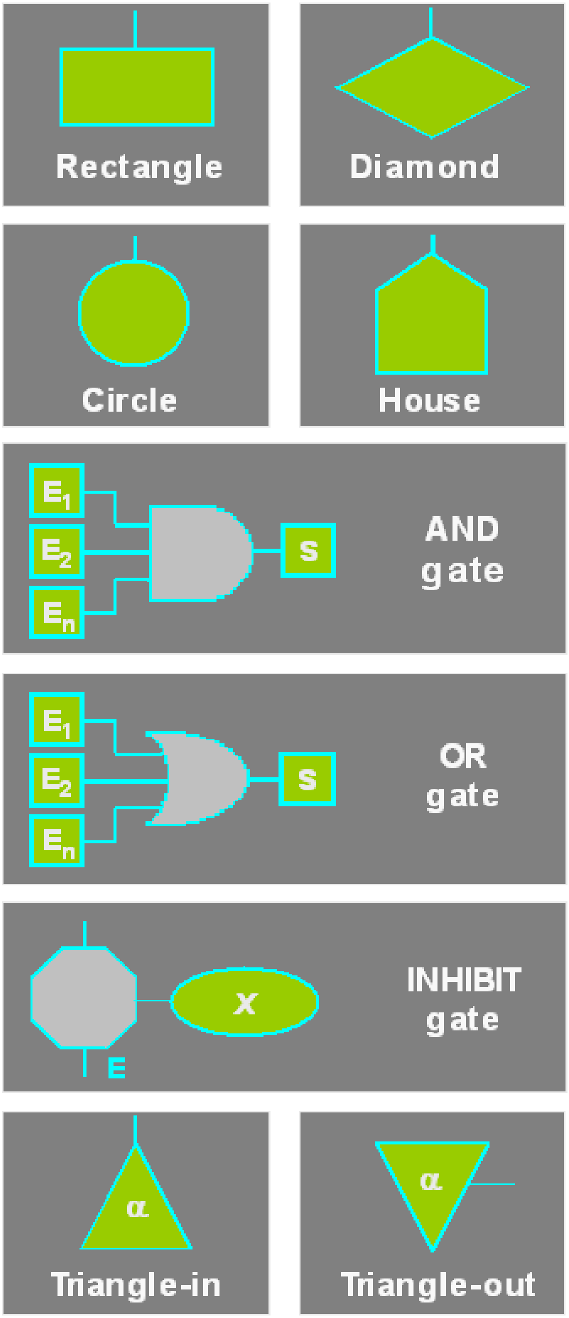


Figure 18 Symbols most commonly used in the graphical representation of fault trees

Synthesis of the fault tree is represented graphically by using logical gates and other appropriate symbols. The symbols most commonly used in FTA are presented in figure 18 and explained below [McCormick, 1981].

Event Symbols:

- *Rectangle* Event; generally result of the logical combination of “lower level” fault events
- *Circle* Basic “terminal” event (assumed to be independent)
- *Diamond* Fault event not fully developed as to its causes; it is only an assumed basic event
- *House* Event normally occurring in the operation of the system; it is not a fault event

Logical Gate Symbols:

- *AND* gate The output event occurs if and only if all the inputs occur (Boolean intersection operation “∩” of the input events)
- *OR* gate The output event occurs if one or more of the inputs occur (Boolean union operation “∪” of the input events)
- *INHIBIT* gate Output exists when the input event E exists and the condition *X* is satisfied; this gate functions somewhat like an AND gate and is used for a secondary fault event E.

Subtree Symbols:

- *Triangle-in* Triangle symbols provide a tool to avoid repeating sections of a fault tree, or to transfer a subtree construction from one sheet to the next. The triangle-in appears at the bottom of a tree structure and represents that branch (subtree) of the tree (in the example: “A”) shown someplace else
- *Triangle-out*The triangle-out appears at the top of a subtree and denotes that the corresponding tree structure (“A” in the example) is a subtree to one shown someplace else

Quantitative Methods: Fault Tree Analysis (FTA), fault tree construction

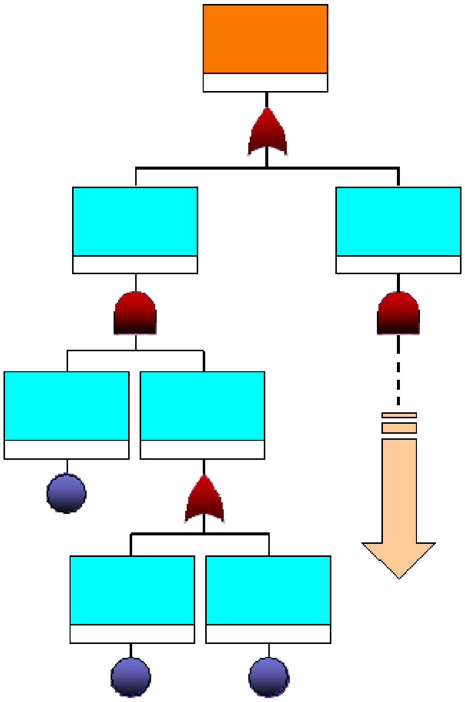


Figure 19 Fault tree construction scheme: from top event to basic events

The first step in fault tree construction is the selection of the top failure event (orange box in Fig. 19) that is to be the subject of the analysis. Because the top event sets the tone for the series of questions that are considered when constructing the fault tree, this event must be precisely stated and be narrow in scope (example: rail blocking and not landslides). If a top event is too vaguely stated, the fault tree is likely to be large, complex, and unfocused. Specifying in the description of the top event the specific mission phase or portion of the mission to which it applies often helps to generate a very concise fault tree.

The next step is to identify the “immediate, necessary and sufficient” (INS) contributing events (light-blue boxes in Fig. 19) that may directly cause the top event to occur. Once the first level of intermediate (INS) contributing events has been established, each branch is examined to decide whether it needs to be further detailed. This deductive process continues until all branches have been terminated by independent basic events.

During this fault tree construction, consistently applying the appropriate nomenclature to events is critical to identifying the same event in multiple fault tree branches. If, for example, a given event is named differently in another branch of the fault tree, cutset analysis, which is described in the "fault tree evaluation" page (5.7), identifies multiple events leading to different failures, rather than the same event leading to different failures. Such a nomenclature error can hide the fact that the event in question is a major contributor to the top event and thereby improvements or controls for it will fail to be recommended by the analyst. Similarly, when two identical components are installed in different locations within a system, they must be identified as physically different components by using distinct designators in the nomenclature. Otherwise, cutset analysis identifies how the same component-type failure contributes to several scenarios when the failures are actually caused by different components.

Quantitative Methods: Fault Tree Analysis (FTA), fault tree construction (cont.)

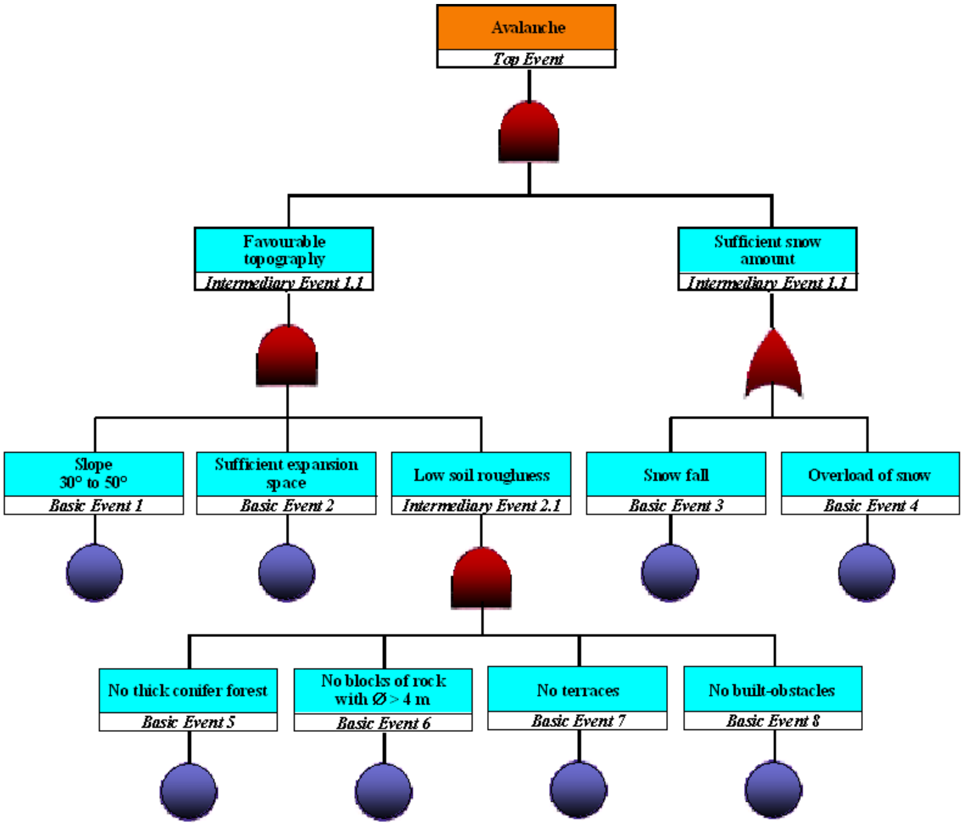


Figure 20 Example of a fault tree for an undesirable natural top event (avalanche in “Cindynia Valley”)

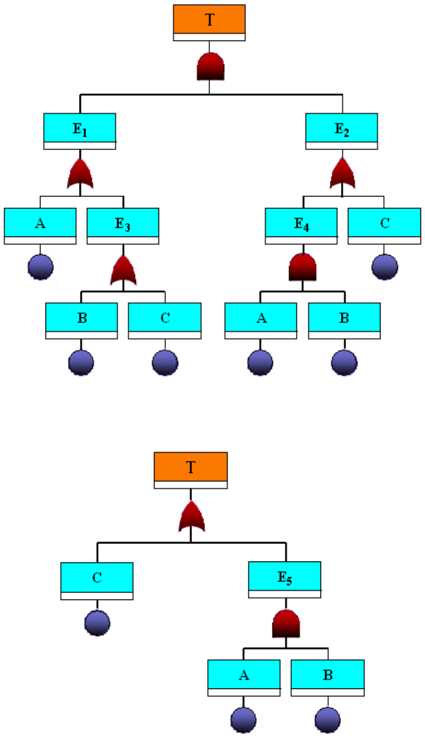
To construct a useful fault tree, the analyst must have a good knowledge of the system components dependencies and interactions, as well as of their reliability parameters and the conditions that determine the components that are considered to have failed.

Fault trees arranged by scenarios (rather than by subsystems, which can fail to correctly take the interface and integration of the system into account) often uncover complex relationships and interactions of systems, components, and actions that are believed to be unrelated. For example, such an FTA can reveal a single-point component failure that can fail two supposedly redundant or independent systems.

Construction of fault trees is an art as well as a science and comes only through experience; the following guidelines are however helpful (from [Lambert, 1973]):

- rule # 1: no “gate-to-gate” relationships, i.e., put an event statement between any two gates;
- -rule # 2: “complete the gates”, i.e. identify all the input events of a logical gate before to start the detailed analysis of one of them;
- -rule # 3: “causes are anterior to consequences”; this rules allow the elimination of certain causes and branches of the tree, facilitating the resolution of so-called “looped systems”;
- -rule # 4: “expect no miracles”; those things that would normally occur as the result of a fault will happen, and only those things!

Quantitative Methods: Fault Tree Analysis (FTA), fault tree evaluation


a) Original fault tree

b) Reduced fault tree

Figure 21 Fault tree reduction process (example from [Villemeur, 1988])

Once all failures, events, and conditions that can lead to the occurrence of the top event have been properly identified, the resulting fault tree can be “translated” into a Boolean algebraic expression. In the example of figure 21, this gives (T = top event):

$$T = (A \cup B \cup C) \cap [C \cup (A \cap B)]$$

]The traditional analysis process is to generate next the system minimal cutsets. Cutsets represent combinations of events that cause the top event to occur. A cutset can be a single-point failure or event, or can be a set of many events. Different cutsets can include different combinations of the same event. A minimal cutset is the smallest group of events that cause the top event to occur. In large trees, the events that cause the top event to occur are often buried deep within the system and are not easily discovered without performing a cutset analysis. Generally (but not necessarily), the cutsets that have the highest probability of occurrence are the ones that are made of the fewest number of events. Minimal cutsets can be found by simplifying the Boolean expression of the top event, using the rules of Boolean algebra. The aim is to obtain a reduced expression made of the logical union of groups of events linked by “AND” logical connectors. By definition, these groups are the minimal cutsets looked for (because the simultaneous realization of each of the events of anyone of these group is a necessary and sufficient condition to cause the top event to occur). For the example of figure 21, this leads to:

$$T = [(A \cup B \cup C) \cap C] \cup [(A \cup B \cup C) \cap (A \cap B)] = \ldots = C \cup (A \cap B)$$

There are thus two minimal cutsets in this example: C and AÇB. This means that the original fault tree can be reduced to the much simpler tree structure given in figure 21 b.

The minimal cutset information obtained during qualitative analysis, together with information about the probability of occurrence of the basic events, can finally be used during quantitative analysis for computing the unavailability or unreliability values of the system. Assuming that the probability of occurrence of the events A, B, C in the above example are respectively: 0.1, 0.2 and 0.01, the probability of occurrence of the top event T becomes:

$$P[T] = 0.01 + (0.1*0.2) – [0.01*(0.1*0.2)] \cong 0.03$$

Quantitative Methods: Event Tree Analysis (ETA), basic principles

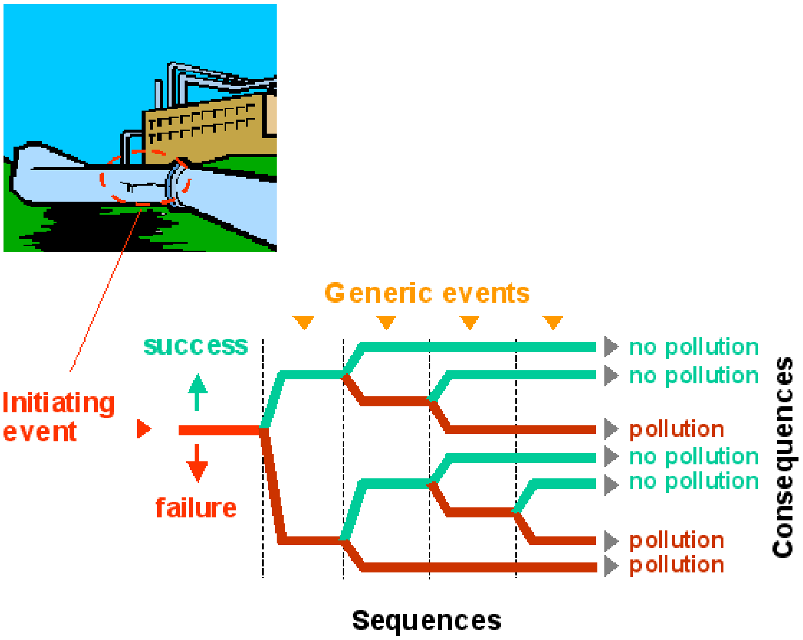


Figure 22 ETA, symbolic representation of an event tree, with the initiating event and the generic events sequences

An event tree is a graphical representation of the logic model that identifies and quantifies the possible outcomes following an initiating event. The consequences of the event are followed through a series of possible paths, involving success or failure of specific combinations of safeguard subsystems or conditions (generic events).The ETA method had originally been applied between 1972 and 1975 by the team of Prof. Norman Rasmussen of MIT in the assessment study of the risk of U.S. commercial light water reactors (WAH-1400 report, 1975). In combination with FTA, it has since then become a standard tool in the analysis of complex industrial systems of the most various types.

Event tree analysis provides an inductive approach to reliability assessment as they are constructed using forward logic. When the generic events exclusively concern decisions to be made after the occurrence of the generic event (human control), the event tree is rather called decision tree.Event trees can be used to analyze systems in which all components (subsystems) are continuously operating, or for systems in which some or all of the components are in standby mode – those that involve sequential operational logic and switching.In the case of standby systems and, in particular, safety and mission-oriented systems, ETA is used to identify the various possible outcomes of the system following a given initiating event which could be an unsatisfactory operating event or situation.

Quantitative Methods: Event Tree Analysis (ETA), event tree construction

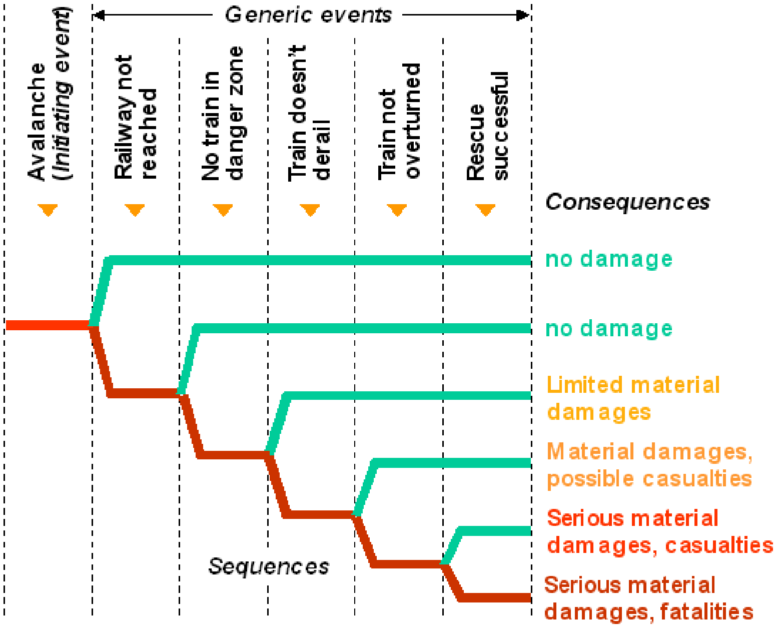


Figure 23 ETA, example of the construction of an event tree (avalanche threatening the railway of “Cindynia Valley”)

An Event Tree Analysis starts by identifying possible initiating events (generally, different event trees must be constructed and evaluated in the framework of the risk analysis of a given system), which could lead to an incident or accident. Such events disrupt normal system operation or condition. The identification of the initiating events can be based on experience, on a technical or scientific preliminary analysis of the system under scrutiny, or on the construction of a fault tree having as top event some general undesirable event considered at the level of the whole system.

After the initiating events have been agreed, all the generic events (subsystem operation, particular condition) that can possibly intervene following the occurrence of each initiating events and prevent an undesirable ending must in their turn be identified. The fate (success or failure) of these events is then examined to determine the sequences that can lead to unacceptable consequences (see example in Fig. 23).

Usually, only a two-state modeling (binary branching logic: complete success or complete failure) is considered. In some cases, it could be necessary to introduce a greater number of discrete states (partial failure states); a separate branch must then be included for each state.

Quantitative Methods: Event Tree Analysis (ETA), event tree evaluation

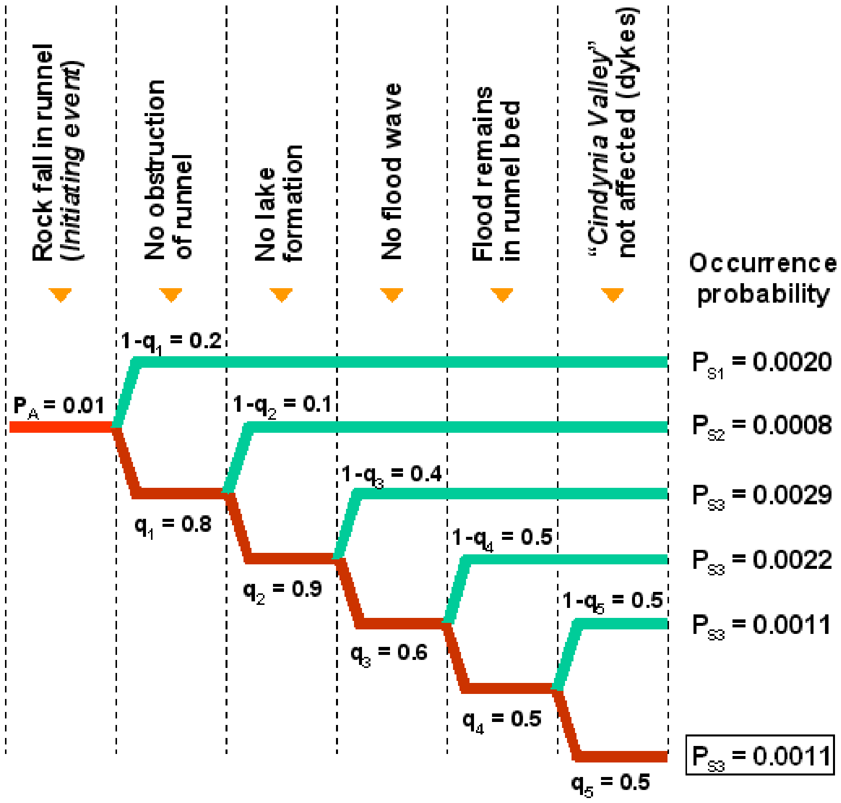


Figure 24 ETA, example of a quantified event tree (rock fall in the runnel of "Cindynia Valley")

The tree evaluation has for final goal the quantification of the sequences in order to allow the frequency (or probability of occurrence) of each of the outcomes to be predicted.

Prior to this operation, the initial (basic) tree must be reduced to its most elementary form. The reduction process in fact already takes place throughout the construction phase of the event tree. Three factors assist in simplifying the tree structure: timing, sequential and conditional dependencies. Taking the time into account allows considering only one arrangement of the generic events, which greatly reduces the number of sequences. For example, there are 25 = 32 sequences to study for a well-ordered binary tree of 5 generic events, but 5! times more, i.e. 3840 sequences, if the generic events can "a priori" be arranged in every possible orders. The dependencies between events allow to "prune" an event tree by eliminating the branches that have a zero conditional probability. This has been done in the examples of figures 23 and 24. For example, in figure 23 if the avalanche does not reach the railway, the failure branches for the following events become pointless.

When the branch point (generic) events are independent of each other, quantification of the diagram is trivial and is simply achieved by calculating the product of the frequency of the initiating event with the probabilities of passing along each branch leading to each outcome consequence (see example of Fig. 24). In principle, however, the system states on a given branch of the event tree are conditional on the previous states having already occurred (dependencies between the branch events). For example, in figure 24, the success or failure of the generic event “no obstruction of runnel” must be defined under the conditions that the initiating event - “rock fall” - has previously occurred (conditional probability).

Quantitative Methods: Event and Fault Trees combinations

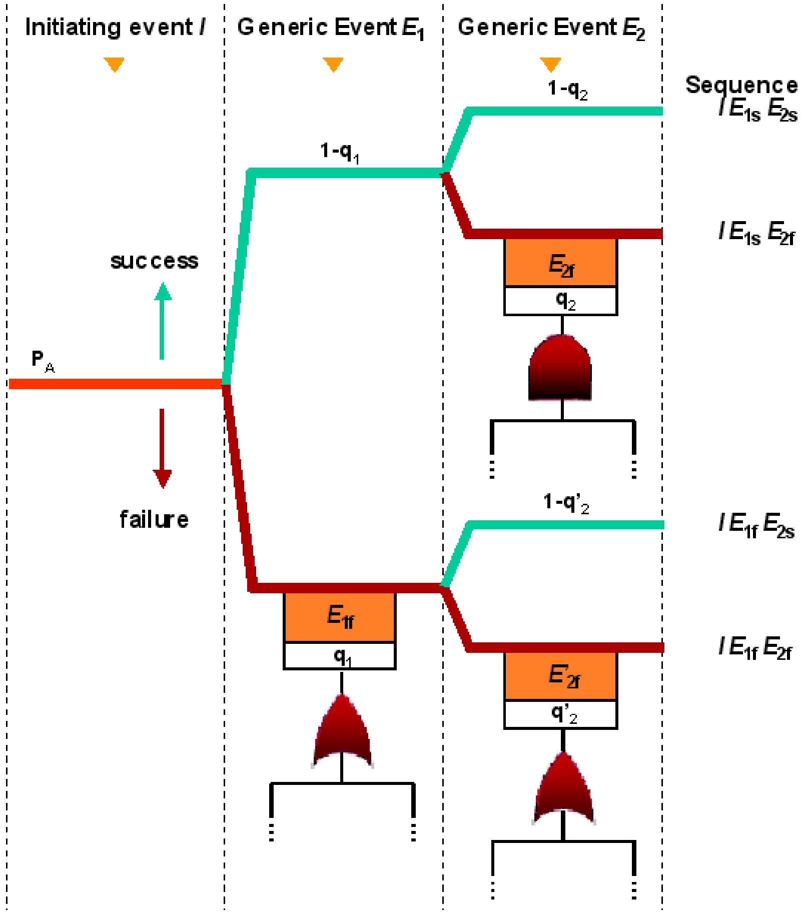


Figure 25 Schematic of an event tree with fault trees used to evaluate the occurrence probabilities of different generic events(adapted from [McCormick, 1981])

The quantification of the probability of passing along different branch points of an event tree become more complex when there are dependencies between the branch events. The quantification is then performed by quantifying a fault tree whose top event is defined as combination of occurrence and non-occurrence of the branch point events that have in turn been developed with fault tree structures (see example in Fig. 25).

It has moreover already been mentioned (page 5.9) that constructing a global fault tree is often a useful means to identify in view of an ETA the different initiating events that could lead to undesirable consequences for the system under study.

Quantitative Methods: Cause-Consequence Analysis (CCA), basic principles

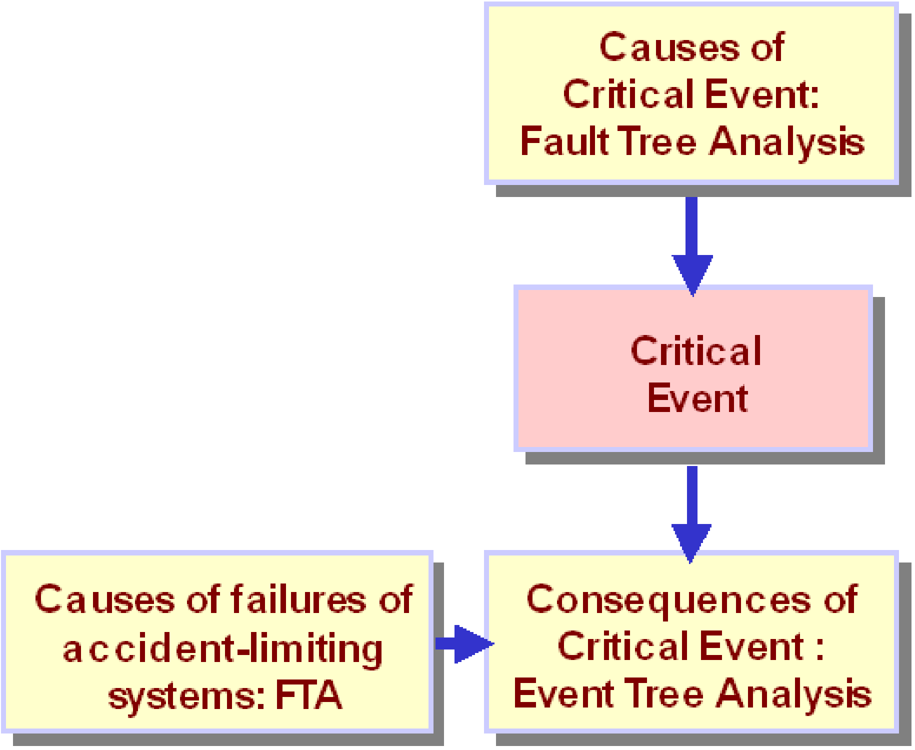


Figure 26 Basic structure of a Cause-Consequence Diagram

Cause-consequence analysis is a well-structured technique that combines cause analysis (described by fault trees) and consequence analysis (described by event trees). Thus, both inductive and deductive analyses are used in this approach.

This technique was initially invented by RISO Laboratories in Denmark to be used in risk analysis of nuclear power plants [Nielsen, 1971]. It was then adopted (and adapted) by other industries in the estimation of the safety of protective or other types of systems

The main principle of the CCA technique is based on the occurrence of a critical event, i.e. an event that disturbs the normal (and safe) behavior of the system under study. Once such critical event has been identified, all relevant causes of this event and potential consequences are developed using FTA (see pages 5.3 to 5.7) and ETA (see pages 5.8 to 5.10) conventional analysis methods. The FTA method is used in two independent situations to describe the causes of an undesired event. Firstly, this approach is used to precise the causes of the critical event. The second function for the FTA method is to clarify the causes of the possible failures of the accident-limiting subsystems. The ETA method is used as a link between the causes of the critical event and the various consequences that could result (see Fig. 5.26).

Like the FTA method, the CCA technique documents the failure logic, but has the extra capability of enabling the analysis of systems subject to sequential failures and the identification of the complete set of systems responses to any given initiating event   CCA is thus a method to explore time-sequenced system responses to initiating “challenges” and to enable probability assessments of success/failure outcomes at staged increments.

Quantitative Methods: Cause-Consequence Analysis (CCA), diagram construction

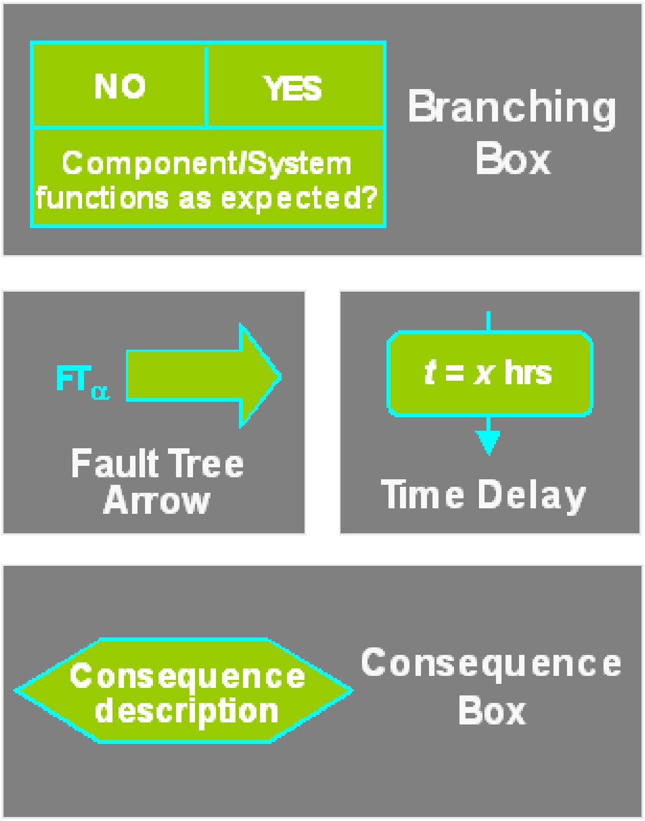


Figure 27 Specific symbols used for construction of a Cause-Consequence Diagram

Rules for the construction of a cause-consequence diagram can be classified in two separate classes: those for the cause part of the diagram and those for the consequence part of the diagram [Ridley and Andrews, 2001].

The rules and symbols used for the construction of the cause parts of the diagram are the same as those developed in the FTA section and will therefore not be repeated here. For the construction of the consequence part of the diagram some new symbols are required, which are shown in figure 27:

- the *branching box* represents a functionality condition to be fulfilled by a component/sub-system; output is “yes” if the condition is met, “no” if it is not met (note that the branching operator my be written in either fault or success domain);
- the *fault tree arrow* indicates under which designation (FT□ in Fig. 27) the fault tree corresponding to the undesirable fulfillment of the condition given in the branching box it points to can be found;
- the *time delay* is used to indicate that the following event in the diagram cannot occur before the time interval given in the symbol is elapsed;
- the *consequence box* represents the event/condition to which analysis of a particular sequence leads, with, usually, severity level stated.

Starting from the initiating critical event, the functionality of each component/sub-system is investigated and the consequences of the corresponding sequences determined. If the branching box is governed by a sub-system, then the probability of failure is obtained via a fault tree diagram.

If any branching box is found irrelevant, e.g. the boxes attached to the “No” and “Yes” branches are identical and their outcomes and consequences are the same, then these should be removed to reduce the CCA diagram to a minimal form (removal of these boxes will in no way affect the end result).

Quantitative Methods: Cause-Consequence Analysis (CCA), example

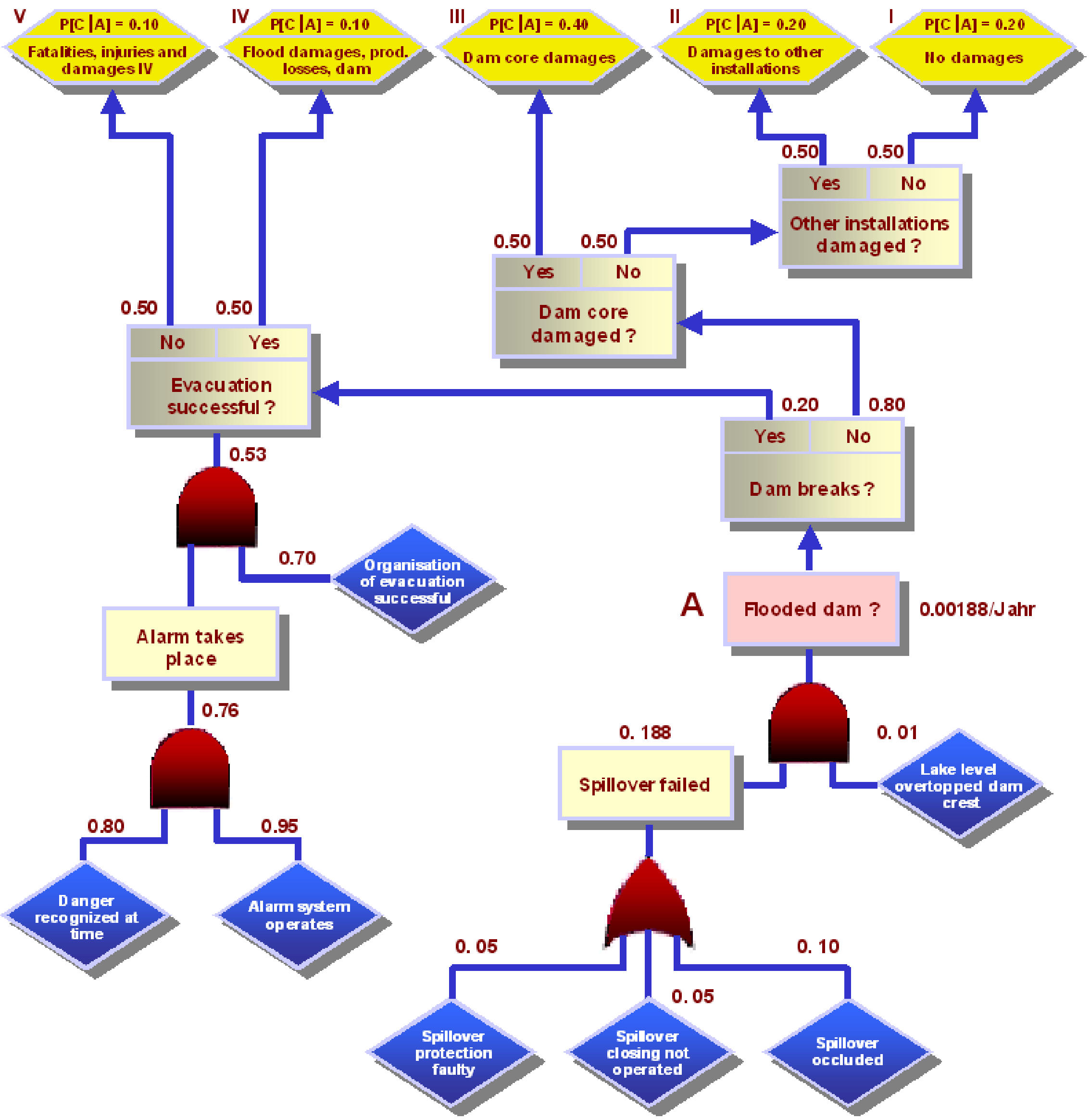


Figure 28 Example of a Cause-Consequence Diagram: dam overtopping due to excess of precipitations in the “Cindynia Valley” (adapted from [Grütter, 1985])

The figure 28 shows an example of a cause-consequence diagram. The critical event (A) consists in the overtopping of the dam of the “Cindynia Valley” due to excess of precipitations in the area. Interest is in the possible damages downstream of the dam, all the way down to the lowest parts of the valley.

The response is given by the event tree constructed on A with the help of the "Yes"7"No" interrogation character-rizing cause-consequence diagrams. In the upper part of the diagram, the possible consequences are presented in five boxes (I – V), each containing a possible consequence written in fuzzy terms.

Other Methods

The methods presented in the preceding pages are only a sample of the existing methods that can be used for safety/reliability assessments. Without in any way pretending to be exhaustive, some additional methods are presented very briefly below. Dynamic systems can be analyzed using Markov Modeling, GO Method, Dynamic Event Tree Analysis, etc.Markov Modeling is a classical modeling technique for assessing the time-dependent behavior of dynamic systems. The state probabilities of the system P(t) in a continuous Markov system analysis are obtained by the solution of a coupled set of first order, constant coefficient differential equations: $dP/dt = M \times P(t)$, where M is the matrix of coefficients whose off-diagonal elements are the transition rate and whose diagonal elements are such that the matrix columns sum to zero.The GO Method can be used to compute the probability that a system exists in each of a few states. The system being studied is modeled in the form of a "GO chart", which consists in selecting functional operators (or "building blocks") to represent each component and logical junction, and connecting them with arrows to represent the flow of information. The GO method can be considered a competitor of FTA.Dynamic Event Tree Analysis Method is an approach that treats time-dependent evolution of systems states, process variable values, and operator states over the course of a scenario. In general, a dynamic tree is an event tree in which branchings are allowed at different points in time. This approach is defined by five characteristics sets: 1) branching set, 2) set of variables defining the system state, 3) branching rules, 4) sequence expansion rules and 5) quantification tools. Monte Carlo Simulation can also be a useful general technique for risk analyses. First, the random numbers are sampled for each of the uncertain assumptions. Secondly, the random numbers obtained are used together with the other assumption values to perform the basic analysis.

Conclusions

Natural risks can in principle be analyzed with the same types of methods used in the analysis of technical or industrial hazards. In the natural risk assessment field, basically the same mechanisms are brought into play as in the case of other types of hazards.   The scientific approaches that can be used for the analysis of natural risk are thus potentially very numerous and varied. One single method can however very seldom “do the job” alone. It is the task of the risk analyst to select in each particular case the best combination of available methods and tools, based on his knowledge and acquired experience.It must nevertheless be noted that the operational application of formalized risk analysis methods is in the natural hazard field far to have become a routinely practice. In this domain, there is still place for extensive research and development studies.

Bibliography

American Chemical Society, 1998: *Understanding Risk Analysis*, Office of Legislative & Government Affairs, 1155 16th St. NW, Washington, DC 20036, U.S.A.

BUWAL, 107/I, 1999: *Risikoanalyse bei gravitativen Naturgefahren, Method*, Bundesamt für Umwelt, Wald und Landschaft, Dokumentation, 3003 Bern, Switzerland

CREALP, Centre de recherche sur l'environnement alpin, Etat du Valais, Suisse, site Web: http://www.crealp.ch/f_principal_close.html

Grütter F., 1985 : *Probabilitische Sicherheits- und Risikoanalysen für Talsperren*, in Risikountersuchungen als Entscheidunsinstrument, Verlag TÜV Rheinland

Hollenstein K., 1997: *Analyse, Bewertung und Management von Naturrisiken*, Diss. ETH Nr. 11878, vdf Hochschulverlag AG an der ETH Zürich, Switzerland

Lambert H.E., 1973: *System Safety Analysis and Fault Tree Analysis*, Lawrence Livermore Laboratory, Rep. UCID-16238

McCormick N.J., 1981: *Reliability and Risk Analysis, Methods and Nuclear Power Applications*, Academic Press, New York, London

Nielsen D.S, 1971: *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*, Danish Atomic Energy Commission, RISO-M-1374

Périlhon P., 1999: Logiciel MADS-MOSAR II, CD Rom version2.09, Ed.Fox Média, Grenoble

PLANAT, plate-forme nationale «Dangers naturels», Confédération Helvétique, site Web : http://www.planat.ch/f/index.htm

Ridley L.M. and Andrews J.D., 2001: *Reliability of Sequential Systems using the Cause-Consequence Diagram Method*, Dep. of Mathematical Sciences, Laughborough University, Laughborough, Leicestershire, LE11 3TU, Great Britain

UNDP (United Nation Development Programme), 1994: *Vulnerability and Risk Assessment*, Disaster Management Training Programme (DMTP), Module prepared by Cambridge Architectural Research Limited, The Oast House, Malting Lane, Cambridge, U.K.

Villemeur A., 1988: *Sûreté de fonctionnement des systèmes industriels*, Collection de la Direction des études et recherches d'Electricité de France, Editions Eyrolles, Paris

Wash-1400, 1975: *Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, Nuclear Regulatory Commission Rep. ("Rasmussen Report"), NUREG-75