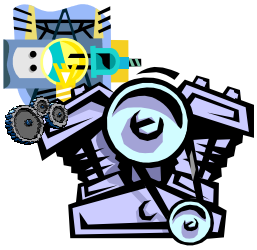
Chapter 4 Qualitative Systems Risk Analysis Methods

4.1 Introduction

The concept of "system"

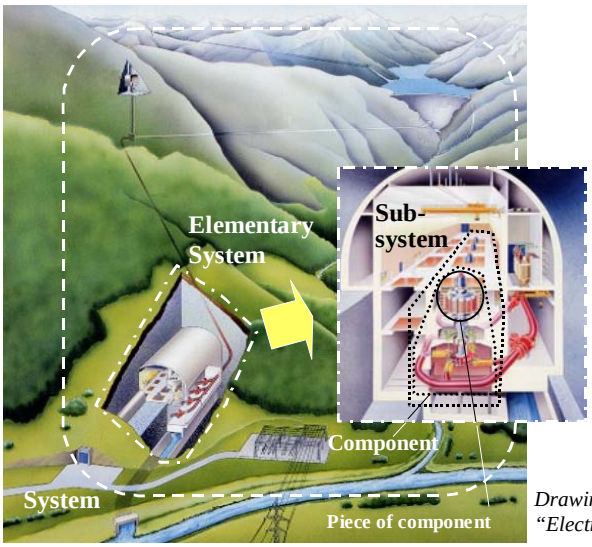


This chapter and the two chapters that follow are devoted to the presentation of methods that can be used for the risk analysis of (more or less complex) *systems*, i.e. well-defined devices, installations, or other physical entities, made of several interconnected or interacting discrete elements. "Well-defined" means that the considered system must be clearly identifiable, which is an obvious requirement. The fact that the system is made of interconnected or interacting elements means moreover that it is not simply equal to the sum, or juxtaposition, of these elements.

As in most scientific investigations, the first step in any risk analysis therefore consists in thoroughly delimitating and describing the system under scrutiny. This operation aims at:

- well defining the physical limits of the system (i.e. its boundaries, delimitating on one hand what belongs to it and on the other hand what belongs to its environment);
- specifying the same way the conditions and limits of the system study (knowing that a fully exhaustive study is rarely achievable because means and time at disposal are never unlimited);
- allowing to disaggregate the global system in more elementary, and thus more easily manageable (in particular with the techniques described in the preceding chapter), elements - hierarchically, and by increasing order of detail: elementary systems, subsystems, components, pieces of components - and to precise their functionalities, characteristics and relationships.

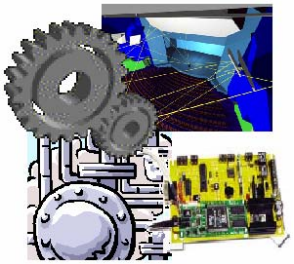
An example of such a system definition and disaggregating process is given in the figure 4.1



Drawing: "Electricité Romande"

Figure 4.1 ***Example of system definition and disaggregating process***

The way of carrying out this definition task strongly depends on the purpose and type of the analysis. There is no unique disaggregating scheme for a given system.



Systems can be of different nature:

- mechanical systems;
- thermal hydraulics systems (systems conveying fluids);
- electric or electronic systems, logic or analog systems, control systems;
- software systems, information systems.

In the definition of a system it is important to specify:

- the functions or missions of the system (main or auxiliary) and their degrees of importance;
- the structure of the system (its components, their roles, characteristics and performances; their relationships; their locations);
- the operating conditions of the system (operating states, configuration changes, etc.);
- the operational requirements (technical specifications, monitoring, periodical tests, maintenance) ;
- the environment of the system (other systems with which it interacts, human operators, natural environment).

In the framework of risk analysis, it should be noted that a system that has undergone some failure becomes strictly speaking a different system, with modified characteristics and behavior (for example, a nuclear power plant that loses one of its cooling loop cannot be considered as the same system anymore, because an additional failure for example could have in this case much more serious consequences). To not make things more complicated, this distinction is however generally ignored and we will continue in this situation to speak of “the system” as if it has remained the same.

The initial phase of a risk analysis is therefore an information-gathering task, which could be more or less tedious according to the system considered, the past experience of the analyst and the objectives of the study. It is followed by more risk-specific tasks as represented schematically in the figure 4.2.

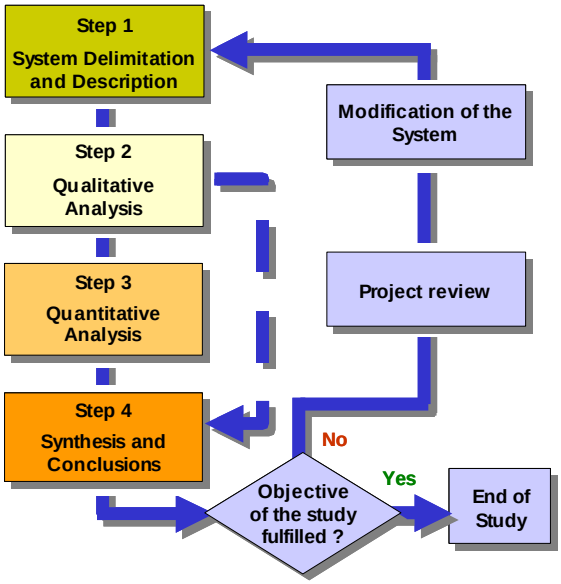


Figure 4.2 ***General iterative scheme of a risk analysis study***

Steps 2 and 3 include themselves various sub-tasks that are further detailed in the figure 4.3.

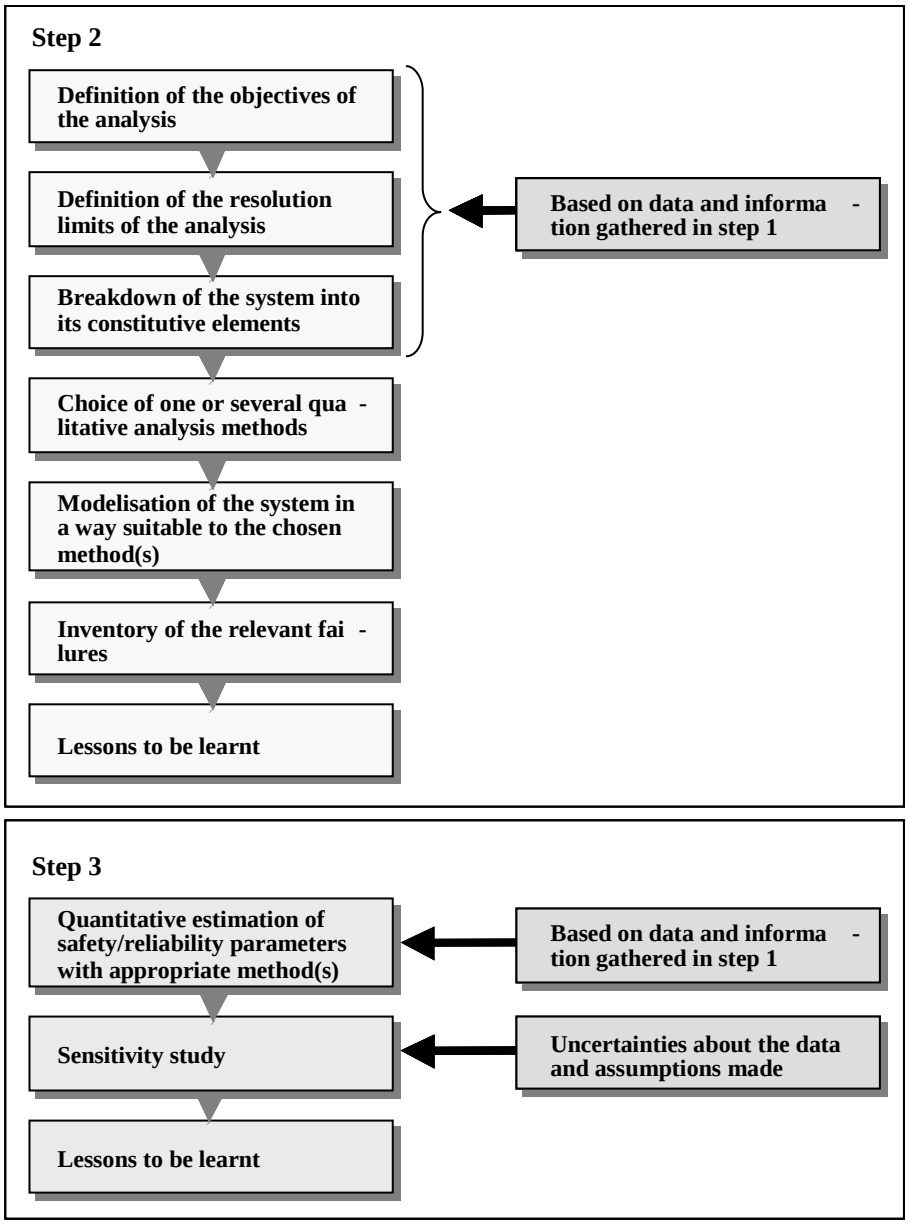


Figure 4.3 ***Detailed description of the sub-tasks involved in the general analysis scheme of Fig. 4.2 (adapted from [Villemeur, 1988])***

Methods that can be used in step 2 are presented in the remaining of this chapter. Methods better suited for step 3 - semi-quantitative and quantitative approaches - are described in chapters 5 and 6 respectively.

Generally speaking, all these methods belong either to the *inductive* or to the *deductive* families of risk analysis approaches. Simply stated, inductive (or *bottom-up*) approaches answer the question “What if event *X* happens?”, while deductive (or *top-down*) approaches ask ``How can event *X* occur?' Although deductive approaches are easier to establish and are often recommended by regulatory agencies as a good starting point, they are generally less informative in the long run than inductive approaches.

4.2 Preliminary Hazard List (PHL) and Preliminary Hazard Assessment (PHA) Methods

Preliminary Hazard List

Qualitative methods aim at carrying out a first and rapid screening of the hazards that can threaten people or assets. 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 approaches, the hazards identification usually draws on lists of keywords that describe possible hazards that could be related to the specific system being studied. A 'Preliminary Hazard Listing' is thus prepared to identify the primary generic hazards and accident scenarios that are associated with the system in question. The process shall highlight any areas on which to focus special design attention. The 'Preliminary Hazard Listing' shall be carried out by means of a checklist-based approach or similar method. Consideration shall be given to previous development and actual incident and accident data relating similar or other applicable systems. The result of such a checklist is an enumeration as exhaustive as possible of potentially dangerous situations or events.

Examples of common hazard sources that could be considered in the framework of a preliminary hazard listing are given in Table 4.1

Table 4.1 ***Example of a "Preliminary Hazard" checklist***

Potential hazards	**Yes/ No**
Flammable/Combustible liquids, gases or vapors	
Toxic Materials	
Carcinogens	
Acids/Caustics	
Other Hazardous Chemicals/Materials	
Explosion Potential (Explosives/Blasting Agents)	
Potentially Hazardous Pressures	
Electrical Hazards	
Particulate (dusts, fumes, fibers)	
Respiratory Hazards (Organic vapors or gases)	
Noise /Vibration	
Temperature extremes	
Radiation (Ionizing/Non-ionizing)	
Cutting, Welding or Hot Work	
Machinery (woodworking, metal working, other)	
Hoisting Apparatus	
Miscellaneous Hazards (Biological, Health, etc.)	

An example of a PHL form is given in the figure 4.4.

DATA ITEM DESCRIPTION

1. TITLE	2. IDENTIFICATION NUMBER
Preliminary Hazard List (PHL)	

3. DESCRIPTION/PURPOSE

The PHL provides a list of HAZARDS that may require special SAFETY design emphasis or hazardous areas where in-depth analyses need to be done. It is compiled very early in the SYSTEM acquisition life cycle to identify potentially hazardous areas on which to put management emphasis.

4. APPROVAL DATE	5. OFFICE OF PRIMARY INTEREST	6. OFFICE OF COLLATERAL INTEREST

7. APPLICATION/INTERRELATIONSHIP

8. ORIGINATOR	9. REFERENCES

10. PREPARATION INSTRUCTIONS

10.1 The PHL shall be prepared in the Contractor's format.

10.2 The PHL shall identify the HAZARDS including, but not limited to, the following information:

a. system/Subsystem/Unit. The particular part of the system that this analysis is concerned with;

b. system Phase. The configuration or phase of the mission the system is in when the hazard is encountered; for example, during maintenance, etc.;

c. hazard Description. A description of the potential/actual hazard inherent in the system being analyzed, or resulting from normal actions or equipment failure, or handling of hazardous materials;

d. Effect of hazard. The detrimental effects which could be inflicted on the subsystem, system, other equipment, facilities or personnel, resulting from this hazard;

e. Risk Assessment. A risk assessment for each hazard (classification of severity and probability of occurrence using the risk assessment matrix, System Safety Program Plan).
This is the assessment of the risk prior to taking any action to eliminate or control the hazard;

f. Recommended Action. The recommended action required to eliminate or control the hazard (if this information is available); and

g. Remarks. Other pertinent information relating to the hazard.

Figure 4.4 ***Example of PHL form***

As mentioned in the above form, Preliminary Hazard Lists are often associated to Risk Assessment Matrixes of the kind presented below to make some qualitative risk assessment feasible.

Risk Matrix

Severity of Consequence	Occurrence Probability				
	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic (Fatal)					
Critical (Major injury/ permanent disability)					
Marginal (Minor injury)					
Negligible (No injury)					

Legend:

1st rank action
2nd rank action
3rd rank action
acceptable risk/ no action

Fig. 4.5 ***Risk Assessment Matrix***

Hazard identification may at first sight seem to be a little structured process but there are a number of techniques to help in this task. In particular, the following general guidelines can prove useful:

- Use historical safety experience, lessons learned, trouble reports, hazard analyses, as well as accident and incident files. Carry out scientific investigation of physical, chemical, and other properties of the system, as well.
- Make an exhaustive inventory of potentially hazardous materials (fuels, propellants, lasers, explosives, toxic substances, pressure systems) in the systems.
- In general, look at potential safety related interface problems such as material incompatibilities, electromagnetic interference, possibilities for inadvertent activation, contamination, etc. Consider environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).
- Examine basic energy sources and flows. How might these energies be released in an uncontrolled manner? How else might these energies participate in an accident?
- Review all possible system uses, all modes of operation, all possible environments, and all times during operation. Accidents often occur when systems are pushed to operate beyond the assumptions the designers had in mind, so examine likely scenarios of operation outside the planned environment of the system.

The advantages of the PHL approach are its easiness of execution, its large domain of application (so long as adapted checklists are available, but many industries have published lists, checklists, standards, and codes of practice that may help guide hazard list development) 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 of course the lack of quantification of its results.

Preliminary Hazard Assessment

The Preliminary Hazard Assessment, or Preliminary Hazard Analysis, method (PHA) is an inductive approach that broadens in some extent the scope of the checklist process. As for this last one, the main purpose of a Preliminary Hazard Analysis is to identify the hazardous states of a system and their implications that may require special safety design emphasis, as well as hazardous areas where in-depth analyses need to be done. This information can then be used to reduce the severity or build-in safeguards against the effects of the identified hazards. The PHA effort must start during the concept exploration phase so that safety considerations are included in tradeoff studies and design alternatives.

Contrary to the simple checklist approach, the PHA is thus not only interested in the constituent parts of the system but also in its potentially dangerous states and corresponding possible correcting measures (see Fig. 4.6).

In addition to the elements mentioned above for the PHL approach, the PHA shall as a minimum consider the following for identification, evaluation and mitigation of hazards:

- Operating, test, maintenance, built-in-tests, diagnosis, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage).

- Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, proof testing of hazardous systems/assemblies) and training (e.g. training and certification pertaining to safety operations and maintenance).
- Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).
- Malfunctions to the system or subsystems. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.

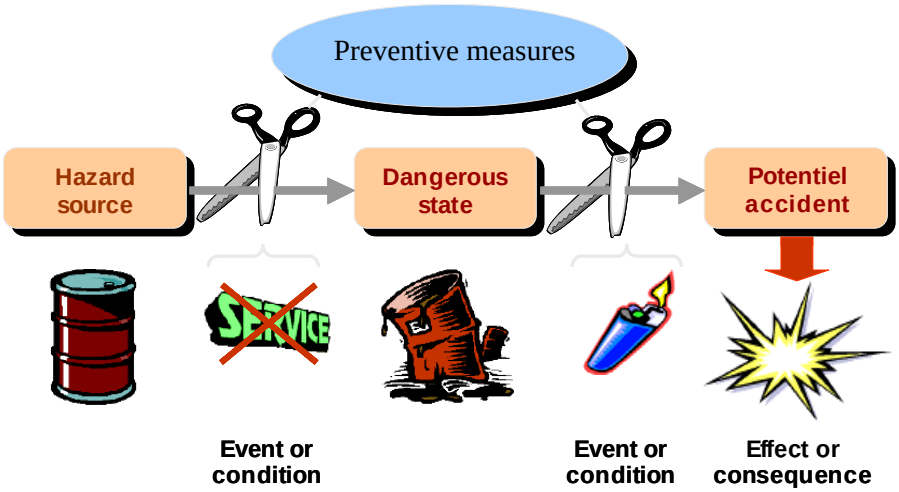


Figure 4.6 ***Chain of events considered in a PHA***

The content of a Preliminary Hazard Analysis report shall include:

- a brief description of the system (incl. subsystems) and its design;
- a list of identified hazards applicable to the system including a description;
- a list of identified accidents applicable to the system including a description and details about associated hazards and accident sequence;
- a description of the system functions and safety features;
- a description of human error which could create or contribute to accidents;
- list of all source documents used, including their issue, dates, and status;
- conclusion and recommendations.

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

- *Hazardous Sources*: a description of the hazards and/or undesirable or unacceptable occurrences.
- *Causal Factors*: a description of why or how the hazards may result in mishaps (events or conditions leading to a dangerous situation).
- *System Effects*: how could the system, subsystems, environment, community or persons be hurt (potential accident)
- *Comments*: preventive measures, recommendation, applicable standards, etc.

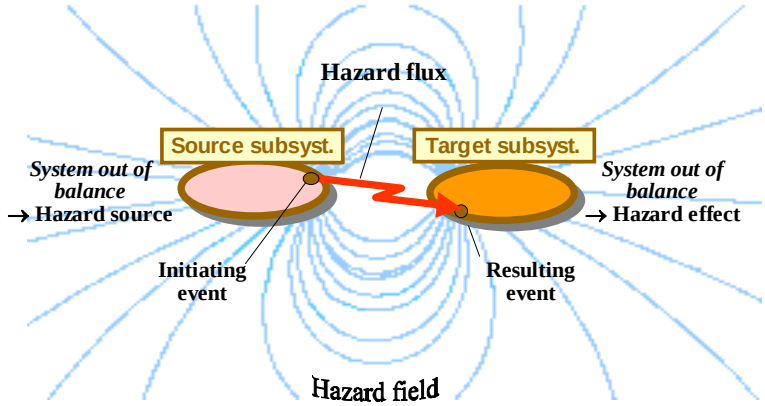
Because the PHA is conducted early in the process and uses preliminary design information, additional analyses are generally required to more fully understand and evaluate hazards and potential accidents identified by this preliminary step. It is worth noting that the susceptibility to omissions, the main drawback of the simple checklist approach is by no means improved with the PHA method.

4.3 Method Organized for a Systematic Analysis of Risks (MOSAR)

The MOSAR model

MOSAR [Périlhon. 1999] is a generic method that aims at providing a well-structured framework for the analysis of the risks of industrial or other types of systems in a stepwise manner. In this approach, the system is considered as a number of reciprocal subsystems that are analyzed on the basis of a "hazard source → flux → target" scheme (Fig. 4.7). This approach can be used as well at the design stage of a new installation as for the diagnosis of an existing installation. It can greatly help identifying the risks incurred by different objects at risk in a given geographical area presenting multiple potential hazards. Finally, it constitutes also a useful decision-aiding tool through the choices that it puts to the fore.

a)



b)

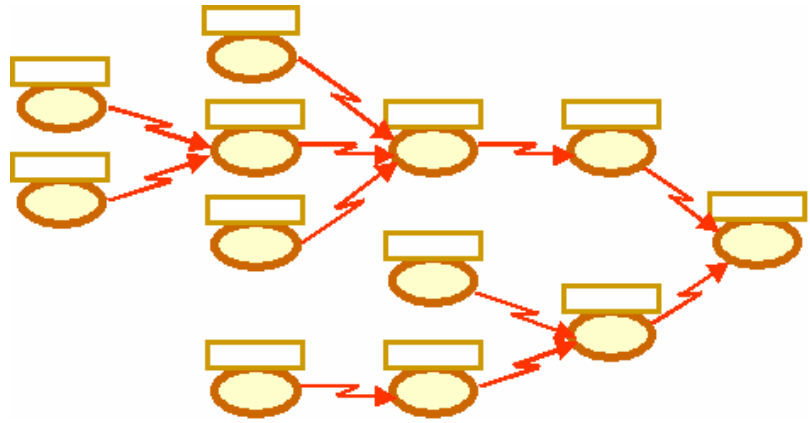


Figure 4.7 ***Reference basic scheme for the MOSAR method (a) and chaining principle (b) (inspired from [Périlhon, 1999])***

To establish the above type of model, one considers as *hazard flux* any undesirable "transaction" of a system or subsystem with its environment, and as *hazard field* the active environment showing fluctuations susceptible to put the system or subsystem out of balance.

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

The hazard source subsystem is at the origin of a hazard flux in consequence of the occurrence of an *initiating event*, or *cause*. Causes can occur by themselves or in combinations. An example of a hazard cause would be a crimped fuel line or water in a fuel tank; such an event could directly lead to an interruption of fuel to an emergency power supply.

The *resulting event*, or *harm*, is a description of the potential outcome of the hazard flux when it affects the considered target subsystem. In the previous example, the effects could describe what happens if the resulting loss of emergency power affects the operating room of a hospital following an initial power outage (chained events, see below). This obviously has the potential for very serious consequences.

The target thus put out of balance can in its turn become a source of hazard for another part of the system, transforming this way this target into a new source subsystem. This gives rise to the chaining phenomena of undesirable events, called an *accident scenario*, symbolically represented in the figure 4.7 b).

Example (simplified Three Mile Island nuclear accident scenario; see Fig. 4.8):

The initial problem at Three Mile Island Unit 2 was the failure of its main reactor coolant pump (# 1 source). When the main coolant pump in Unit 2 failed, the pressure inside the reactor (# 1 target; # 2 source) spiked. It had to be released through an emergency release valve (# 2 target; # 3 source) to vent the pressurized steam. This valve did its job but then failed to close after the pressure was no longer inside the specified range. The temperature in the reactor (# 3 target; # 4 source) was rising dangerously high, because all of the coolant was being released through this valve. As a result, Unit 2 of the Three Mile Island nuclear station was left uncooled. It was to remain so for longer than sixteen hours. Temperature inside the fuel rods (# 4 target) began to reach unimaginable temperatures. The damage had been done.

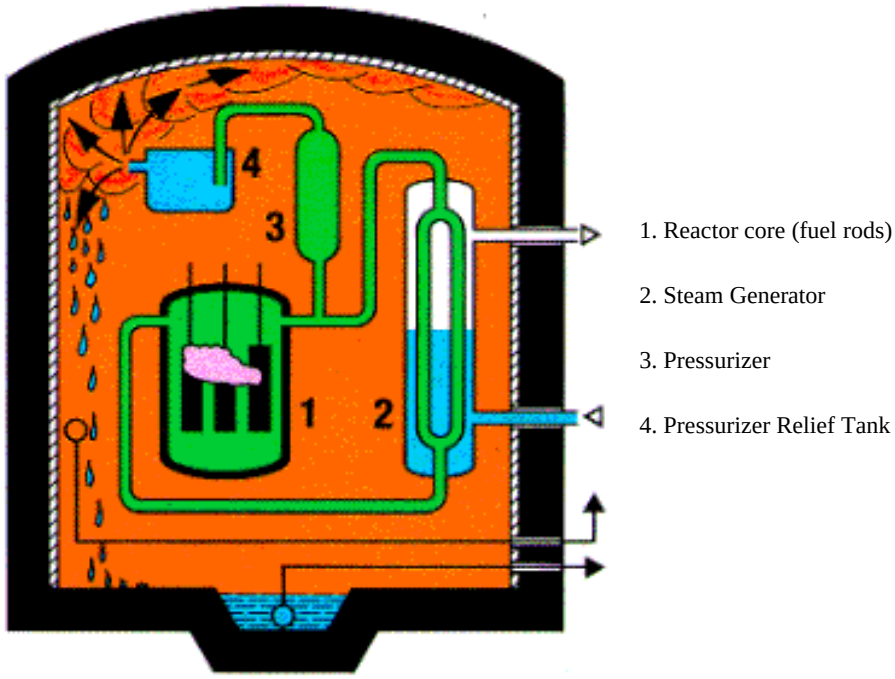


Figure 4.8 ***Schematic description of the Three Mile Island nuclear accident*** **(source: KWU)**

A modular approach

Mosar is a method divided in two successive or independent phases. The phase *A* (*preliminary analysis of risks*) is the part of the method that essentially falls in the category of qualitative approaches. It is normally, but not necessarily, followed by a phase *B* (*analysis of operating risks*) that calls for some of the methods that will be presented in the two following chapters and are therefore of a more quantitative nature. In total, the method counts ten different modular levels.

The method is thus an approach:

- by *levels*: each level enables the analyst to solve a specific problem, from the more simple to the more complex;
- *with scale effect*: thanks to its logic and modular structure, MOSAR can be adapted to installation of different sizes;
- *transverse*: MOSAR can be used to analyze the risks of any type of installation and of its natural or artificial environment;
- *structuring*; considering its well-defined structure, MOSAR is well suited to structure any kind of risk problems;
- *multipurpose*; MOSAR can as well be used for the analysis of industrial or natural risks, as for carrying out audits, expert appraisals, or to answer training needs in the concerned domain.

The five modular levels associated with the phase *A* of the method are briefly defined in Table 4.2 and those associated with the phase *B* in Table 4.3.

Table 4.2 ***Modular levels of the MOSAR phase A***

A-1	*Description of the system*	From a layout sketch, a technical file (design study), a visual observation (diagnostic study)
A-2	*Identification of the hazards*	From a reference list of the hazards of all types, identification of the hazards related to the system
A-3	*Evaluation of the potential hazard consequences*	With the help of software or other tools enabling to cover the full spectra of the possible consequences of accident scenarios
A-4	*Prioritization of the risks*	Through the use of a Probability-Intensity Matrix that could be negotiated after assessment of the accident scenarios
A-5	*Definition of the prevention and protection means*	Identification of prevention and protection barriers, and their qualification along the time; regulation

Table 4.3 ***Modular levels of the MOSAR phase B***.

B-1	*Identification of the operating risks*	Of an operating (human activity) and/or of a technical (equipment) nature, using methods such as FMEA, HAZOP, etc.
B-2	*General risk assessment*	Through the use of tools such as logic trees and their possible quantification
B-3	*Negotiation of specific objectives*	By negotiating the number and type of barriers to provide in order to neutralize the operating risks
B-4	*Definition of complementary protection means*	By identifying the possible missing protection barriers as well as the residual risks
B-5	*Risk management*	By developing intervention plans for the identified accident scenarios

Phase *A* provides a good analysis of the major risks associated with an installation. It can be carried out by any engineer or technician having a good knowledge of the system under study and requires in principle no more than a few days for a classical installation.

Phase *B* is more complex and could be quite time consuming, depending on the level of details required. It demands not only a good knowledge of the system under study but also of some of the analysis tools presented in the following chapters.

The logical relationships between the different modules of a full MOSAR analysis are represented graphically in the figure 4.9.

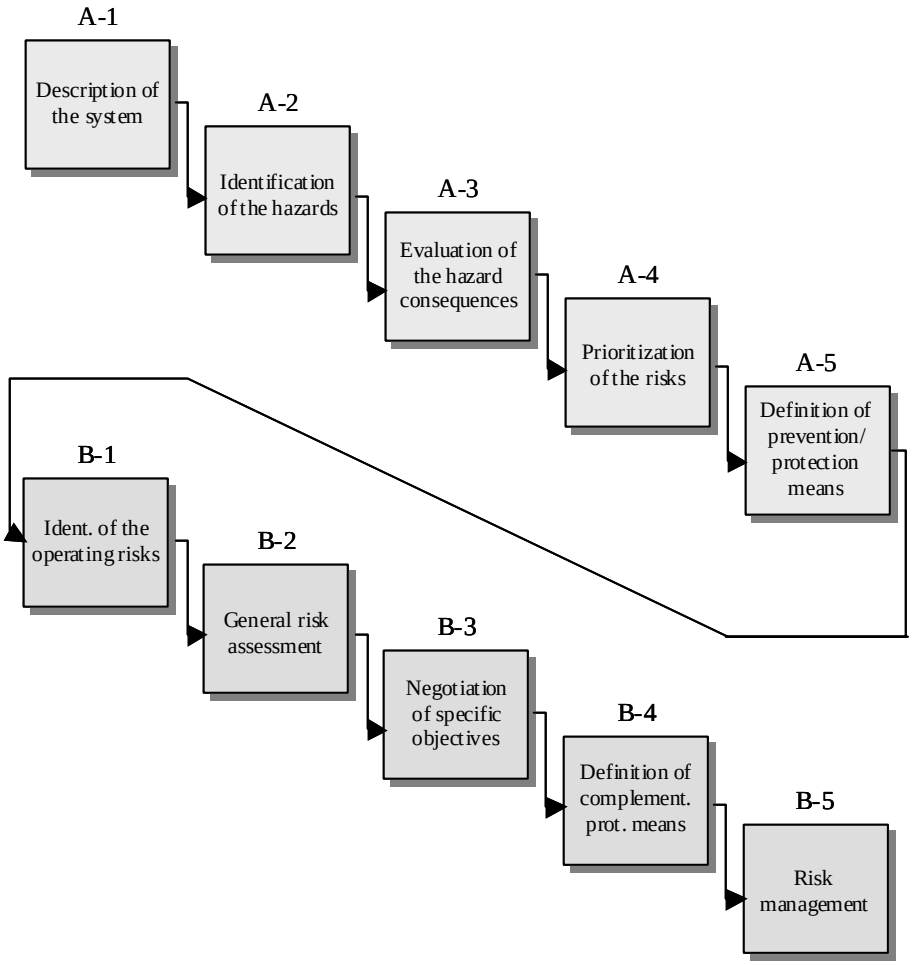


Figure 4.9 ***Full modular structure of the MOSAR approach (inspired from [Périlhon, 1999])***

The MOSAR approach is in particular currently used in France by important enterprises such as EDF (“Électricité de France”), CEA (“Commissariat à l’Énergie Atomique”), Saint-Gobain, etc.