A FRAMEWORK FOR APPLICATION OF PROBABILISTIC RISK ANALYSIS TECHNIQUES

Acires Dias, acires@emc.ufsc.br
Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Engenharia Mecânica
Núcleo de Desenvolvimento Integrado de Produtos – NeDIP
Campus Universitário – Cx. P. 476 – CEP 88040-900 – Florianópolis – SC. – Brasil

Bernardo L.R. Andrade, bernardo.andrade@poli.usp.br
Escola Politécnica da USP
Departamento de Engenharia Naval e Oceânica
Av. Prof. Mello Moraes 2231, Cidade Universitária
CEP 05508-030 – São Paulo – SP – Brasil

Douglas Roberto Zaions, douglas.zaions@unoesc.edu.br
Universidade do Oeste de Santa Catarina
Engenharia de Produção Mecânica
Av. Getúlio Vargas, 2125
CEP 89600-000 – Joaçaba – SC – Brasil

Luís Fernando Peres Calil, calil@nedip.ufsc.br
Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Engenharia Mecânica
Núcleo de Desenvolvimento Integrado de Produtos – NeDIP
Campus Universitário – Cx. P. 476 – CEP 88040-900 – Florianópolis – SC. – Brasil

Abstract. *Since the beginning of the last century the complexity of technical systems is increasing, and new technologies are being developed and embedded in those systems. As a consequence the hazards related to the operation of technical systems also have increased, especially in industries like energy generation, chemical plants, petroleum production, air and maritime transport, etc. To deal with this situation in the last thirty years a large number of laws, regulations, methodologies, techniques and tools for hazard and risk assessment have been developed and implemented. However, despite the great improvement in the analysis and management incidents with catastrophic consequences are still happening during the operational phase of technical systems. Motivated by these facts a study has been conducted to understand and clarify differences in some of these industries – more specifically nuclear, maritime and air navigation industries. This paper describes some frameworks for Probabilistic Risk Assessment (PRA) and some of the main analysis techniques like Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagram (ESD) and Failure Mode Effects and Criticality Analysis (FMECA). In the last section it is proposed a simplified framework for the application of these analysis techniques in a system risk assessment at the operational phase.*

Keywords*: risk analysis, operational risk, risk techniques*

1. INTRODUCTION

Complex technical systems as those in the aerospace and nuclear industries have several demands. Managers, designers and workers at the operation and maintenance have to operate the systems and ensure profit, but also availability, reliability, maintainability, safety and low levels of risk. These attributes were popularized for other industrial sectors as the naval, electric, petroleum, etc. Risk assessment in these industries are nowadays being performed using Probabilistic Risk Assessment (PRA) methodologies. To support this analysis, several techniques were developed, like: Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagram (ESD) and Failure Mode Effects and Criticality Analysis (FMECA). A thorough compilation and description of the available techniques can be found in EUROCONTROL (2004) and Everdij and Blom (2004). A review and classification of some of the main techniques can also be found in Tixier et al. (2002).

In spite of this, accidents occur and questions are formulated: What should be done to avoid accidents? How to anticipate the danger? How to estimate the financial lost? Are there differences between simple and complex technical system? According to our vision, PRA is a generic process. However the application always should be focused. Besides the technical variable, they are preponderant the human and economic variables. The goal of this paper is to introduce the approach adopted in the nuclear, air navigation and maritime sectors, focusing the analysis in the macro-structures and in the techniques to support the methodologies.

The current application of Probabilistic Risk Analysis (PRA) in safety assessments of technical systems has spread out thanks to initiatives taken in nuclear sector, especially in the USA. However, the first use of probabilistic techniques was in the aerospace industry through the application of Fault Tree Analysis (FTA) in the design of the Minuteman missile (KELLER; MODARRES, 2005). In 1970s, the United States Nuclear Regulatory Commission (USNRC) has supported many works and studies related to the application of PRA in the safety assessment of nuclear power plants. Some of these works turned out to be basic references for PRA and influenced the development of guidelines and procedures for risk analysis in other sectors. The next section presents a brief historical overview and description of the application of PRA in the nuclear (mostly American), maritime and air navigation industries and of the guidelines, standards and methodologies adopted in each sector.

2.1 Nuclear Sector

The safety of nuclear power plants has been assessed based in a deterministic approach, by which the performance of the safety systems must be checked against a basic set of design accidents. The fundamental assumption is that if a plant could withstand the design accidents then it will be capable to withstand any other kind of accident. As a consequence of that approach the plants design has been characterized by the use of high safety margins and multiples barriers and independent safety systems (KELLER; MODARRES, 2005). Although, the deterministic approach has been conceived in the 1940s it is still today the basic methodology for plant licensing and approval.

In the early 1970s, with the growing up of the size and complexity of nuclear plants, there was a strong public questioning about the adequacy of the criteria adopted for licensing the plants. At that time emerged a perception that new approaches should be developed and applied to assess the safety of the plants (KELLER; MODARRES, 2005). In response the USNRC started a Reactor Safety Study that end up with the famous WASH-1400 report (USNRC, 1975) which describes the first comprehensive application of PRA to a technical system. Since this seminal study it took more than 20 years until the PRA methodology was accepted as a complementary approach to safety assessment in the licensing of nuclear power plants in the USA (USNRC, 2003).

The WASH-1400 report suffered a lot of criticism and, it was not until the Three Mile Island accident that it became the basic reference for all the posterior development of the PRA methodology in the nuclear sector. Many of the procedures and techniques described in this report are still in use nowadays and many of them served as a base to procedures adopted in other industries (KELLER, MODARRES, 2005).

In an attempt to standardize the PRA procedure the USNRC published in 1982 the guideline NUREG/CR-2300 (USNRC, 1983). It was in this guide that it was first proposed the concept of dividing the risk analysis in three levels according to the analysis depth of the accidents and consequences. This guide was the basic reference for the analysis performed in the 1980s and 1990s (USNRC, 2003).

In 1986 the USNRC started a major PRA review in 5 plants and by the end of 1990 issued the report NUREG-1150 (USNRC, 1990), which became a reference for the performance of PRA in nuclear power plants. Also in late 1980s, as a mean to spread out the knowledge about PRA, the USNRC issued the Generic Letter 88-20 requesting the industry to perform an individual plant examination for severe accident vulnerabilities. As a result, up to 1992, 74 PRAs were performed by the utilities.

In the international arena, following the development in the USA and based on compilation and review of practices in various Member States, the International Atomic Energy Agency (IAEA) issued 2 guides intended to assist technical persons to perform and manage PRAs (IAEA, 1992 and IAEA,1995).

At that time, although the knowledge about the procedures and techniques of PRA was reasonably mature, its use in the american nuclear industry only became effective after the issuance of a policy statement (USNRC, 1995) and a regulatory guide (USNRC, 1998) establishing objective criteria to the acceptance of the results of PRA in the licensing of plants. According to these guidelines the utilities should demonstrate the safety of their plants through a combined approach considering both deterministic analysis and PRA.

Once the PRA became part of the regulatory process the concern about the quality of these analysis emerged and in 1997 the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) started to develop a industry standards for PRA. In 2002 the first of these standards (ASME, 2002) was approved by the American National Standard Institute (ANSI) and in 2003 the ANS issued his first standard concerning PRA considering external events to the plant (ANS, 2007). Other two standards are yet being prepared by the ANS.

Essentially, the PRA methodology in the nuclear sector is a procedure to identify failure scenarios that could result in reactor core damage and to obtain numerical estimates of the risks to the society and environment from radioactive releases. Figure 1 depicts the main steps (KUMAMOTO; HENLEY, 1996) of the analysis which can be performed at the following three levels, depending on its scope (IAEA, 2002):

- Level 1: identify the sequence of events that can lead to core damage; estimate the core damage frequency; provide insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage.

- Level 2: group the accident sequences in plant damage states with similar characteristics; identify ways in which radioactive releases from the plant can occur; estimate the magnitude and frequency of the releases.
- Level 3: group release categories; estimate consequences and risks to public health and environment.

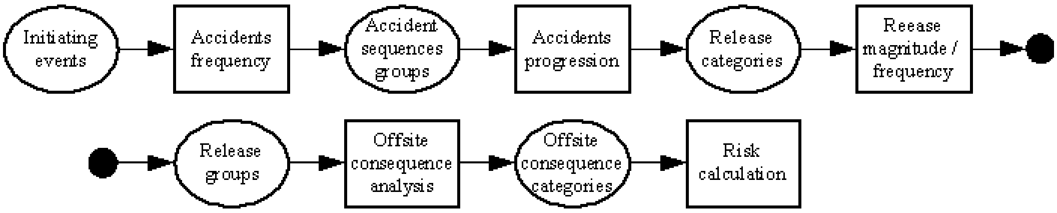
Initiating events
Accidents frequency
Accident sequences groups
Accidents progression
Release categories
Reease magnitude / frequency
Release groups
Offsite consequence analysis
Offsite consequence categories
Risk calculation

Figure 1.Steps for PRA (KUMAMOTO; HENLEY, 1996)

2.2 Maritime Sector

Due to its international character the maritime transportation industry and the operation of ships are one of the most regulated activities, subjected to many rules, regulations, laws, etc. enforced by different coastal states, organizations and institutions. These regulations are related to different aspects of the operation of ships like, construction, navigation, ports and channel transit, crew work and, particularly to the safety of the ship, of the environment and of those involved in the ship operation.

The safety regulations are basically established by the International Maritime Organization (IMO) and complementary by Classification Societies like Det Norsk Veritas (DNV), American Bureau of Ships (ABS) and others through theirs rules for classification of ships. The most notorious regulations in effect are the SOLAS Convention (IMO, 2004) and the MARPOL Convention (IMO, 2006) which establish requirements and minimum standards related, respectively, to the safety of the ships and to marine pollution prevention. The Classification Societies establish rules and technical standards related to the design, construction and inspection of ships aiming basically the structural integrity of the ships hull and the reliability and adequacy of the main systems and equipments which are responsible to assure a minimum level of essential functionalities of the ship, like propulsion and maneuverability.

The main characteristic of these rules and regulations is that they are prescriptive in nature, i.e. they set up direct requirements and constraints related to characteristics and attributes of the ship and its systems and components without clarifying the safety goals behind them. The basic assumption is that the safety of the ship is assured once all the rules and regulations are complied with. As part of this philosophy of compliance many of the specifications inside these regulations are developed based in the past experience and many of them are implemented through a reactive process, after the occurrence of some major accident (Wang, 2002). In this sense it's worthwhile to remember that the first version of the SOLAS Convention was settled in 1914, just after the Titanic accident. The version in effect today is that of 1974 with many amendments included during the following years as a response to ship accidents.

One of those accidents, the capsizing of the ferry Herald of Free Enterprise on 1987, became notorious from the point of view of safety regulation because it was from the investigation of the causes of that accident that the PRA was first considered as a new approach to the safety assessment in the maritime transport. According to Wang (2001), the report from that investigation, issued in 1992 and known as Lord Carver's Report, suggested that a new and more scientific approach should be considered on issues related to the safety regulation of the maritime transport. The report recommended that the regulatory approach should be a non-prescriptive and performance based one. This was, according to Wang (2001), the initial idea that gave rise to the concept of Formal Safety Assessment (FSA) in the maritime industry, which was proposed to IMO by the United Kingdom in 1993 as a safety assessment approach based on probabilistic risk analysis (PRA).

After this initial proposition and, during the following decade, IMO has supported many studies and workshops in order to discuss and improve the FSA methodology, including some experimental applications of the methodology in different kinds of ships and safety issues (IMO, 1998 and IMO, 2002a). Finally, in 2002 the methodology was approved by IMO as a technique to support the development and revision of new and existing regulations and issued the first guideline describing the FSA methodology and the requirements for its application (IMO, 2002b). Although, it was initially conceived for generic applications related to the development of safety regulations, the FSA methodology could also be applied to an individual ship or fleet aiming a design or operational improvement or to help predicting and controlling hazardous situations that could result in incidents (WANG, 2001).

Following that trend the Classification Societies started the development of guidelines for the application of PRA as a first step to introduce this approach in the process of classification and of safety assessment of ships (ABS, 2003).

Formal Safety Assessment (FSA) is a structured methodology for safety assessment of ships and maritime transport based on probabilistic risk analysis. The FSA methodology as described in IMO (2002) and depicted in Figure 2, comprises the following 5 steps:

1. Identification of Hazards: the purpose is to identify hazards and associated scenarios that could lead to accidents like contact or collision, grounding, explosion, fire, flooding and foundering.
2. Risk Analysis: the purpose is to investigate the causes and consequences of the more important scenarios, to estimate the frequencies and consequences of accidents and to identify the high risk areas that need to be addressed.
3. Risk Control Options: the purpose is to propose effective and practical risk control options to reduce the risk level in the high risk areas. For each option, steps 1 and 2 should be done again and the changes in the risk level determined (see figure 2).
4. Cost Benefit Assessment: the purpose is to identify and compare the benefits and costs associated with the implementation of the risk control options.
5. Recommendations for Decision Making: the purpose is to define recommendations for decision making, based on comparison of alternative options, on the potential reduction of risks and on costs to implement the alternatives.

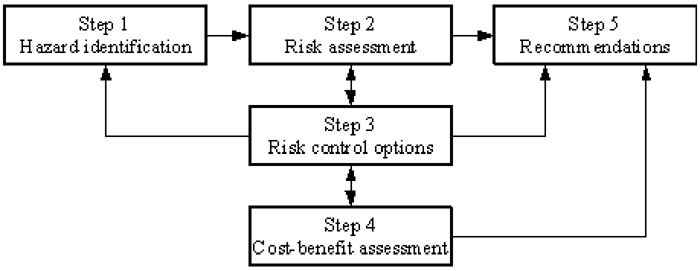

Figure 2. FSA methodology (IMO, 2002)

2.3 Air Navigation Systems

In the beginning of 60's, the increasing complexity of aircraft design (Concord illustrate that) required the use of probabilistic safety assessment (SILVA, 2006).

Fault Tree Analysis, for example, was first conceived by H. A. Watson of Bells Laboratory in connection with a U.S. Air Force contract to study Minuteman missile launch control system. After that, Boeing began to use FTA during the design of commercial aircraft and present several papers on FTA at System Safety Conference – in 1965 (ERICSON, 1999).

Nowadays, organizations – SAE, U.S./FAA, European JAA and EUROCONTROL, for example – are developing methodologies and requirement to assurance safety. For instance, EATMP (European Air Traffic Management Programmer) propose the Air Navigation System Safety Assessment Methodology (ANS SAM), that has been developed to reflect best practices for safety assessment of Air Navigation Systems and to provide guidance for their application. It applies to Air Navigation Systems considering the three types of system elements: people, equipment and procedures and their interactions (within the system and with its environment) in a specific environment of operation (EUROCONTROL, 2006).

EATMP SAM was based on SAE ARP 4761 (SAE, 1996b) that describes several techniques for evaluation of the safety in equipment and systems of civil aviation and is applied jointly with SAE ARP 4754 (SAE, 1996a).

SAE ARP 4754 (SAE, 1996a), for instance, was developed in the context of the American regulation of the FAR – Federal Aviation Regulations (Federal Regulation of Aviation) and JAR – Joint Airworthiness Requirements (Common Requirements of Navigability) – JAR Part 25, 23, 27, 29 and 33. SAE ARP 4754 (SAE, 1996a) in general also is applied to the engines systems and equipment correlates.

Figure 3 illustrates the methodology. The process comprehends all the life-cycle of an air navigation system, from system definition, passing through design, implementation, and integration, operations, maintenance and decommissioning.

The objectives of the FHA, the PSSA and the SSA are (EUROCONTROL, 2004):

Functional Hazard Assessment (FHA) analyses the potential consequences on safety resulting from the loss or degradation of system functions. Using service experience, engineering and operational judgment, the severity of each hazard effect is determined qualitatively and is placed in a class 1, 2, 3, 4 or 5 (with class 1 referring the most severe effect, and class 5 referring to no effect). Safety Objectives (SO) determine the maximum tolerable probability of occurrence of a hazard, in order to achieve a tolerable risk level.

Preliminary System Safety Assessment (PSSA) determines that the proposed system architecture is expected to achieve the safety objectives. PSSA examines the proposed system architecture and determines how faults of system elements and/or external events could cause or contribute to the hazards and their effects identified in the FHA. Next, it supports the selection and validation of mitigation means that can be devised to eliminate, reduce or control the hazards and their end effects. System Safety Requirements are derived from Safety Objectives; they specify the potential means identified to prevent or to reduce hazards and their end effects to an acceptable level in combination with specific possible constraints or measures.

System Safety Assessment (SSA) collects arguments, evidence and assurance to ensure that each system element as implemented meets its safety requirements and that the system as implemented meets its safety objectives throughout its lifetime. It demonstrates that all risks have been eliminated or minimized as far as reasonably practicable in order to be acceptable, and subsequently monitors the safety performance of the system in service. The safety objectives are compared with the current performances to confirm that they continue to be achieved by the system.

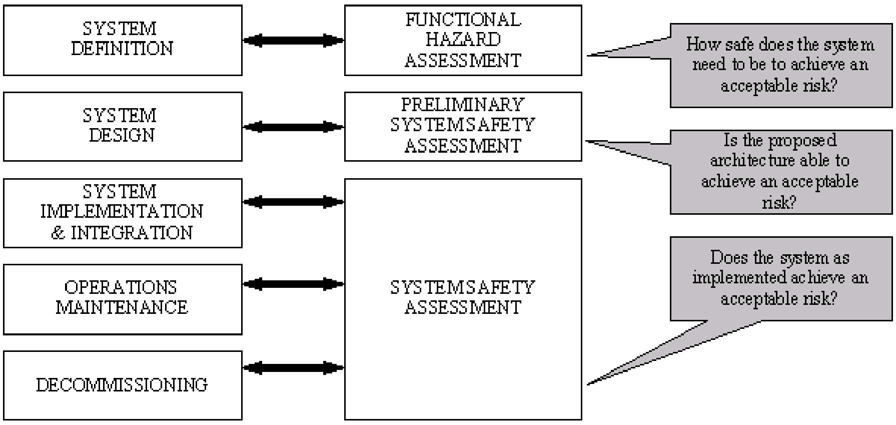
SYSTEM DEFINITION
FUNCTIONAL HAZARD ASSESSMENT
How safe does the system need to be to achieve an acceptable risk?
SYSTEM DESIGN
PRELIMINARY SYSTEM SAFETY ASSESSMENT
Is the proposed architecture able to achieve an acceptable risk?
SYSTEM IMPLEMENTATION & INTEGRATION
Does the system as implemented achieve an acceptable risk?
OPERATIONS MAINTENANCE
SYSTEM SAFETY ASSESSMENT
DECOMMISSIONING

Figure 3. Relationships between the Safety Assessment Process and System Life Cycle (EUROCONTROL, 2006)

3. TECHNIQUES TO SUPPORT PRA

Independent of the area, the methodology adopted or the knowledge required, risk assessment should be supported by techniques to ensure availability of the necessary information to manage risk during design, operation or contingency. Some of these techniques are presented in the sequel.

3.1 Failure Mode Effects and Criticality Analysis (FMECA)

FMECA was first published in the U.S. military procedure MIL-P-1629 (Procedures for performing a failure mode, effects and criticality analysis) in 1949.

It is an inductive technique that its purpose is “to study the results or effects of item failure on system operation and, to classify each potential failure according to its severity” (DOD, 1980).

Despite it was first published in a standard procedure, FMECA has some variation, depending from organization and application. Table 1 shows an example of a design FMECA from SAE standard J1739 (SAE, 2002), where:

- “Item / function” is the identification of the analysed item and the functions to meet the design.
- “Potential Failure Mode” is the manner in which the item could potentially fail to meet or deliver the intended function (the potential failure mode may also be the cause of a potential failure mode in a higher level subsystem, or system, or be the effect of one in a lower level component).
- “Potential Effect(s)” are the effects of the failure mode on the function, as perceived by the customer.
- “S – Severity” is the rank associated with the how serious these effects are, and only through a design change it can be reduced.
- “Potential Cause(s) / Mechanism(s)” is an indication of a design weakness, the consequence of which is the failure mode.
- “O – Occurrence” is the likelihood that a specific cause/mechanism will occur during the design life (the ranking number has a relative meaning rather than an absolute value).
- “Current Design Controls” are those activities which are completed or committed to and that will assure the design adequacy for the failure mode and/or cause/mechanism under consideration (e.g., road testing, design reviews, etc.) that have been or are being used with the same or similar designs.
- “D – Detection” is the rank associated with the best detection design control listed.
- “RNP – Risk Priority Number” is the product of the severity (S), occurrence (O), and detection (D) ranking.
- “Recommended Action(s)” aim to reduce risks and increase customer satisfaction and should be first directed at high severity, high RPN, and other items designated by the team.
- “Responsibility & Target Completion Date” is the name of the responsible for the recommended action and the target completion date.

- "Actions Taken and new indices" is a description of the actual action and effective date, after an action has been implemented.
- "Revised ratings" is the estimative and record of the resulting rankings and calculate RPN, after the preventive/corrective action has been identified.

Table 1. FMECA example: Front Door (SAE, 2002)

Item / Function	Potential Failure Mode	Potential Effect(s)	S	Potential Cause(s) / Mechanism(s)	O	Current Design Controls	D	RNP	Recommended Action(s)	Responsibility & Target Completion Date	Actions Taken	S	O	D	RNP
Front Door L.H H8HX-0000-A - Ingress to and egress from vehicle - Occupant protection from weather, noise, and side impact …….. ………..	Corroded interior lower door panels	Deteriorated like of door leading to: - Unsatisfactory appearance due to rust through paint over time - Impaired function of interior door hardware	7	Upper edge of protective wax application specified for inner door panel is too low	6	Vehicle general durability test veh . T-118, T-109, T-301	7	294	Add laboratory accelerated corrosion testing	A Tate-Boby Engrg 8X 09 30	Based on test results (Test Nº 1481) upper edge spec raised 125mm	7	2	2	28
			7	Insufficient wax thickness specified	4	Vehicle general durability testing – as above	7	196	- Add laboratory accelerated corrosion testing - Conduct Design of Experiments (DOE) on wax thickness	- Combine x/test for wax upper edge verification - A Tate-Body Ergrg 9X 01 15	Test results (Test Nº 1481) show specified thickness is adequate. DOE shows 25% variation in specified thickness is acceptable	7	2	2	28

3.2 Functional Hazard Assessment (FHA)

The Functional Hazard Assessment (FHA) consists of a systematic and inclusive examination of the functions of a system, in order to identify and clarify the failure conditions of these functions in accordance with the severity of its effect (SILVA, 2006). It is a top-down iterative technique and the objective is to determine: how safe does the system need to be (EUROCONTROL, 2006).

The exact history of this technique is unknown however, believes that the initial studies have been carried through from 1992. In FHA according to JAA JAR-25, all system functions are systematically examined in order to identify potential failure conditions of the aircraft. SAE ARP 4761 (SAE, 1996b) made a refinement and extension of FHA present in JAA JAR-25 and covers software as well as hardware. (EVERDIJ; BLOM, 2006).

The FHA according to EATMP SAM was originally based on SAE ARP 4761 (SAE, 1996b) but, it goes further and its scope is extended to Air Navigation Systems (EUROCONTROL, 2006).

Table 2 is an example of FHA. It is part of an ATCC (Air Traffic Control Centre) building FHA, where:

- "Function" describe each of the system functions to be performed;
- "Hazard" identifies the specific hazard being postulated and evaluated for stated functional failure;
- "Effect" identifies the effect and consequences of hazard, should it occur;
- "Severity Class" is the maximum tolerable likelihood of occurrence (for example: 1 is extremely rare).
- "Comments/Remarks" is a place to record useful information regarding the hazard.

Table 2: Example of part of an ATCC building FHA (EUROCONTROL, 2006)

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BU_1	Building ATC rooms	**Total loss of ATC rooms** due to object collision (aircraft, meteorite, vehicle…), severe damage of building	Immediate evacuation of personnel. No way to operate	Total inability to provide or maintain safe ATM (Air Traffic Management) services. Loss of the service.	1	Event so unlikely to happen. It has been decided to do nothing to avoid or to mitigate this hazard (sometimes nothing can be done). This risk is classified as acceptable by management.

Than, it's possible to specify safety objectives and present them in the synthesis table – Table 3 shows an example of part of a safety objectives synthesis for the example in Table 2.

Table 3. Example of part of a safety objectives synthesis (EUROCONTROL, 2006)

Hazard Ref	Function	Hazard	Severity	Safety objectives	SO Ref
H-BU_1	Building ATC rooms	**Total loss of ATC rooms** due to object collision (aircraft, meteorite, vehicle…), severe damage of building	1	No safety Objective. As this event is so unlikely to happen, it has been decided to do nothing to avoid or to mitigate this hazard (sometimes nothing can be done). This risk is classified as acceptable by management.	SO-BU_1

3.3 Fault tree analysis (FTA)

Fault Tree analysis (FTA) was first conceived by H. A. Watson of Bell Laboratories in connection with an U.S. Air Force contract to study the Minuteman missile launch control system – circa 1961 – and in 1965, the first technical paper on FTA were presented at the first System Safety Conference, held in Seattle – USA (ERICSON, 1999).

FTA is one of the most important logic and probabilistic techniques used in PRA and system reliability assessment. It is a deductive technique whereby an undesired event (or state) of a system is analyzed in the context of its environment and operation to find all credible ways in which the undesired event – called "top-event" – can occur (USNRC, 1981). FTA is an extremely effective technique for modeling hardware failures, and efficient algorithms exist for solving large models of complex systems (MOSLEH; et al. 2004).

The fault tree itself is a graphic representation of the various parallel and sequential combinations of faults – using logical gates like "and", "or", etc. – that will result in the occurrence of the top-event, that allow a qualitative analysis. Quantitative analyses include applying Boolean algebra to the fault tree to obtain the equations for each gate of the fault tree. Figure 4 shows a typical FT. In this analysis the top-event "rupture of a water tank" will occur if either a "basic tank failure" occurs or the "relief valve jammed closed" and at least one of three events occur: "gas valve jammed closed", "controller fails to close gas valve" or "basic failure of temperature monitor".

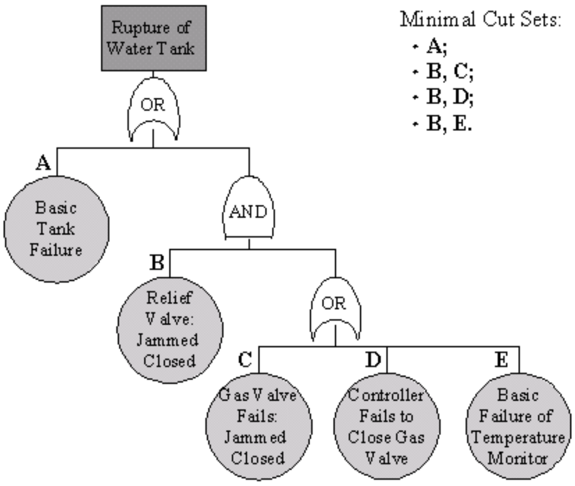
Rupture of Water Tank
OR
A
Basic Tank Failure
AND
B
Relief Valve: Jammed Closed
OR
C
D
E
Gas Valve Fails: Jammed Closed
Controller Fails to Close Gas Valve
Basic Failure of Temperature Monitor
Minimal Cut Sets:
• A;
• B, C;
• B, D;
• B, E.

Figure 4. A simplified fault tree for a domestic hot-water system (KUMAMOTO; HENLEY, 1996)

3.4 Event tree analysis (ETA)

ETA appears to have been developed during the WASH-1400 nuclear power plant safety study – around 1974 – (ERICSON, 2005) to support risk assessment and, nowadays widely used on several areas (CNPGB, 2005).

An Event Tree Analysis is an inductive technique that shows credible outcomes resulting from an initiating event, taking into account intermediary events. Usually, each event is instantiated as "occurred" or "not occurred", those results in a 2^n scenario (where "n" is the number of events).

Figure 5 shows an ET where an atmosphere leak is the initiator event. If this atmosphere leakage is not detected, is conservatively postulated to result in an LOC (Loss of Crew). If the leak is detected, the planned response is to seal the leaking compartment. Sealing the compartment engenders end state, 0K. Inability to seal the leaking compartment requires crew evacuation. A successfully evacuation results in loss of mission, otherwise in LOC (STAMATELATOS; et.al, 2002b).

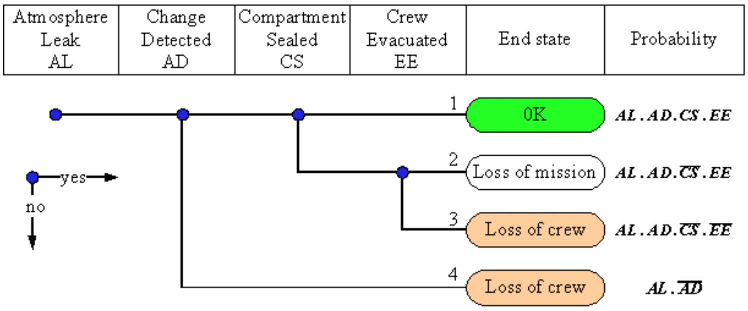

Figure 5. Atmosphere Leak ETA, considering events independent of each other
(Adapted from Stamatelatos; et.al. 2002b)

3.5 Event sequence diagram (ESD)

ESD age from 1992 or older (EUROCONTROL, 2004) and is another technique to describe an accident scenario, but is better to engineering thinking than an ET (STAMATELATOS; et.al, 2002b)[1].

An Event Sequence Diagram is a schematic representation of the sequence of events leading to different end states. Each path through this flowchart is a scenario where pivotal events are identified as either occurring or not. (STAMATELATOS; et.al, 2002b). ESDs are used to define context within which various causal factors would be viewed as hazard (MOSLEH, et al. 2004).

Figure 6 shows the same example of atmosphere leakage present in the ETA section.

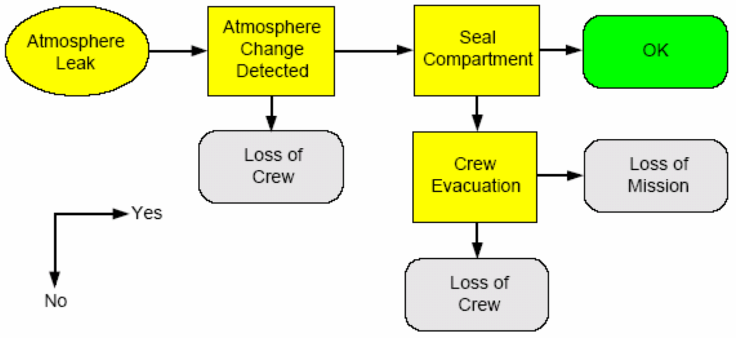

Figure 6. Atmosphere Leak ESD (STAMATELATOS; et.al. 2002b)

4. PROPOSED FRAMEWORK

The framework that is proposed in this paper, representing a generic PRA methodology, is shown in Figure 7.

The first step of this framework is to know what is in risk. Thus, it is necessary to get acquainted with the technical system (hardware and software) and its functions. To understand the technical system it is recommended to obtain (or make) documents such as lay-out; manual of equipments; electrical diagram; etc. For the functional mapping it is recommended the use of IDEF0 technique – it enhances system visualization and communication between members of the group and equalize knowledge about it.

Once system functions were identified, a Functional Hazard Analysis (FHA) can be done to determine the objectives that the system should be able to accomplish.

The next step is risk assessment – that can be divided into risk identification and analysis; and risk evaluation.

The recommended techniques to perform risk identification and analysis are FMECA, employing ESDs and ETs to analyse failure mode consequences to technical system, man and environment – either to the organization and external to it – and FTs to analyse the causes of failure modes and ESDs / ETs pivotal events.

Once system functions were identified, a FHA can be done to determine the objectives that the system should be able to accomplish.

ESD should be used to elicit expert knowledge and, than, converted into ET to perform the statistical analysis, together with FTA.

[1] Usually ESDs are used to help modeling ETs but Swaminathan and Smidts (1998) proposes an extension of the current ESDs to allow modeling of dynamic situations.

As outcomes of the risk analysis there are FMECA tables associated with ETs (that represent the chain of events leading to consequences) and FTs (that represents the causal chain), which allows a better understanding of incident scenarios and enhance knowledge management.

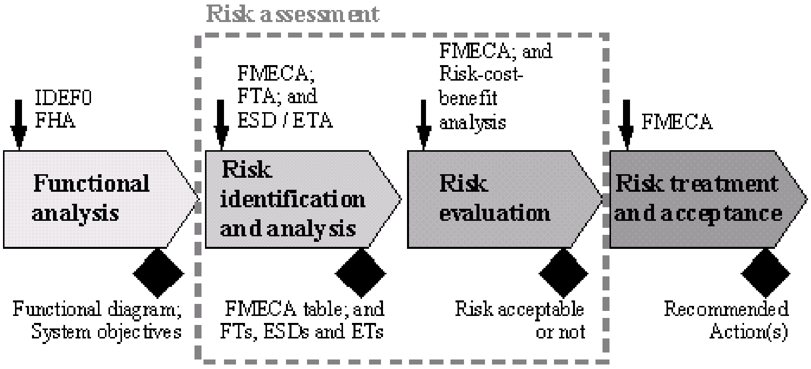
Risk assessment
IDEF0
FHA
FMECA;
FTA; and
ESD / ETA
FMECA; and
Risk-cost-benefit analysis
FMECA
Functional analysis
Risk identification and analysis
Risk evaluation
Risk treatment and acceptance
Functional diagram; System objectives
FMECA table; and FTs, ESDs and ETs
Risk acceptable or not
Recommended Action(s)

Figure 7. Proposed framework

Risk treatment refers to measures that: eliminate the hazard; reduce incident occurrence probability and / or incident intensity; transfer the risk (either contracting insurance or outsourcing the technical system); or retain it.

Risk acceptance doesn't means “do nothing”. It's possible to accept a risk in a passive or active way. Passive risk acceptance doesn't require any proactive measure, leading the organization to deal with the incident when it occurs. On the other hand, active risk acceptance means planning for the incident occurrence. This planning could be either monitoring indicators of incident occurrence, or making the organization more resilient to it (mitigating its consequences or implementing alternative processes that could maintain the function of the technical system – even with degradation).

5. CONCLUSIONS

The study presented in this paper identified that PRA is being developed during the last 50 years. However, it realizes that a structured knowledge about this issue have no more than 15 years. In fact, the necessary consensus to develop and put in effect rules and standards was only possible after the year 2000. There are a lot of uncertainties in PRA process, due mainly to the lack of relevant statistical data or because of its dependency on some qualitative evaluation, like in operation and maintenance process. Because of this, it is very hard to work with PRA. It is important to consider the particularities of the each sector of the technical system, and the human culture presents in each place where the system operates. Special attention should be given to legal and financial issues related to contingency scenarios. The authors understand that the hazards can be analysed from fragments, but the risk always requires a global analysis. It is known that the human element is involved in more than 90% of the registered risks in the technical literature. So, it is evident that the PRA should be adapted for the characteristics of each sector, but a generic framework, not biased with specific conditions of any industry, could be very useful in the beginning of its implementation and for the instruction of people that work in each technical system.

To this end a generic simplified PRA framework was proposed in this paper, which could guide PRA implementation in industries, regardless its specific characteristics. In the proposed framework, risk assessment takes, as input, the risk objectives defined in the Functional Analysis phase, to either accept the risk or not. In the next phase, Risk Treatment and Acceptance, the outcomes are a feedback for a risk assessment review and should yield Recommended Actions. Although it was pointed out some techniques to support this framework, many others could be used. For instance, hazard analysis techniques like HAZOP and “Check-lists”, may be used as input to FMECA.

7. REFERENCES

ABS, 2003. “Guide for Risk Evaluations for the Classification of Marine-Related Facilities”. American Bureau of Shipping, USA.

ANS, 2007. “ANSI/ANS-58.21-2007: External Events in PRA Methodology”. American Nuclear Society

ASME, 2002. “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, American Society of Mechanical Engineers”. New York.

CNPGB (Comissão Nacional Portuguesa das Grandes Barragens), 2005. Grupo de trabalho de análise de riscos em barragens. “1º relatório de progresso”. Lisboa: CNPGB.

ERICSON, Clifton A. II, 1999.“Fault Tree Analysis: A History”. In: 17th International System Safety Conference. Proceedings.

ERICSON, Clifton A. II., 2005. “Hazard Analysis Tecniques for System Safety”. Hoboken: John Wiley & Sons, Inc, 2005. 499 p.

EUROCONTROL, 2001. “The EUR RVSM pre-implementation safety case”. Bruxelles: EUROCONTROL.

EUROCONTROL, 2004. “Review of Techniques to support the EATMP Safety Assessment Methodology”. Bruxelles: EUROCONTROL.

EUROCONTROL, 2006. “SAM Electronic V2.1”. 03 Apr. 2007, <http://www.eurocontrol.int/safety/gallery/content/public/library/SAM/SAM_Electronic_Self_Assessment.zip>.

EVERDIJ, M. H.C.; BLOM, H. A.P., 2004. “Safety Methods Database”. Version 0.6. NLR.

IAEA, 1995.” Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2)”. International Atomic Energy Agency, Safety Series No. 50-P-8.

IMO, 1998. “Aspects of the FSA methodology. Experience gained from the trial application undertaken by the United Kingdom”. MSC 69/INF.14.

IMO, 2002a. “Bulk Carrier Safety”. Report on FSA Study on Bulk Carrier Safety, MSC 75/5/2.

IMO, 2002b. “Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process”. MSC/Circ.1023, MEPC/Circ.392, London, U.K.

IMO, 2004. “International Convention of Safety of Life at Sea – SOLAS”. Consolidated edition.

IMO, 2006. “International Convention for the Prevention of Pollution from Ships – MARPOL”. Consolidated edition.

KELLER, W., MODARRES, M., 2005, “A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen”. Reliability Engineering and System Safety 89 (2005) 271–285, Elsevier.

KUMAMOTO, H. and HENLEY, E.J., 1996. “Probabilistic Risk Assessment and Management for Engineers and Scientists”. 2nd Ed., IEEE Press.

MOSLEH, A, DIAS, A., EGHHALI, G., FAZEN, K., 2004. “An Integrated Framework for Identification, Classification and Assessment of Aviation Systems Hazards”. International Conference on Probabilistic Safety Assessment and Management (PSAM 7 and ESREL 04). Berlim, Germany. Jun 2004. Ref. H11 – Risk and Reliability Theory and Frameworks, p.34. Proceedings...

USNRC, 1981. “Fault Tree Handboo”k. NUREG-0492. Washington.

SAE (Society of Automotive Engineers), 2002. “SAE-J1739: Potential Failure Mode and Effects in Design (Design FMEA), Potential Failure Mode and Effects in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects in Machinery (Machinery FMEA)”. Warrendale.

SAE (Society of Automotive Engineers), 1996a. “SAE ARP 4754: Certification Considerations for Highty-Integrated or Complex Aircraft Systems”. Warrendale. 105 p.

SAE (Society of Automotive Engineers), 1996b. “SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”. Warrendale.

SILVA, Paulo Celso da, 2006. “A confiabilidade e a avaliação de segurança no projeto de aeronaves”. Simpósio Internacional de Confiabilidade. Salvador: Proceeding...

STAMATELATOS; et.al., 2002a. “Fault Tree Handbook with Aerospace Applications”. Ver. 1.1. Washington: NASA.

STAMATELATOS; et.al., 2002b. “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners”. Version 1.1. Washington: NASA.

TIXIER, J., Dusserre, G., Salvi O., Gaston, D., 2002. “Review of 62 risk analysis methodologies of industrial plants”, Journal of Loss Prevention in the Process Industries 15, pp.291–303, Elsevier.

DOD (Department of Defense of United States of America), 1980. “MIL-STD-1629A: Procedures for performing a Failure Mode, Effects and Criticality Analysis”.

USNRC, 1975. “Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400”. NUREG-75/014.

USNRC, 1983. “PRA Procedures Guide. A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants”. Final Report, Vol. 1-2, NUREG/CR-2300.

USNRC, 1990. “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants” NUREG-1150.

USNRC, 1995. “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities, Final Policy Statement, Federal Register”. Vol. 60, No. 158.

USNRC, 1998. “An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant Specific Changes to the Current Licensing Basis”. Regulatory Guide 1.174.

USNRC, 2003. “Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making”. NUREG/CR-6813.

WANG, J., 2001.“The current status and future aspects in formal ship safety assessment”, Safety Science 38, pp. 19-30.

WANG, J., 2002.“A Brief Review of Marine and Offshore Safety Assessment”, Marine Technology, 39, N.2, pp. 77-85.