RISK ANALYSIS MODELS IN ASSESSING THE LEVEL OF STRUCTURAL INTEGRITY-SIL

Costin Ilinca[1], Liviu Toader[2], Gheorghe Spireanu[3], Nicolae Persicanu[4], Serban Iacob[5], Virgil Dumbrava[6]

The scope of a safety analysis is to ensure that the risks that could be a potential source of harm, damage of property and degradation of the environment, are sufficiently minimized by addressing all the relevant safety lifecycle stages including the design, implementation, operation, and maintenance through to decommissioning.

Keywords: risk analysis, structural integrity level, fault tree analysis

1. Introduction

Unusual technological development of last decades has given a great importance to certain domains and industrial fields – thermo energetic industry, nuclear energetic, chemical and petrochemical industries and so on – characterized by the usage of highly performing and complex technological equipments, in the context of development of sententious technological processes.

The effective exploitation of the used technological lines and units – this meaning their quasi – continuous functioning, by significantly decreasing the pitfalls due to certain malfunctioning - in the circumstances of corresponding protection of the employed staff's health as well as of population 's health, as well as in the context of protecting the environment, needs ensuring (in the conception and execution stages) and maintaining (during technological exploitation) high degrees of reliability and technical security[4].

In such a context, relatively recently, as an individual branch of Science has risen the Theory of Reliability, which deals both with substantiating qualitative and quantitative analysis methods and approaches of behaviour of exploited technical/technological systems, and with general measures study,

[1] Phd.Lecturer.,Oil and Gas University, Ploiesti, Romania
[2] Phd.Lecturer.,Oil and Gas University, Ploiesti, Romania
[3] Eng., IPA, Bucuresti, Romania
[4] Eng., ISPE, Bucuresti, Romania
[5] Eng., ISPE, Bucuresti, Romania
[6] Assoc. Prof., PhD, University "Politehnica", Bucuresti, Romania,

which have to be taken into consideration when operating these, in order to assure a maximum efficiency in exploitation.

2. Risk analysis models

Generally speaking, the technical risk characterises an undesirable event - specific to technical/technological system's exploitation and associated with a potential danger state of the system – by probability (ρ, $0 \leq \rho \leq 1$) of the event occurrence, by gravity (G a) of its consequences and by the level of detection (D) of the event. According to this interpretation, a so- called structural equation may be realised, as mentioned below[2,4]:

$$\underbrace{\text{RISK}}_{\text{Technical risk}} = \underbrace{\text{G}}_{\text{Gravity}} \times \underbrace{\rho}_{\text{Probability}} \times \underbrace{\text{D}}_{\text{Detectability}}$$

Any risk analysis method needs two different approaches: analytical and systemic approach. The analytical character is given by the necessity of a systematized and rigorous analysis of the investigated technical/technological system – that is to outline the subsystems /component elements and to study their constructive and functioning characteristics – in order to identify possible faults which may occur during its exploitation stage[1].

As a result of substantiating some evaluation/appreciation criteria of technical accident gravity consequences – materialized in the adoption of a conventional scale of gravity G – and of imposing (establishing) their acceptability limits, in the coordinators plan ρ - G, the main characteristic fields of technical risk may be defined:

a) **The negligible risk field**, usually associated with proper faults or minor damages (with reduced degree of gravity), rare and very rare (with reduced probability, respectively much reduced probability of occurrence);
b) **The acceptable risk field**, characteristic of frequent minor faults (with high probability occurrence) or major faults (with high gravity consequences), rare and very rare;
c) **The unacceptable risk field**, characteristic of possible or frequent major faults (with occurrence probability that needs to be taken into consideration).

The cost of performing the hazard identification step depends on the size of the problem and the specific techniques used. Techniques such as what-if analyses or checklists tend to be less expensive than other more structured methods. Hazard and operability (HAZOP) analyses, failure modes and effects analyses (FMEA) and fault tree analyses (FTA) involve many people and tend to be more expensive.

However, no technique can guarantee that all hazards or potential accidents have been identified.

Performing a quantitative risk analysis, involves the next steps:

- Hazard identification
- Consequence analysis
- Frequency analysis
- Risk evaluation and presentation

The experience gathered in engineering established many methods – already known as classical ones- for analysing technical/technological risk.

The following are mentioned[2,4]:

a) **What if** – substantiated on the multitude of questions which are spontaneously asked by the study group of the discussed case; it is an unstructured method, limited by time, based on the experience of the people who formulate the questions, having an important subjective structure;

b) Checklist – based on a pre-established checking list, which values the gathered experience in the respective field; the list structure is not universal (generally valid), being complete only when there exits a rich and systematized data base, that is information about similar cases; however, the checking lists cannot be mechanically 'important' from one case to another, as they only facilitate the identification of certain risks involved in the technical/technological system which is investigated;

c) **Hazard and Operability Study (HAZOP)** - substantiated on a systematized (structured) investigation of the inaccuracies which may appear when a known technical/technological system is being used, in all its stages (conception, realization and exploitation), this presupposing the constitution of a study model; it is a flexible method which may be used in new (atypical) situations, and which stimulates the analysis and guarantees an appropriate conception on the studied system; the disadvantages of this approach lay, on the one hand, on the fact that its success depends on the analyst's qualifications, and , on the other hand on the considerable time which may be spent.

d) **Fault Mode and Effect Analysis (FMEA)** – is based on the analysis of possible faults/ giving ups of each individual part of the system; the method's limits are imposed by the stages of analysis procedure and/or by the number of parts of the investigated technical/technological system; it needs a proper and accurate modelling, but it has a high degree of generality, being perfectly available in new (atypical) case; the method's success depends on the analyst's experience and training.

FMECA aims are:

a) evaluation of effects and successions of events resulted from any known failure mode of parts belonging to different levels of the system;
b) showing potential faults and identification of their effects;
c) determining the importance or criticality for each fault, taking into account its influence on normal working or on performance level of the system or

unit which is a part of the system, as well as evaluation of the impact on reliability or security of the process;

d) Classification of known fault modes taking into account the following: the facility which may be used in identifying, diagnosing and stimulating them; the necessary means for maintaining the system working (preventive, corrective, etc. maintenance) and any other pertinent characteristics.

e) Evaluation of significance degree of faults and their possibilities of occurrence, on condition that all the necessary information is known.

The standards and recommendations frequently used at international level in order to realise a FEMEA/FEMECA analysis are the following[1,2]:

• **MIL-STD1629A:** Procedures for Performing a Failure Mode Effects and Criticality Analysis, US Department of Defence, Washington, DC, August 1998;

• **SAE Aerospace Recommended Practice ARP5580**: Recommended Failure Modes and effects Analysis (FEMEA). Practices for Non-Automobile Applications. SAE International, Warrendale, PA, 2001;

• **SAE Surface Vehicle Recommended Practice J1739**: Potential Failure Mode and effects in Design (Design FEMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FEMEA) and Potential Failure Mode and Effects Analysis for Machinery (Machinery FEMEA), SAE International, Warrendale, PA, 2000

e) **Faults Tree Analysis** (FTA) – is based on formulating a logical model (that is faults tree) of the investigated technical/technological system; the method mainly outlines the continuity of the faults, whose final point is a technical accident; the results of this type of analysis (faults trees) may be used in the identification and evaluation of possible consequences of a fault, in the quantification of occurrence possibilities of technical accidents and in the choice of methods, means and their occurrence prevention; the main disadvantage of this method is the important data quantity needed for the evaluation.

FTA is a logical method of deduction utilizing a graphical depiction of events, faults, or logical combinations (Boolean expressions such as AND, OR, etc.) thereof. It begins at the top of the fault tree with an undesirable event. Next, the possible events and logical combinations are developed for the fault tree until the root causes are determined. The root causes can be triggering events or basic faults. It is best to use fault trees on the major events because the trees can grow quite large. FTA can be applied to hardware and to operational modes of the system (i.e., startup, operation, maintenance, and shutdown).

Fault trees are suited to analysis of static situations; thus, dynamic situations involving timing are difficult to implement. Also, fault trees can be qualitative or quantitative. A quantitative fault tree uses probabilities for the

events and faults. Finally, the traditional fault tree for the system hardware has been extended to software fault-tree analysis. This is best suited for analysis of the most critical software at the module level of detail. There is a standard set of graphical symbols to construct the tree. Additional symbols are used for special situations.

3. Safety integrity level and risk evaluation models

The level of risk is used to determine which hazards have an unacceptable risk and which have acceptable risks. Once the risks are identified, the safety performance or degree of safety to mitigate risk is determined. The safety performance is quantified by assignment of a level 1, 2, or 3, where 3 is the highest degree of safety performance. These levels are called safety integrity levels (SILs).

BS EN 61508 offers the next methods of determining SIL requirements:

· Quantitative method.

· Risk graph, described in the standard as a qualitative method.

· Hazardous event severity matrix, also described as a qualitative method.

BS IEC 61511 offers:

· Semi quantitative method.

· Safety layer matrix method, described as a semi-qualitative method.

· Calibrated risk graph, described in the standard as a semi-qualitative method, but by some practitioners as a semi-quantitative method.

· Risk graph, described as a qualitative method.

· Layer of protection analysis (LOPA). (Although the standard does not assign this method a position on the qualitative / quantitative scale, it is weighted toward the quantitative end).

Safety integrity is defined as "The probability of a Safety Instrumented Function satisfactorily performing the required safety functions under all stated conditions within a stated period of time."

Safety integrity consists of two elements: 1) hardware safety integrity and 2) systematic safety integrity.

Hardware safety integrity which is based upon random hardware failures can normally be estimated to a reasonable level of accuracy.

ANSI/ISA-84.01-1996[3] addresses the hardware safety integrity by specifying target failure measures for each SIL. For SIF operating in the demand mode the target failure measure is PFDavg (average probability of failure to perform its design function on demand).

PFDavg is also commonly referred to as the average probability of failure on demand. Systematic integrity is difficult to quantify due to the diversity of causes of failures; systematic failures may be introduced during the

specification, design, implementation, operational and modification phase and may affect hardware as well as software. ANSI/ISA-84.01-1996 addresses systematic safety integrity by specifying procedures, techniques, measures, etc. that reduce systematic failures.

The FTA process begins with the determination of the Top Event[3]. For SIL determination, the Top Event is the probability of the SIF to fail on process demand for a given safety function. Fault trees can also be constructed to determine the potential for the SIF to spurious trip. The structure of the fault tree is different for SIL determination and spurious tripping, so the Top Event to be modeled must be defined prior to proceeding with the fault tree analysis.

A process unit often has more than one safety function that will require SIL determination. Each safety function has a defined Top Event that is associated with a specific process hazard that has been identified by the Process Hazards Analysis (PHA)[3].

The Top Event will, in turn, have failure logic associated with the event that can be modeled in a Fault Tree.

6. Conclusions

Any risk analysis method needs two different approaches: analytical and systemic approach. The analytical character is given by the necessity of a systematized and rigorous analysis of the investigated technical/technological system – that is to outline the subsystems /component elements and to study their constructive and functioning characteristics – in order to identify possible faults which may occur during its exploitation stage. The systemic character of an evolved risk analysis method lays in the necessity of outlining the existing connections and interactions both at the level of the subsystems /component elements and between the investigated technical/technological system and other connected systems, in order to identify possible scenarios of technical accidents occurrence and risks evaluation.

R E F E R E N C E S

[1]. *C. Ilinca, D. Paraschiv* „Managementul riscului tehnic si tehnologic - Risc tehnic/tehnologic in transportul feroviar al HGL". EdituraTerra.Focsani, 2006.

[2]. *C. Ilinca, I. Ristea, A. Pavel* „Risk, Reliability, Monitoring and Technical Diagnosis Analises Applied in Industry", Buletinul Asociației Române de Mecanica Ruperii, 2005.

[3]. ***- ISA-TR84.00.02-2002, „Safety Instrumented Functions" (SIF) – Safety Integrity Level Evaluation Techniques, Part 1: Introduction; Part 2: Determining the SIL of a SIF via Simplified Equations; Part 3: Determining the SIL of a SIF via Fault Tree Analysis.

[4]. *A. Pavel, D. Popescu* „Managementul riscului tehnic-tehnologic. Metoda MADS-MOSAR". Bucureşti, Editura Briliant 1998.