# Review of Available System Safety Assessment Tools and Techniques-Integrated Approaches for Accident Prevention in Process Industry

Praveen Patel
*Associate Professor, Department of Fire Technology & Safety Engineering*
*Institute of Engineering & Science IPS Academy, Indore, M.P., India.*

Dr. Nagendra Sohani
*Associate Professor, Institute of Engineering & Technology DAVV, Indore, M.P., India*

**Abstract- An individual technique cannot achieve the optimum system safety assessment result in the work places. Many techniques have been developed to undertake the system safety assessment on a process industry. In order to understand their application it is very essential to examine the available documentation in the form of input data, methods used and decision as output data of a particular system. In particular the system safety assessment techniques are classified into three main categories: (i) the qualitative (ii) the quantitative and (iii) the hybrid techniques which is qualitative-quantitative, semi-quantitative the objective of this paper is to review the available system safety assessment techniques and their classification. This paper also highlights the problem in taking into account during the system safety assessment with the application fields and the main limitations of these techniques.**

**Keywords – System safety assessment, quantitative and qualitative system safety assessment techniques, hazard evaluation techniques, Occupational accidents.**

## I. INTRODUCTION

System safety is a specialty within system engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety. The goal of System Safety is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence. The System Safety assessment is an essential and systematic process for assessing the impact, occurrence and the consequences of human activities on systems with hazardous characteristics. The diversity in risk assessment techniques is such that there are many appropriate techniques for any circumstance and the choices have become more a matter of taste.

To cope up with major accidents, a previous analysis should be done. The forward-looking system safety analysis permits an exhaustive identification of potential hazardous sources to prevent accident scenarios and to assess potential impact on human, environmental and equipment targets in order to propose prevention or protection. The system safety assessment methodologies focus on the main hazard sources. Two principal sources of system safety can be first industrial establishment and second transport of dangerous goods. These two types of sources are quite different. At first sight, the quantities involved are not really comparable, and the environment is unsettled for an industrial site whilst the opposite is true for the case of transport of dangerous goods. So to analyze and to manage safety aspects, various approaches are proposed, they focus on organizational and technical features.

.

## II. CONCEPT OF SYSTEM SAFETY ASSESSMENT

Hazards are the potential for harm. They are unsafe acts and/or unsafe conditions that can result in an accident. An accident is usually the result of many contributors (or causes) and these contributors are referred to as either initiating or contributory hazards. Depending on the context of the discussion, either hazards or their associated risks are referred to that accident has a specific credible worst case severity. If the hypothesized accident's outcome changes, the scenario changes, and as a result, a different risk must be considered. The steps in a risk assessment are:

· Hypothesize the scenario.
· Identify the associated hazards.
· Estimate the credible worst case harm that can occur.
· Estimate the likelihood of the hypothesized scenario occurring at the level of harm (severity).

Fig 1 shows the sequence of events that could cause an accident from a fuel tank rupture on board an aircraft. There are a number of contributory hazards associated with this event: fuel vapor present, ignition spark, ignition and tank over pressurization, tank rupture and fragments projected. The contributors associated with this potential accident involve exposed conductors within the fuel tank due to wire insulation degradation, and the adequate ignition energy present. The outcome could be any combination of aircraft damage, and/ or injury, and/or property damage.

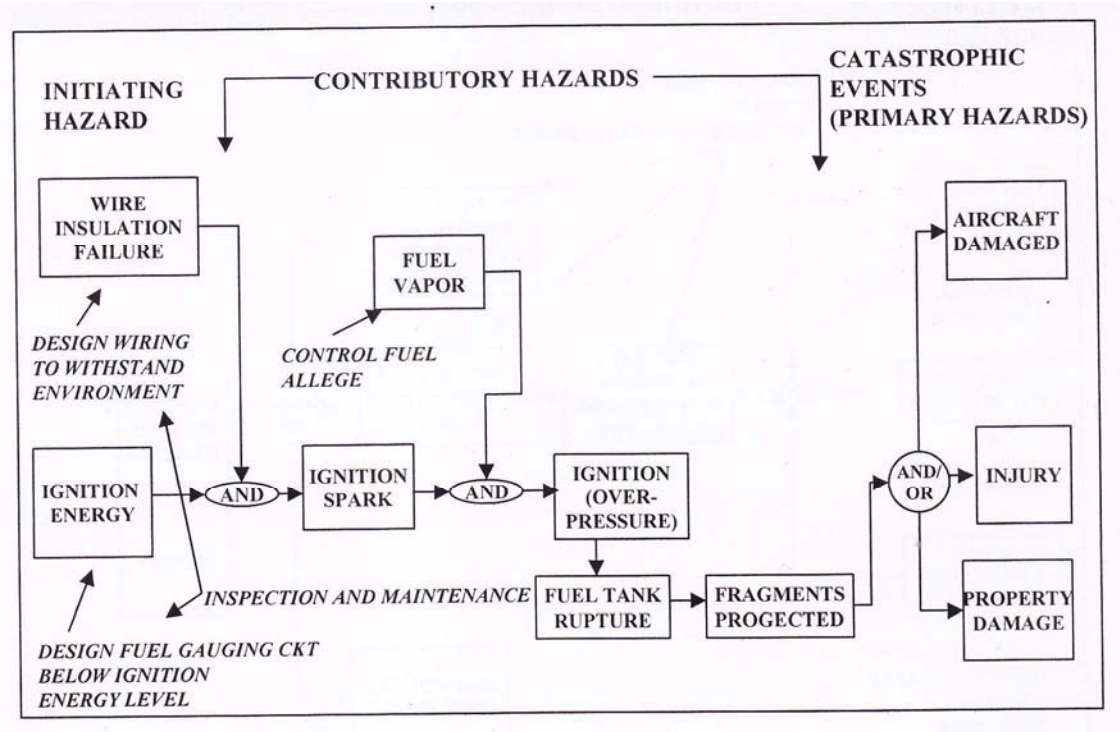


Fig 1 Fuel tank Rupture scenario

## III. TYPES OF TECHNIQUES

The available techniques can be sorted out in two principal groups, one qualitative and the other quantitative. Each group can be divided into three categories first only deterministic, second only probabilistic and in last a combination of deterministic and probabilistic approach.

The deterministic techniques take into consideration the products, the equipment and the quantification of consequences for various targets such as people, environment and equipment. The probabilistic techniques are based on the probability or frequency of hazardous situation on the occurrence of potential accident. The probabilistic techniques are mainly focused on failure probability of equipment or their components. On the one hand, probabilistic methods are used to lead an analysis on a restricted part of a plant. On the other hand, deterministic and combined deterministic and probabilistic techniques are used to analyze the whole industrial establishment.

The classification of the techniques is based on the type of output data. In each category, techniques can be ranked from the simple, which comprises only one step to the more complex ones that are based on the three steps (identification, evaluation and hierarchy phases). The complex techniques are generally composed of modules issued from simple methods and other modules are added in order to realize a more complete system safety analysis with easier results to analyze.

In Table 1, various techniques are ranked according to the four defined criteria. The great majority of techniques are deterministic, because historically operators and public organizations have initially tried to quantify damages and consequences of potential accidents, before to understand why and how they could occur.

Table 1Classification of System Safety Assessment Techniques

| System Safety Assessment Techniques | | | | |
|---|---|---|---|---|
| | S No | Qualitative Techniques | S No | Quantitative Techniques |
| | | | | |
| **Deterministic approach** | 1 | **Action Errors Analysis AEA (Rogers, 2000)** | **31** | **Accident Hazard Analysis AHI (Khan & Abbasi, 1997b; Khan & Abbasi, 1998a)** |
| | 2 | **Checklist Khan & Abbasi, 1998b** | **32** | **Annex 6 of SEVESO II Directive (La directive Seveso II: Annexe 6, 1997)]** |
| | 3 | **Concept Hazard Analysis CHA (Rasmussen & Whetton, 1997; Rogers, 2000)** | **33** | **Chemical Runaway Reaction Hazard Index RRHI (Kao & Duh, 1998)** |
| | 4 | **Concept Safety Review CSR (Rogers, 2000)** | **34** | **Dow's Chemical Exposure Index CEI (American Institute of Chemical Engineers, 1994)** |
| | 5 | **Failure Mode Effect Analysis FMEA (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000)** | **35** | **Dow' Fire and Explosion Index FEI (American Institute of Chemical Engineers, 1987; Khan & Abbasi, 1998a)** |
| | 6 | **Goal Orinted Failure Analysis GOFA (Rogers, 2000)** | **36** | **Fire and Explosion Damage Index FEDI (Khan & Abbasi, 1998a)** |
| | 7 | **Hazard and Operability HAZOP (Kennedy & Kirwan, 1998; Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000; Tweeddale, Cameron, & Sylvester, 1992)** | **37** | **Hazard Identification and Ranking HIRA (Khan & Abbasi, 1997b; Khan & Abbasi, 1998b)** |
| | 8 | **Human Hazard and Operability Human HAZOP (Kennedy & Kirwan, 1998)** | **38** | **Instantaneous fractionnal loss index IFAL (Khan & Abbasi, 1998a; Khan & Abbasi, 1998b)** |
| | 9 | **Insurers involvement in risk reduction process (Sankey, 1998)** | **39** | **Methodology of domino effects analysis (Dolladille, 1999)]** |
| | 10 | **Manager (Pitblado, Williams, & Slater, 1990)** | **40** | **Methods of potential risk determination and evaluation (Ja¨ger & Ku¨hnreich, 1998)** |

(Table-1 Continued )

| System Safety Assessment Techniques | | | | |
|---|---|---|---|---|
| | S No | Qualitative Techniques | S No | Quantitative Techniques |
| Deterministic approach | 11 | Optimal Hazard and Operability Opt HAZOP (Khan & Abbasi, 1997a; Khan & Abbasi, 1998b | 41 | Mond Fire Explosion and Toxicity Index FETI (Khan & Abbasi, 1998a; Khan & Abbasi, 1998b) |
| | 12 | Plant Level Safety Analysis PLSA (Toola, 1992) | 42 | SAATY methodology (Troutt & Elsaid, 1996) |
| | 13 | Potential domino effects identification (Delvosalle, Fievez, & Benjelloun, 1998) | 43 | Toxic Damage Index TDI (Khan & Abbasi, 1998a) |
| | 14 | Preliminary Risks Analysis PRA (Nicolet- Monnier, 1996; Rogers, 2000;) | | |
| | 15 | Process Risk Management Audit PRIMA Hurst, Young, Donald, Gibson, & Muyselaar, 1996 | | |
| | 16 | Profile Deviation Analysis PDA (Korjusiommi, Salo, &Taylor, 1998) | | |
| | 17 | Safety related questions for computer controlled plants (Chung, Broomfield, & Yang, 1998; Yang & Chung, 1998) | | |
| | 18 | Seqhaz Hazard Mapping SHM (Korjusiommi et al., 1998) | | |
| | 19 | Sneak Analysis (Rogers, 2000) | | |
| | 20 | Task Analysis TA (Rogers, 2000) | | |
| | 21 | What if? Analysis (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000) | | |
| | 22 | World Health Organisation WHO (Khan & Abbasi, 1998b) | | |
| Probabilistic approach | 23 | Accident Sequences Precursor ASP (Holmberg, 1996) | 44 | Defi method (Rogers, 2000) |
| | 24 | Delphi Technique (Rogers, 2000) | 45 | Event Tree Analysis ETA (Gadd, Leeming, & Riley, 1998; Nicolet-Monnier, 1996; Rogers, 2000; Tiemessen & van Zweeden, 1998;) |
| | 25 | Earthquake safety of structures and installations in chemical industries (Jezler, 1998) | 46 | Fault Tree Analysis FTA (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000) |
| | | | 47 | Maintenance Analysis MA (Rogers, 2000) |
| | | | 48 | Short Cut Risk Assessment SCRA (Rogers, 2000) |
| | | | 49 | Work Process Analysis Model WPAM (Davoudian, Wu, & Apostolakis, 1994) |
| Deterministic and probabilistic approaches | 26 | Maximum Credible Accident Analysis MCAA (Khan & Abbasi, 1998b) | 50 | AVRIM2 (Ham, van Kessel ,& Wiersma, 1998) |
| | 27 | Reliability Block Diagram RBD (Rogers, 2000) | 51 | Facility Risk Review (Schlechter, 1996) |
| | 28 | Safety Analysis SA (Khan & Abbasi, 1998b) | 52 | Failure Mode Effect Criticality Analysis FMECA (Rogers, 2000) |
| | 29 | Safety Culture Hazard and Operability SCHAZOP (Kennedy & Kirwan, 1998) | 53 | IDEF3 (Kusiak & Zakarian, 1996; Larson & Kusiak, 1996) |
| | 30 | Structural Reliability Analysis SRA (Rogers, 2000) | 54 | International Study Group on Risk Analysis ISGRA (Khan & Abbasi, 1998b) |
| | | | 55 | IPO Risico Berekening Methodiek IPORBM (Tiemessen & van Zweeden, 1998) |
| | | | 56 | Method Organised Systematic Analysis of Risk MOSAR (Perhillon, 2000; Rogers, 2000) |
| | | | 57 | Optimal Risk Assessment ORA (Khan & Abbasi, 1998b) |

Table-1 Continued )

| System Safety Assessment Techniques | | | | |
|---|---|---|---|---|
| | S No | **Qualitative Techniques** | S No | **Quantitative Techniques** |
| **Deterministic and probabilistic approaches** | | | **58** | **Probabilistic Safety Analysis PSA (Khan & Abbasi, 1998b; Papazoglou, Noivolianitou, Aneziris, & Christou, 1992)** |
| | | | **59** | **Quantitative Risk Assessment QRA (Khan & Abbasi, 1998b; Leeming & Saccomanno, 1994; Oien, Sklet, & Nielsen, 1998; Puertas, Sanz, Vaquero, Marono, & Sola, 1998; Rogers, 2000)** |
| | | | **60** | **Rapid Ranking RR (Larson & Kusiak, 1996Tweeddale et al., 1992)** |
| | | | **61** | **Rapid Risk Analysis Based Design RRABD (Khan & Abbasi, 1998)** |
| | | | **62** | **Risk Level Indicators RLI (Oien et al., 1998)** |

## IV RELATIONSHIP BETWEEN AVAILABLE INPUT, OUTPUT AND TECHNIQUES WITH IN SYSTEM

Now, it is relevant to underline how relationship between available input, output and techniques are running. Fig2 can be used according to whether the user expects some results or has some available data:
First, if industrialists need a certain type of results, then they will read through the results (output data) columns given in fig 2. So different types of techniques are proposed and finally the necessary input data can be identified
Secondly, if only several input data are available, then the user will read through the input data columns given in fig 2 .The combination of available input data permits the identification of methods which are conceivable to use in the risk analysis. Fig 2 is a synthesis of this study and a tool for an identification of techniques which could be used according to objectives and available input data. The analysis of fig 2 highlights that many input data are necessary to realize qualitative and deterministic risk analysis, quantitative and deterministic risk analysis, and quantitative and deterministic and probabilistic risk analysis.

Whatever qualitative or quantitative Techniques, results are complete when both deterministic and probabilistic techniques are used. Probabilistic techniques need some input data, but they do not take into account some specificities of the industrial establishment like Policy or Environment. Now, the running of techniques has been brought to the fore, and it is necessary to discuss two important points: on the one hand, the application fields of those techniques and on the other hand, their main limitations.

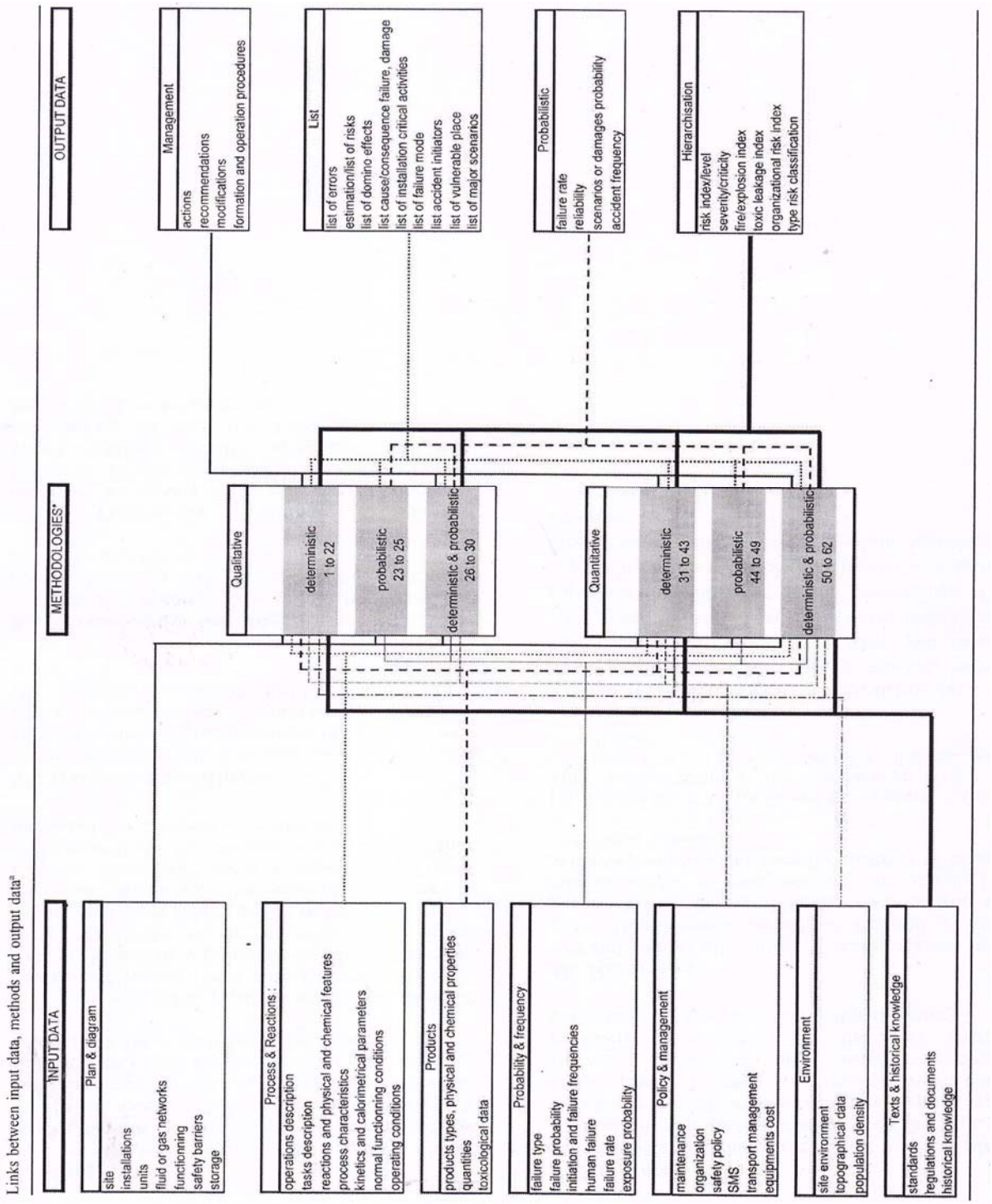


Fig 2 Relationship between available input, output and techniques with in system

## V. APPLICATION FIELDS OF TECHNIQUES

The application field of these different Techniques can be ranked into three categories (Table 2). First, this is the most important in number of developed techniques, concerns industrial site. Generally, some techniques are developed for specific application or process and they are not transposable to different types of industrial establishment. The second application field is the transportation of dangerous goods and the third one permit to take into account human factors in a specific environment.

Table 2 Application fields of System Safety Assessment Techniques

| S.No | Applied field | System Safety Assessment Techniques |
|---|---|---|
| 1. | Industrial Site | Accident Hazard Analysis AHI (Khan & Abbasi, 1997b; Khan & Abbasi, 1998a) |
| | | Event Tree Analysis ETA (Gadd et al., 1998; Nicolet-Monnier, 1996; Rogers, 2000; Tiemessen & van Zweeden, 1998) |
| | | Failure Mode Effect Analysis FMEA (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000) |
| | | Fault Tree Analysis FTA (Khan & Abbasi, 1998b;Nicolet-Monnier, 1996; Rogers, 2000) |
| | | Hazard and Operability HAZOP (Kennedy & Kirwan, 1998; Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000; Tweeddale et al., 1992;) |
| | | Hazard Identification and Ranking HIRA (Khan & Abbasi, 1997b; Khan & Abbasi, 1998b) |
| | | Methodology of domino effects analysis (Dolladille, 1999)] |
| | | Quantitative Risk Assessment QRA (Alonso & Gavalda, 1998; Khan & Abbasi |
| | | Short Cut Risk Assessment SCRA (Rogers, 2000) |
| 2. | Transport | Checklist (Khan & Abbasi, 1998b) |
| | | Failure Mode Effect Analysis FMEA (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000) |
| | | Fault Tree Analysis FTA (Khan & Abbasi, 1998b;Nicolet-Monnier, 1996; Rogers, 2000) |
| | | What if? Analysis (Khan & Abbasi, 1998b; Nicolet-Monnier, 1996; Rogers, 2000) |
| 3. | Human | Action Errors Analysis AEA (Rogers, 2000) |
| | | Human Hazard and Operability HumanHAZOP (Kennedy & Kirwan, 1998) |
| | | Task Analysis TA (Rogers, 2000) |
| | | Work Process Analysis Model WPAM (Davoudian et al., 1994) |
| | | Process Risk Management Audit PRIMA (Hurst et al., 1996) |

## VI. LIMITATIONS OF TECHNIQUES

The main limitations of those techniques can be summarized in the following points.

- The more general the technique is, the less it takes into account the specificities of the studied case.
- On the contrary, if the technique is too specific it will be less transposable to another case.
- Knowledge of people, who are participating in the system safety assessment, is quite important (different types of competences and levels of people involvement).
- For probabilistic analysis, the validity of data is a decisive parameter.
- The updating of data takes a lot of time work.
- For some techniques, the operational application is difficult to realize because of the lack of description.
- It is useful to provide a guide book to explain how techniques could be used.
- The complexity of techniques requires specific training for their implementation.
- It can be noticed that there is a great disconnection between system safety assessment techniques and human factors.

## VII.CONCLUSION

The use of system safety assessment techniques contributes to the prevention of accidents and to the preparation for emergency response. This paper highlights on the review of these techniques underlines the difficulty in taking in to account all risks for an industrial site. This paper highlights the different types of input data, methods, output data and their inter relation ship. A system safety assessment technique can be simple and only focus on the identification of hazards or a combined system safety analysis. A combined system safety analysis can be composed of several simple system safety assessment techniques, with an identification, estimation and hierarchy phases in order to obtain a system safety level index.

The application fields of techniques are industrial site, transport of hazardous goods and human factors. The human factor safety analysis is often disconnected with classical safety analysis that is due to the complexity of human safety analysis. The types of results are recommendations, lists, safety level index, event frequency and damage probability.

The mentioned techniques show that there is not a uniqueness of technique to realize a system Safety assessment. On the contrary, it is necessary to combine several techniques .The application of these techniques requires experience to obtain good results. In fact, the acquired knowledge through the analysis of these techniques can constitute a starting point to elaborate a new methodology. Such methodology presents an overall process of system safety assessment in order to provide some ways of improvement and help in decision-making

## REFERENCES

[1] FAA's System Safety Handbook(2000). *Federal Aviation Administration.*
[2] Holmberg, J. (1996). Risk follow up by probabilistic safety assessment-experience from a finish pilot study. *Reliability Engineering and System Safety*, *53*, 3–15.
[3] *J. Tixier et al. (2002),* Review of 62 risk analysis methodologies of industrial plants *Journal of Loss Prevention in the Process Industries 15, 291–303.*
[4] Khan, F. I., & Abbasi, S. A. (1997a). OptHazop—an effective and optimum approach for Hazop study. *Journal of Loss Prevention in the Process Industries*, *10*(3), 191–204.
[5] Khan, F. I., & Abbasi, S. A. (1998b). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries*, *11*, 261–277.
[6] Toola, A. (1992). Plant level safety analysis. *Journal of Loss Prevention in the Process Industries*, *5*(2), 119–124.