CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4; **ISSN** 2283-9216
DOI: 10.3303/CET2290036

Holistic review of Risk Assessment Methodologies

Alexis Pey[a,*], Marc Steinkrauß[b]

[a] Stahl Holdings bv, Pol. Ind. Llevant, c/ Llevant 7 - 08150 Parets del Vallès (Spain)
[b] TÜV SÜD Schweiz, Mattenstrasse 22, CH-4058 Basel (Schweiz)
alexis.pey@stahl.com

The evolution of risk identification and risk assessment practices lead to a situation where several methodologies are usually required to go through a complete process from a project management and engineering design point of view.
As well, the evolution of technology and tools, especially in relation with data mining, fuzzy data and model fitting, allows introducing new criteria and considerations in elements of risk assessment methodologies which were formerly determined in a rather simple way.
The paper will define, in first place, the common elements and underlying structure of the methodologies most commonly involved in risk assessment practices: HAZOP, ZHA, FTA, FMEA, Event Tree, LOPA, SIS-SIL. Understanding the application and aim of each methodology allows finding clear relations that help to integrate them in an effective and clear way.
Having a holistic view on the structures and relations of risk assessment methodologies is paramount to define risk assessment practices in a company and define an effective and reliable practices risk assessment. It has many times said that systems should help people to work and not determine the way people work. This is also applicable to risk assessment methodologies.
The paper will also define the principles and conditions that need to be considered to streamline the integration of methodologies. In this sense the boundary conditions of each methodology will be described and the characteristics of the interfaces between them defined.
Finally, considerations will be presented which may lead to risk acceptance by systematically underestimating the risk level. In view of the authors, these considerations should lead to a review of current common criteria and rules applied in some risk assessment methodologies.

1. Introduction

Organisations, processes and facilities are defined by the decisions taken in the teams conceiving, designing, implementing and managing them. In many cases, conclusions and actions that are finally put in practice are reached during risk assessments processes and they provide the foundation that justify such decisions.
It is quite common that several methodologies are required to conclude a full risk assessment process, for this reason, understanding the fundamentals of risk assessment methodologies is paramount for organisations to integrate these processes effectively and efficiently into their safety management systems.
Risk assessment methodologies shall be seen as tools having the aim to provide an effective support during the task of identifying and assessing risks throughout conception, engineering, development and life of a facility. A risk assessment methodology is a tool. Hence, it needs to serve a purpose, which, in fact, justifies its existence.
The description of the needs, facts and conditions that justify the existence of a methodology need to be clear. From these explanations, the methodological principles and structure design are derived and its application boundaries and/or scope can be clearly defined.
In the following points, the structure and elements of risk assessment methodologies are described.

Paper Received: 10 February 2022; Revised: 30 March 2022; Accepted: 3 May 2022
Please cite this article as: Pey A., Steinkrauß M., 2022, Holistic review of Risk Assessment Methodologies, Chemical Engineering Transactions, 90, 211-216 DOI:10.3303/CET2290036

2. Systematics

In any risk assessment methodology, it is crucial to understand the systematics by which the methodology is governed. The aim of a methodology is to ensure completion in terms of hazard identification and assessment, meaning that after the methodology is applied no relevant situation is left unidentified within the defined scope of the application nor wrongly assessed. However, systematics also defines the degree of freedom by which hazards can be identified and assessed.

As an example of a very open methodology, it is possible to mention a brainstorming with no structure in the identification of hazards and description of conclusions. On the other hand, as an example of a closed methodology one could mention a checklist with binary answers.

A very open or closed methodology may not provide enough guarantees in terms of hazard identification and assessment completion, in one case because discussion is not structured enough so it is easy to forget something, in the other case because discussion is so tight that even if some hazard is known is not possible to reflect it in the assessment.

The degree of freedom in terms of identification of hazards and argumentation for solutions needs to be defined as a function of the purpose and scope of the methodology.

Typically, systematics also defines the morphology of the methodology and, therefore, defines the way in which the identification and assessment is done, making the methodology more simple or complex from a cognitive point of view. Consequently, it is important that the methodology considers the way it will be implemented in an organisation and who will be the final users. This means considering the selection of participants a risk assessment meeting, the team in charge of filling in a form in the field, the team in charge to assess a change on the spot due to an equipment failure, etc.

3. Scenario definition

After a near miss, close call or mishap, “What happened?” is often one of the first questions being asked and the expectation is to get an explanation of the event (the so-called root cause) that lead to the undesired situation, the chain of subsequent events, and what have been the consequences, which considered as a whole defines a scenario. (CCPS, 2001)

3.1 Causes

In risk assessment methodologies, these events are usually referred to as root causes, conditions, deviations, failures, circumstances, etc. In any case, at some point in a risk assessment methodology, the necessary events that will trigger a scenario will be considered and, again, depending on the scope and aim of the risk assessment they will be pre-defined and developed in more or less detail.

As a remark, a risk assessment and a near miss or mishap investigation methodology may be defined by the same structure, being the only difference that, in risk assessment, prediction and induction are done on what needs to happen to lead to some consequences, while, in an accident investigation, deduction is used instead of prediction and induction. In a risk assessment, events are projected forward, while investigating an accident, events are projected backwards.

In any case, the definition of cause-consequence relations requires knowledge, which is mainly linked to one of the next areas:

Processes

A process is defined as a set of physical and/or chemical conditions that define the way in which we intend the substances to behave.

Assets

Assets are defined as a set of facilities and equipment where processes will be implemented. Facilities layout and equipment functions and operational limits shall be in accordance with the necessary physical and chemical conditions of the processes to be carried out.

Operations

Operations consider the actions that will be performed in the facilities and equipment so that the processes are carried out achieving the desired result. Operations are defined by the process sequence and conditions as well as the characteristics of the facilities and equipment, both facts together define the procedures to be followed and the capacity to track and control them.

Procedure

Procedures are defined as the sequence of actions that shall be performed to achieve the intended process within the given assets.

3.2 Focus on knowledge

Considering points above, actual and complete knowledge on processes, assets and operations will inherently allow to define the right values and conditions for all relevant variables, parameters and configurations required so that the desired results are achieved, as well it will allow to identify the potential failures and mistakes that can appear.
If the effect of a deviation or change is unknown, the knowledge is not complete enough.
The focus on knowledge, shall also consider that complete knowledge is often not available in development stages of processes or design phases of plants, thus, the assumptions, doubts and knowledge-related remarks, shall be clearly described and reviewed as knowledge becomes gradually available during the development of a project. In any case, the goal is to ensure that, in each step, the best available knowledge is considered to a reasonable extend.
Results of a risk assessment inherently involve some degree of uncertainty, however, without proper knowledge there is no guarantee that the results of a risk assessment allow defining safe process conditions in any sense and regardless of the methodology used.

3.3 Consequences

When a hazard or a deviation from the intended process is identified, its consequences are assessed. Depending on the risk assessment methodology, consequences may be more or less pre-established and implicitly or explicitly described.
The magnitude (severity, impact, etc.) of the consequences may be also considered in more or less detail; however, this need is typically linked with the criteria used in terms of risk acceptance. In some risk assessment methodologies, the single fact of a hazard being present is enough to trigger the requirement for safety measures, without explicitly describing the consequences nor its magnitude. For instance, in a work permit to work at height, the single condition of working at height requires taking safety measures without the need to specify the consequences in case of falling; in this sense, they are pre-established and implicitly considered. This applies to all cases where internal directives or legal requirements prescribe measures for certain activities or conditions.
On the other hand, in a FMEA, HAZOP or similar methodologies, to justify the severity, consequences need to be explicitly described and cannot be pre-established.
In any case, all risk assessment methodologies integrate in some way the consideration of the potential consequences that deviations from the intended process may trigger and, in this sense, it is very important to understand the underlying criteria on consequence assessment.
Finally, as an undesired event may have consequences in different areas, it is necessary to clearly define them and provide criteria accordingly.

4. Action plan

It is a self-evident truth saying that risks are not reduced until measures are implemented. However, perception sometimes is that risks have already improved after finishing a risk assessment. All risk assessment methodologies must have the focus on a clear definition of actions and their effective implementation.
Risk assessment methodologies must, therefore, either lead to a clear selection of the necessary actions when they are closed methodologies or define as a requirement that actions must be clearly specified when they are open methodologies, in the latter case, this is an important task of the risk assessment moderator.
In case that not enough knowledge is available to assess the risk or to define appropriate measures (see point 3.2), an action can be defined to search for the necessary knowledge. This consideration is important, because, as abovementioned, there is a direct link between the reliability of a risk assessment and the knowledge that has been available while performing it.

5. Risk acceptance

Beside systematics, risk acceptance is the other factor that clearly influences the definition of a risk assessment methodology.
Risk acceptance defines the maximum risk that will be accepted to carry out a process or to perform an activity. The risk acceptance must be clearly defined when a risk assessment methodology is adopted.

5.1 Risk

Generally, risk is defined as the combination of two factors: frequency and severity.
However, it must be remembered that while determining frequency and severity in a risk assessment, both are mostly a function of the scenarios identified and, at the same time, the scenarios identified depend mostly on the knowledge degree available in relation with processes, assets and operations, ultimately risk identification depends on knowledge. (Rausand and Haugen, 2020)
A possible way to classify risk acceptance criteria is distinguishing between deterministic and probabilistic approaches. Both approaches are briefly described in the next points.

5.2 Deterministic risk approach

A deterministic approach is based on a precautionary principle focused on consequences, neglecting the frequency to a large extent.
The approach is based on the fact that every time an action or process is executed there is a risk for deviations to occur. Consequently, it is considered that if a potential hazard is present or a deviation may occur, as long as they cannot be discarded, safety measures must be ready in case they happen.
As well, severity is often approached from a worst-case point of view or with some, typically short, ranking criteria. Following the same conservative criteria than that of frequency, if a specified degree of consequence cannot be discarded, argumentation and assessment is defined based on these credible worst-case effects.
In a deterministic approach, both severity and specially frequency are reduced to a single point concept that determines the required safety measures. In practical terms, risk acceptance considers that if an accident happens, the consequences are not acceptable regardless of how high or low the probability was. Therefore, risks are accepted when appropriate measures have been adopted.

5.3 Probabilistic risk approach

A probabilistic approach is based on the traditional concept of risk as a combination of severity and frequency having both factors a progressive range of values.
In this sense, risk is defined as the result of a numerical evaluation, meaning that it is defined by a distribution of values.
Due to the need of providing a specific value to severity and frequency within their available range, the details required are typically more complex and the causes and consequences are analysed and described with a higher level of detail in comparison to a deterministic approach.
The probabilistic risk approach aims to provide an as realistic as possible approach to risk; however, this does not mean that no safety margin is considered in the estimation leading to the numerical evaluation.

6. Structure relations and methodology integration

Having described the structure and fundamental criteria for risk assessment methodologies, it is possible now to propose the points where several methodologies can be linked and effectively integrated. Before continuing, it shall be clear that all methodologies integrate somehow the points described above, however, their main character is linked to a specific factor which is mostly giving the character to the methodology.

6.1 Focus on Systematics

In first place, there are several methodologies which put the focus on their systematic background, these methodologies are broadly used, for instance:

- HAZOPs are based on a strong systematics consisting in dividing the process into nodes and then identifying deviations by combining guide words with process variables.
- ZHA is based on a systematically identifying those hazards which, in case of releasing their potential in an undesired way or manner, will lead to an accident.
- Checklists are based on defining a set of questions and systematically answer them.
- A work permit is usually based on a checklist; however, it commonly includes some systematic approach as a kind of expert system leading to final conclusions and measures to adopt to ensure a safe specific work.
- LOTOTO methodologies are based on systematically identify hazard or energy sources and then, locking, tagging and trying them out.

Many times, these methodologies provide a backbone to a full risk identification and assessment process. In a general sense, it can be said that methodologies in the following points provide specialties to

6.2 Focus on Causes

As said before, without neglecting the fact that the methodologies in this chapter are also based on a strong systematic approach, their main character is defined by being methodologies used to provide an in-depth assessment of the causes leading to undesired situations, in this point, most relevant methodologies are:

- FTA is based on a deductive analysis which describes the sequence of failures and how they combined with each other until they led to the final event.
- Fishbone diagrams are also focusing on describing the causes leading to a final defect or failure.
- FMEA focusses on identifying potential failures modes and their causes.

When it is necessary to investigate causes in detail, these methodologies

6.3 Focus on consequences

Next methodologies are considered to focus on having a strong focus on describing the consequences of a deviation:

- Event trees describe all potential consequences that may be derived from an initial event. As a note, this event can be the result of an FTA and the combination of both methodologies is known as Bow Tie risk assessment.
- Consequence modelling are methodologies focused on quantitatively determining the consequences of an event. There are several types of techniques available, and all are characterized by an in-depth focus on determining the magnitude of the consequences and their reach.

6.4 Focus on risk acceptance

Finally, the focus on risk acceptance is considered. These methodologies are specially characterized by having their focus on the parameters leading to consider a risk as acceptable or not acceptable.

- Risk value. Risk factors are quantified in a scale and then the values of different factors are combined to obtain a final single value. Limits to the potential final values are pre-defined, which define the potential risk categories. Therefore, the final value directly defines a risk level, for instance the RPN criteria of an FMEA.
- Risk Acceptance Matrix is a classical methodology to define risk acceptance based on a combination of severity and frequency.
- Quantitative Risk Assessment defines risk acceptance based on individual risk contours and/or societal risk in terms of F-N curves. (Pasman and Reniers, 2014)

Linked to risk acceptance focus the following two methodologies need also to be mentioned:

- LOPA is an assessment aimed to ensure that measures considered in terms of risk reduction effectively achieve the reduction target defined. (Fang and Mannan, 2007)
- SIL methodology focusses on defining the reliability that a SIS requires to also achieve the reduction target defined.

Understanding the focus of each methodology allows an effective and pragmatic integration, but also defining an efficient management system by using the potential of each methodology only when required and not on systematic basis by considering all potential scenarios and hazards in the same way. Emphasis and focus must be set in depth where necessary.

7. RAMS Concept

Finally, a schematic approach to a Risk Assessment and Management System is presented.

7.1 Phase 1. Hazard Scanning

First phase to effectively manage risks consists in recognizing hazards, the main purpose in Phase 1 is to ensure that all hazards are effectively identified and addressed before allowing an activity to start, regardless of the previous existence or not of the process, equipment, technology, etc. involved in the activity.

The most effective methodologies to scan for hazards consist of lists aiming to cover the potential areas where hazards may arise. Consequently, the methodology to scan and identify relevant, will be based in a set of structured checklists.

The advantage of using lists is that they ensure a systematic approach and review of areas able to play a relevant role for SHE&PS. The main disadvantage is that when a potential hazard source is not addressed in a list, it remains unassessed. The selection of fields and structure of checklists, as well as the type of answers required, are critical to ensure a thoroughly scan for hazards.

The risk approach at this stage is deterministic; therefore, safety measures are defined based on the single presence of a hazard.

The methodologies with a focus on Phase I are Check-lists, Management of Change, Work Permits, LOTOTO.

7.2 Phase 2. Risk Assessment

Second phase to effectively manage risks consists in assessing them.
In contrast to Phase I, where methodologies are based on a deterministic approach to risk, in Phase II a probabilistic approach is applied. This means that the methodologies have, as main target, to provide a clear risk rating. This target is achieved when comparing the assessment results with the risk acceptance criteria essentially defined by considering a combination of frequency of the events and severity of the consequences.
Considering that Phase II methodologies have a probabilistic approach, they require the definition of severity and probability scales which to define the risk level and, together with a risk acceptance criterion, will finally help to determine whether risks are acceptable or not.
Examples of methodologies of Phase II are HAZOP, FMEA, ZHA, Explosion Protection Document, PRORA, SHIRAM, Thermal Process Safety Assessment, Quantitative Risk Assessment, Major Accidents Report.

7.3 Phase 3. Risk assurance

The third and last phase of RAMS backbone focusses on the fact that after reaching an acceptable risk level, this level needs to be assured during the lifetime of the process, facility or equipment.
Main motivation for methodologies in this phase arises from the following statements:

A. Risks are only effectively reduced when the defined safety measures are in place and active.
B. No process, equipment, facility or organisation is totally resilient in front of a high enough number of small changes.

Linked to the first point, it is necessary to ensure that the safety measures defined are in place and that the desired facility condition is ensured before an activity effectively starts.
In relation to the second point, the basic concept is that during the lifetime of a process, equipment, facility or organisation, it is not possible to implement an absolute approach to change management.
As Phase I and II methodologies shall provide a reliable risk strategy, it is reasonable to assume that activities are resilient to changes of a certain degree. Therefore, small changes will hardly lead to an immediate mishap. However, in a long-time frame, the combined effect of many small deviations may lead to changes in activities that can be considered out of the scope of the methodologies applied in the original condition.
Methodologies usually considered in Phase III are Pre-Start-Up reviews, Risk assessment periodic reviews, Safety integrity audits.

8. Conclusions

The structural elements of risk identification and assessment have been described so that it is possible to identify them in any methodology.
As well, most well-known methodologies have been described in terms of main focus and potential integration points between them. Knowing when to use a methodology or its main purpose is equivalent to select the proper tool for a manual work.
Finally, the concept of a risk assessment and management system has been proposed to understand where each methodology can be used and the role it plays while ensuring safe operations in the process industry.

Nomenclature

FMEA - Failure Mode and Effects Analysis
FTA - Fault Tree Analysis
HAZOP - Hazard and Operability Study
LOPA - Layer of Protection Analysis
LOTOTO - Lock Out Tag Out Try Out
SIL - Safety Integrity Level
SIS - Safety Instrumented System
ZHA - Zürich Hazard Assessment

References

Center of Chemical Process Safety (CCPS), 2001, Layers of Protection Analysis, Simplified Process Risk Assessment. American Institute of Chemical Engineers, New York, US.
Fang J.S., Mannan, M.S., 2007, Value at risk perspective on layers of protection analysis, J. Process Safety and Environmental protection, 85, 83-87.
Pasman H., Reniers G., 2014, Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP), J. Loss Prev. Proc. Ind. 28, 2-9.
Rausand, M., Haugen, S., 2020, Risk Assessment: Theory, Methods, and Applications, 2nd Ed., Wiley.