

Some Risk Assessment Methods and Examples of their Application

Pavel Fuchs, Jan Kamenicky, Tomas Saska, David Valis, Jaroslav Zajicek

Technical University of Liberec, <http://risk.rss.tul.cz/>

CONTENT

1	Hazard and operability study (HAZOP).....	2
1.1	Introduction	2
1.2	HAZOP characteristic.....	2
1.3	HAZOP Methodology	3
1.4	Conclusion	8
1.5	Annex A - HAZOP study.....	8
2	Fault tree analysis (FTA)	11
2.1	Introduction	11
2.2	Terms and definitions	11
2.3	Symbols	11
2.4	Fault tree description and structure	11
2.5	Fault tree graphical description and structure	12
2.6	Fault tree development and evaluation - general.....	12
2.7	Annex B - FTA symbols.....	13
2.8	Annex C - FTA application.....	14
3	Event tree analysis (ETA).....	16
3.1	Introduction	16
3.2	Terms and definitions	16
3.3	General description	16
3.4	Benefits and limitations of event tree analysis	17
3.5	Development of event trees - general.....	17
3.6	Evaluation	18
3.7	Annex D - ETA application	18
4	Failure Modes and Effect Analysis (FMEA)	21
4.1	Introduction	21
4.2	Terms and definitions	21
4.3	General description	21
4.4	Annex E - FMECA application	22
	Bibliography	24

1 Hazard and operability study (HAZOP)

1.1 Introduction

Hazard and Operability Analysis (HAZOP) is a structured and systematic technique for system examination and risk management. The HAZOP technique was initially developed to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems. HAZOP is based on a theory that assumes risk events are caused by deviations from design or operating intentions. Identification of such deviations is facilitated by using sets of “guide words” as a systematic list of deviation perspectives. This approach is a unique feature of the HAZOP methodology that helps stimulate the imagination of team members when exploring potential deviations. The HAZOP is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team (HAZOP team) during a set of meetings.

HAZOP is also commonly used in risk assessments for industrial and environmental health and safety applications. Additional details on the HAZOP methodology may be found within The International Standard *IEC 61882 Hazard and Operability Studies (HAZOP) - Application Guide* [1].

1.2 HAZOP characteristic

HAZOP is best suited for assessing hazards in facilities, equipment, and processes and is capable of assessing systems from multiple perspectives:

Design

- assessing system design capability to meet user specifications and safety standards
- identifying weaknesses in systems

Physical and operational environments

- assessing environment to ensure system is appropriately situated, supported, serviced, contained, etc.

Operational and procedural controls

- assessing engineered controls (ex: automation), sequences of operations, procedural controls (ex: human interactions) etc.
- assessing different operational modes – start-up, standby, normal operation, steady & unsteady states, normal shutdown, emergency shutdown, etc.

Advantages

1. Helpful when confronting hazards that are difficult to quantify, i.e.:
 - hazards rooted in human performance and behaviours
 - hazards that are difficult to detect, analyse, isolate, count, predict, etc.
 - methodology doesn't force you to explicitly rate or measure deviation probability of occurrence, severity of impact, or ability to detect
2. Built-in brainstorming methodology
3. Systematic & comprehensive methodology
4. More simple and intuitive than other commonly used risk management tools

Disadvantages

1. No means to assess hazards involving interactions between different parts of a system or process
2. No risk ranking or prioritization capability
 - teams may optionally build-in such capability as required
3. No means to assess effectiveness of existing or proposed controls (safeguards)
 - may need to interface HAZOP with other risk management tools

Effectiveness

The effectiveness of a HAZOP will depend on:

- a) the accuracy of information (including P&IDs) available to the team — information
- b) should be complete and up-to-date
- c) the skills and insights of the team members
- d) how well the team is able to use the systematic method as an aid to identifying
- e) deviations
- f) the maintaining of a sense of proportion in assessing the seriousness of a hazard
- g) and the expenditure of resources in reducing its likelihood
- h) the competence of the chairperson in ensuring the study team rigorously follows
- i) sound procedures.

Key elements of a HAZOP are:

- HAZOP team
- full description of process
- relevant guide words
- conditions conducive to brainstorming
- recording of meeting
- follow up plan.

1.3 HAZOP Methodology

The HAZOP analysis process is executed in four phases as illustrated below:

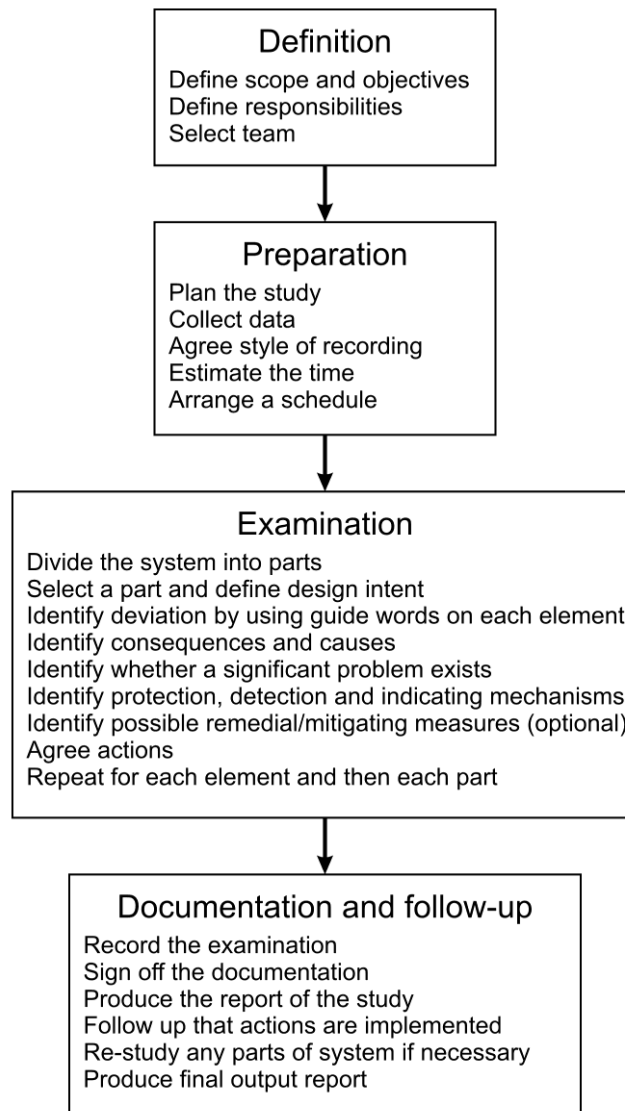


Figure 1: The HAZOP analysis process [1]

Definition Phase

The Definition Phase typically begins with preliminary identification of risk assessment team members. HAZOP is intended to be a cross-functional team effort, and relies on specialists (SMEs) from various disciplines with appropriate skills and experience who display intuition and good judgment. SMEs should be carefully chosen to include those with a broad and current knowledge of system deviations. HAZOP should always be carried out in a climate of positive thinking and frank discussion. During the Definition Phase, the risk assessment team must identify the assessment scope carefully in order to focus effort. This includes defining study boundaries and key interfaces as well as key assumptions that the assessment will be performed under.

Preparation Phase

The Preparation Phase typically includes the following activities:

- identifying and locating supporting data and information
- identification of the audience and users of the study outputs
- project management preparations (ex: scheduling meetings, transcribing proceedings, etc.)

- consensus on template format for recording study outputs
- consensus on HAZOP guide words to be used during the study

HAZOP guide words are key supporting elements in the execution of a HAZOP analysis. The example of basic HAZOP guide words see table 1.

Table 1: The example of basic HAZOP guide words

Guide word	Meaning	Parameter (for example)	Deviation	Example
No	Negation of the design intent	Flow	No flow	No flow when production is expected
Less	Quantitative decrease	Pressure	Low pressure	Lower pressure than normal
More	Quantitative increase	Temperature	High temperature	Higher temperature than designed
Part of	Qualitative decrease	State	Degraded state	Only part of the system is shut down
As well as	Qualitative increase	One phase	Two phase	Other valves opened and not only liquid indicated (logic fault or human error)
Reverse	Logical opposite of the intention occurs	Intended objective	Mismatch	Back-flow when the system shuts down
Other than	Complete Substitution (another activity takes place)	Operation	Maintenance	Loss of electric power caused by chaotic maintenance

Examination Phase

The Examination Phase begins with identification of all elements (parts or steps) of the system or process to be examined. For example:

- physical systems may be broken down into smaller parts as necessary
- processes may be broken down into discrete steps or phases
- similar parts or steps may be grouped together to facilitate assessment

The HAZOP guide words are then applied to each of the elements. In this fashion a thorough search for deviations is carried out in a systematic manner. It must be noted that not all combinations of guide words and elements are expected to yield sensible or credible deviation possibilities. As a general rule, all reasonable use and misuse conditions which are expected by the user should be identified and subsequently challenged to determine if they are “credible” and whether they should be assessed any further. There is no need to explicitly document the instances when combinations of elements and guide words do not yield any credible deviations.

The analysis should follow the flow or sequence related to the subject of the analysis, tracing inputs to outputs in a logical sequence. Hazard identification techniques such as HAZOP derive their power from a disciplined step by step examination process. There are two

possible sequences of examination: "Element first" and "Guide word first", as shown in following figures.

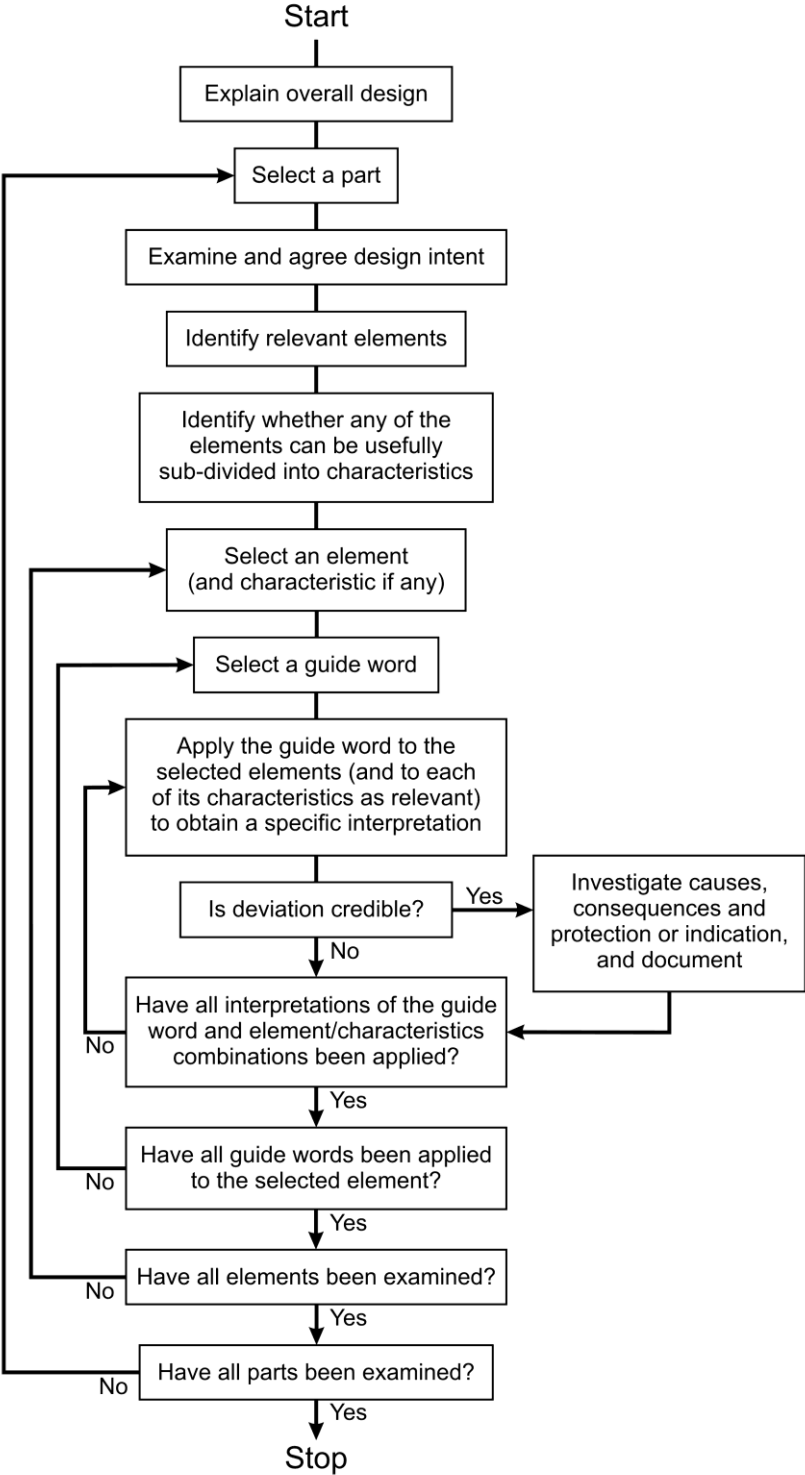


Figure 2: Flow chart of the HAZOP examination procedure – „Element first sequence“ [1]

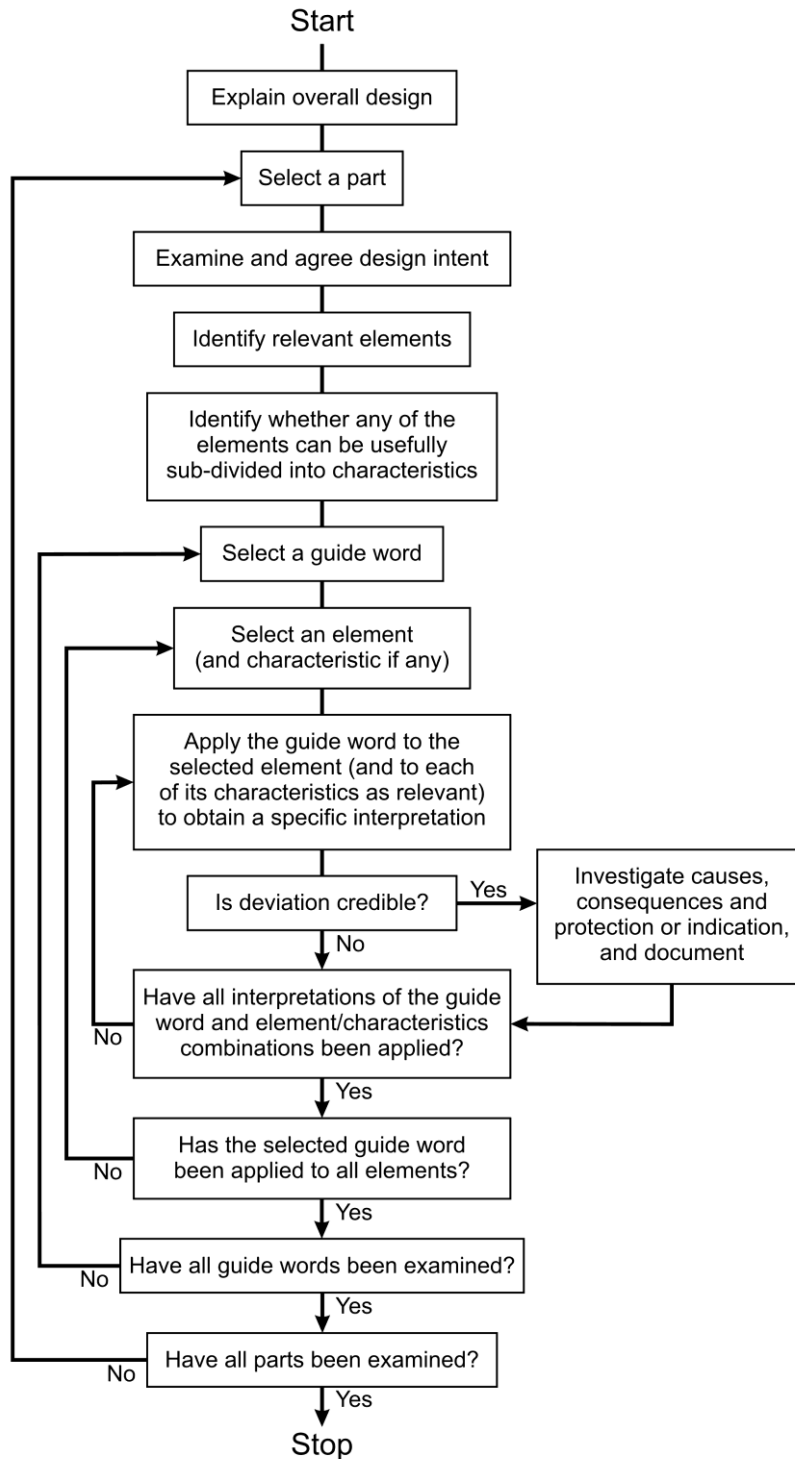


Figure 3: Flow chart of the HAZOP examination procedure – „Guide word first sequence“ [1]

Documentation & Follow-up Phase

The documentation of HAZOP analyses is often facilitated by utilizing a template recording form as detailed in IEC Standard 61882. Risk assessment teams may modify the template as necessary based on factors such as:

- regulatory requirements

- need for more explicit risk rating or prioritization (ex: rating deviation probabilities, severities, and/or detection)
- company documentation policies
- needs for traceability or audit readiness
- other factors

1.4 Conclusion

HAZOP is a powerful tool. The output of the tool should always be presented at a level of detail appropriate for the various stakeholders. This is important not just for presenting results, but also for obtaining early buy-in on the approach.

On a long-term basis, operational feedback should confirm that the assessment and control steps are adequately addressing the risk question. If this is not the case, it may be necessary to review all assumptions. Feedback should correspond to ensuring that assumptions made about the level of residual risks are still valid. Residual risks are risks that are expected to remain after risk control strategies have been exercised. It is also important to note that new risks may arise from risk control practices. Sometimes risks that were not originally identified or may have been filtered out during the initial risk assessment can become aggravating factors due to the implementation of risk control measures.

1.5 Annex A - HAZOP study

Example – HAZOP study (ADR road tank and train crash cause assessment on grade crossing) – sheet 1

Study title: ADR road tank and train crash cause assessment on grade crossing									Sheet: 1 of 2
Scheme: Grade crossing scheme									Datum: 29.4.2010
Team composition:									Meeting date:29.4.2010
Part considered: ADR road tank and train crash on grade crossing									
No.	Element	Characteristics	Guide word	Deviation	Possible causes	Consequences	Safeguards	Comments	Action required
1	Light signalling	Shining lamp	No (not, none)	The lamp is not shining	Cracked fibber	Without consequence	No	Without consequence (crossing gate and tone bleep work like back up system by functionless light signalling)	Changing for diode light
2	Light signalling	Good visibility	Other than	Impossible to see light signalling	Meteorological situation, non-transparent hood	Without consequence	No	Without consequence (crossing gate and tone bleep work like back up system by functionless light signalling)	Light signalling better shielding against reflection
3	Light signalling	Relay/switching	Other than	Relay is not switching	Ordinary wear and tear	Without consequence	No	Without consequence (crossing gate and tone bleep work like back up system by functionless light signalling)	Back-up system
4	Tone bleep	Tone/signalling	No (not, none)	Impossible to hear a tone	Ordinary wear and tear	Without consequence	No	Without consequence (crossing gate and light signalling work like back up system by functionless tone bleep)	No

Example – HAZOP study (ADR road tank and train crash cause assessment on grade crossing) – sheet 2

Study title: ADR road tank and train crash cause assessment on grade crossing									Sheet: 2 of 2
Scheme: Grade crossing scheme									Datum: 29.4.2010
Team composition:									Meeting date:29.4.2010
Part considered: ADR road tank and train crash on grade crossing									
No.	Element	Characteristics	Guide word	Deviation	Possible causes	Consequences	Safeguards	Comments	Action required
5	Crossing gat	Functional drive	Other than	The Crossing gate are not going down in consequence of functionless drive	Ordinary wear and tear	Without consequence	No	Without consequence (tone bleep and light signalling work like back up system by functionless crossing gate)	Drive back up system
6	Crossing gate	Drive gear	No (not, none)	The crossing gate are not going down in consequence of functionless drive gear	Ordinary wear and tear	Without consequence	No	Without consequence (tone bleep and light signalling work like back up system by functionless crossing gate)	No
7	Crossing gate	Crossing gate integrity	Other than	Mechanical damage	Ordinary wear and tear, vandalism, weather effects	Without consequence	No	Without consequence (tone bleep and light signalling work like back up system by functionless crossing gate)	Crossing gate bracing
8	Alarm system sensor	Incoming train signal registering	No (not, none)	No signal of incoming train	Ordinary wear and tear, vandalism	Crash on grade crossing	No		Sensor back up system
9	Alarm system sensor	Incoming train signal registering	Other than	Garbled signal of incoming train	Ordinary wear and tear	Crash on grade crossing	No		Sensor back up system
10	Alarm system power supply	Power supply	No (not, none)	Light signalling, tone bleep and crossing gate functionless	Ordinary wear and tear	Crash on grade crossing	No		Own power supply generator
11	ADR road tank	Move/transport	No (not, none)	No possibility of moving on grade crossing	Ordinary wear and tear, insurable cheat	Crash on grade crossing	No		No

2 Fault tree analysis (FTA)

2.1 Introduction

Fault tree analysis (FTA) is concerned with the identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event. With FTA this event is usually seizure or degradation of system performance, safety or other important operational attributes, while with STA (success tree analysis) this event is the attribute describing the success.

FTA is often applied to the safety analysis of systems (such as transportation systems, power plants, or any other systems that might require evaluation of safety of their operation). Fault tree analysis can be also used for availability and maintainability analysis. However, for simplicity, in the rest of this standard the term “reliability” will be used to represent these aspects of system performance.

There are two approaches to FTA. One is a qualitative approach, where the probability of events and their contributing factors, – input events – or their frequency of occurrence is not addressed. This approach is a detailed analysis of events/faults and is known as a qualitative or traditional FTA. It is largely used in nuclear industry applications and many other instances where the potential causes or faults are sought out, without interest in their likelihood of occurrence. At times, some events in the traditional FTA are investigated quantitatively, but these calculations are disassociated with any overall reliability concepts, in which case, no attempt to calculate overall reliability using FTA is made.

The second approach, adopted by many industries, is largely quantitative, where a detailed FTA models an entire product, process or system, and the vast majority of the basic events, whether faults or events, has a probability of occurrence determined by analysis or test. In this case, the final result is the probability of occurrence of a top event representing reliability or probability of fault or a failure.

2.2 Terms and definitions

For the purpose of Fault Tree Analysis the terms and definitions are given in IEC 61025 Ed. 2.0: Fault tree analysis (FTA) [2]. In fault tree methodology and applications, many terms are used to better explain the intent of analysis or the thought process behind such analysis.

2.3 Symbols

The graphical representation of a fault tree requires that symbols, identifiers and labels be used in a consistent manner. Symbols describing fault tree events vary with user preferences and software packages, when used. A separate table of symbols is attached.

2.4 Fault tree description and structure

Several analytical methods of dependability analysis are available, of which fault tree analysis (FTA) is one. The purpose of each method and their individual or combined applicability in evaluating the flow of events or states that would be the cause of an outcome, or reliability and availability of a given system or component should be examined by the analyst before starting FTA. Consideration should be given to the advantages and disadvantages of each method and their respective products, data required to perform the analysis, complexity of analysis and other factors.

A fault tree is an organized graphical representation of the conditions or other factors causing or contributing to the occurrence of a defined outcome, referred to as the "top event". When the outcome is a success, then the fault tree becomes a success tree, where the input events are those that contribute to the top success event. The representation of a fault tree is

in a form that can be clearly understood, analysed and, as necessary, rearranged to facilitate the identification of:

- factors affecting the investigated top event as it is carried out in most of the traditional fault tree analyses;
- factors affecting the reliability and performance characteristics of the system, when the FTA technique is used for reliability analysis, for example design deficiencies, environmental or operational stresses, component failure modes, operator mistakes, software faults;
- events affecting more than one functional component, which could cancel the benefits of specific redundancies or affect two or more parts of a product that may otherwise seem operationally unrelated or independent (common cause events).

Fault tree analysis is a deductive (top-down) method of analysis aimed at pinpointing the causes or combinations of causes that can lead to the defined top event. The analysis can be qualitative or quantitative, depending on the scope of the analyses.

A quantitative FTA can be used when the probabilities of primary events are known. Probabilities of occurrence of all intermediate events and the top event (outcome) can then be calculated in accordance with the model. Also, the quantitative FTA is very useful in reliability analysis of a product or a system in its development. FTA can be used for analysis of systems with complex interactions between sub-systems including software/hardware interactions.

2.5 Fault tree graphical description and structure

Components of a fault tree are as follows:

Gates:

- Symbols showing the logical relationship between input events and the output event
- Static gates – outcome not dependent on the order of occurrence of inputs,
- Dynamic gates – outcome dependent on the order of occurrence of inputs.

Events

- Lowest level of inputs in a fault tree. Commonly used event symbols and their definitions are shown in attached table.


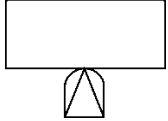
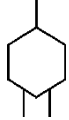

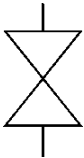
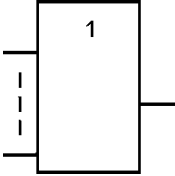
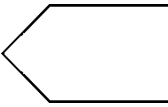
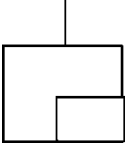
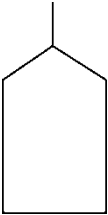

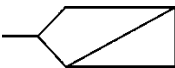
2.6 Fault tree development and evaluation - general

Development of a fault tree starts with the definition of the top event. Development of a fault tree in its traditional application, or for the system reliability and the failure mode analysis, is a deductive method where the analysis starts from the top undesired event as it is defined for the scope of analysis. Once developed to the intended extent, the fault tree becomes a graphical representation of all events that either by themselves or in conjunction with other events contribute to the occurrence of the top event.

2.7 Annex B - FTA symbols

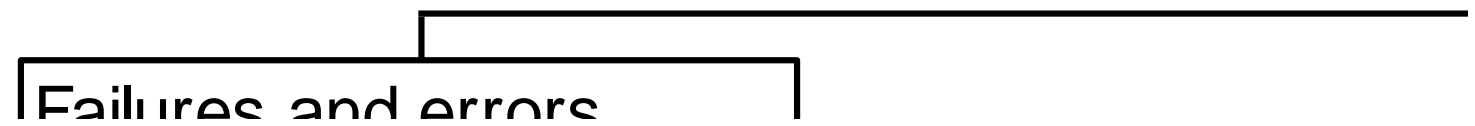
According to [2] these symbols are used.

Symbols			Name	Description
			BASIC EVENT	The lowest level event for which probability of occurrence or reliability information is available
			CONDITIONAL EVENT	Event that is a condition of occurrence of another event. when both have to occur for the output to occur
			DORMANT EVENT	A primary event. that represents a dormant failure; an event that is not immediately detected but could, perhaps, be detected by additional inspection or analysis
			UNDEVELOPE D EVENT	A primary event. that represents a part of the system that is not yet developed
			TRANSFER gate	Gate indicating that this part of the system is developed in another part or page of the diagram
			OR gate	The output event. occurs if any of the input events occur
			MAJORITY VOTE gate	The output occurs if m or more inputs out of a total of n inputs occur
			EXCLUSIVE OR gate	The output event. occurs if one, but not the other inputs occur
			AND gate	The output event. occurs only if all of the input events occur

Symbols		Name	Description	
		PRIORITY AND (PAND) gate	The output event. (failure) occurs only if the input events occur in sequence from left to right	
			INHIBIT gate	The output occurs only if both of the input events take place, one of them conditional
			NOT gate	The output event. occurs only if the input event does not occur
			SEQ gate	The output event. (failure) occurs only if all input events occur in sequence from left to right. This gate is identical to the PAND gate if the number of inputs to the PAND gate is not limited to 2 as done by some analysts
			SPARE gate	The output event. will occur if the number of spare components is less than the number required
			House event	Event which has happened, or will happen with certainty
			Zero event	Event which cannot happen

2.8 Annex C - FTA application

Example – Application of FTA on Railway Crossing



3 Event tree analysis (ETA)

3.1 Introduction

The basic principles of this methodology have not changed since the conception of the technique in the 1960's. ETA was first successfully used in the nuclear industry in a study by the U.S. Nuclear Regulatory Commission the so-called WASH 1400 report in the year 1975. Over the following years ETA has gained widespread acceptance as a mature methodology for dependability and risk analysis and is applied in diverse industry branches ranging from aviation industry, nuclear installations, automotive industry, chemical processing, offshore oil and gas production, and defense industry to transportation systems.

In contrast to some other dependability techniques such as Markov modelling, ETA is based on relatively elementary mathematical principles. However, as mentioned in IEC 60300-3-1, the implementation of ETA requires a high degree of expertise in the application of the technique. This is due in part to the fact that particular care has to be taken when dealing with dependent events. Furthermore, one can utilize the close relationship between Fault Tree Analysis (FTA) and the qualitative and quantitative analysis of event trees.

3.2 Terms and definitions

For the purposes of Event Tree Analysis the terms and definitions given in IEC 62502 Analysis techniques for dependability – Event tree analysis (ETA) [3] are applied.

3.3 General description

The Event Tree Analysis (ETA) is an inductive logic technique to model a system with respect to dependability and risk related measures as well as to identify and assess the frequency of the various possible outcomes of a given initiating event. According to the IEC 60050(191) the dependability of a system is defined as the ability to meet success criteria, under given conditions of use and maintenance. The core elements of dependability are the reliability, availability and maintainability of the item considered. Starting from an initiating event the ETA deals with the question "What happens if..." and thus constructs a tree of the various possible outcomes. It is therefore crucial that a comprehensive list of initiating events is compiled to ensure that the event tree properly depicts all the important event sequences for the system under consideration. Using this forward logic, the ETA can be described as a method of representing the mitigating factors in response to the initiating event - taking into account additional mitigating factors. From the qualitative point of view ETA is a means of identifying all potential accident scenarios (fanning out like a tree with success- or failure-branches) and of identifying design or procedural weaknesses. As with other dependability techniques, particular care has to be taken with the modelling of dependencies bearing in mind that the probabilities used for quantifying the event tree are conditioned on the event sequence that occurred prior to the occurrence of the event concerned. Clause 9 deals with these qualitative aspects of the analysis as well as the basic quantitative rules for the calculations used to estimate the (dimensionless) probabilities or frequencies ($[1/h]$) of each of the possible outcomes. Caveats concerning the quantification of software failures as well as the quantification of human factors will not be dealt with in this standard, since these issues are covered by other IEC publications.

The advantages of ETA as a dependability and risk related technique as well as the limitations are discussed below. As an example of the limitations of ETA, the restrictions to the modelling of the time-dependent evolution of the events should be noted.

Event Tree Analysis bears a close relationship with the Fault Tree Analysis (FTA) whereby the top events of the FTA yield the conditional probability for a particular node of the ETA.

3.4 Benefits and limitations of event tree analysis

Benefits

An ETA provides the following merits:

- a) It is applicable to all types of technical systems;
- b) It provides visualization of event chains following an initiating event;
- c) It enables the assessment of multiple, coexisting system faults and failures as well as order dependent events;
- d) It functions simultaneously in the failure or success domain;
- e) Its end events need not be anticipated;
- f) It identifies potential single-point failures, areas of system vulnerability, and low-payoff countermeasures. This provides for optimized deployment of resources, improved control of risk through improved procedures and safety functions;
- g) It allows for identification and traceability of failure propagation paths of a system;
- h) It enables decomposition of large and complex systems into smaller, more manageable parts.

The strength of ETA – compared to many other dependability and risk related techniques – is its ability to model the sequence and interaction of various mitigating factors that follow the occurrence of the initiating event. Thus the system and its interactions in an accident scenario, with all mitigating factors become visible to the analyst for further risk evaluations.

Limitations

An ETA has the following limitations:

- a) The initiating events are not disclosed by the analysis, but must be foreseen by the analyst;
- b) Possible operating scenarios must be anticipated by the analyst;
- c) Subtle system dependencies might be overlooked, leading to unduly optimistic estimates of dependability and risk related measures; also sometimes being in a particular state for too long a time can result in a failure state, which is difficult to model in an event tree.
- d) Method needs practical experiences of the analyst and preceding system investigations, e.g., to address correct handling of conditional probabilities and dependent events;
- e) ETA is not very suitable for handling common cause failures in the quantitative analysis. This aspect should be covered by fault tree analysis which can then be linked to the ETA;
- f) Although multiple pathways to system failure may be identified, the levels of loss associated with particular pathways may not be distinguishable without additional analysis; however, awareness of such a need is required

3.5 Development of event trees - general

The events delineating the event sequences are usually characterized in terms of:

- a) Functional event tree: The fulfilment (or not) of mitigating functions;
- b) System event Tree: The intervention (or not) of mitigating factors which are supposed to take action for the mitigation of the accident;

- c) Phenomenological event tree: The occurrence or non-occurrence of physical phenomena.

Typically the functional event trees are an intermediate step to the construction of system event trees: following the initiating event, the safety functions which need to be fulfilled are identified; these will later be replaced by the corresponding mitigating factors. The system event trees are used to identify the sequences involving the mitigating factors. The event trees involving physical phenomena describe the accident with physical phenomena evolution taking place inside and outside the system under consideration (e.g. pressure and temperature transients, fire, containment dispersion, etc.).

3.6 Evaluation

Before starting the quantitative analysis of the frequency or probability of the outcomes of the different event sequences, one has to carefully analyse the qualitative aspects of the event tree model, i.e., the dependence of the events, including the initiating event and the top events as well as the intermediate or basic events of the linked fault trees.

In order to facilitate the depiction of the basic principles of the evaluation following figure 4 shows the basic graphical representation of an event tree used in this clause for illustration purposes.

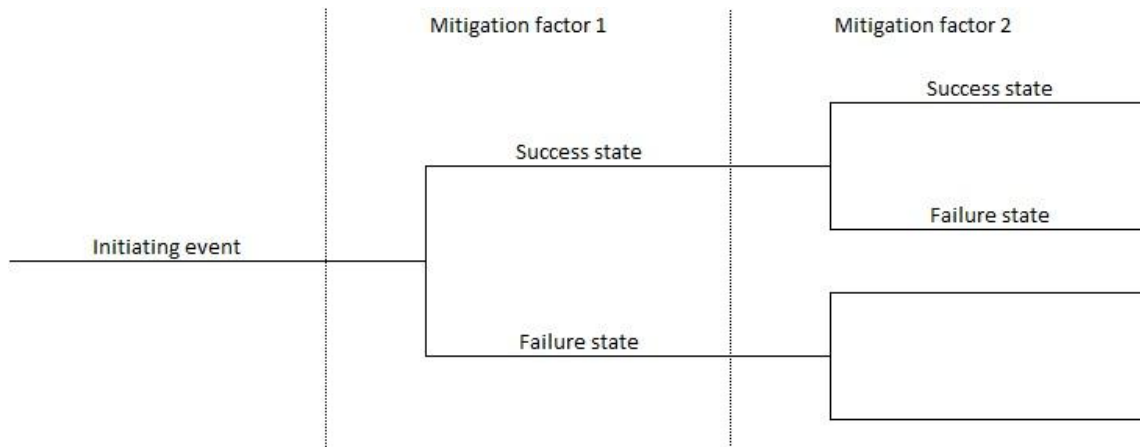
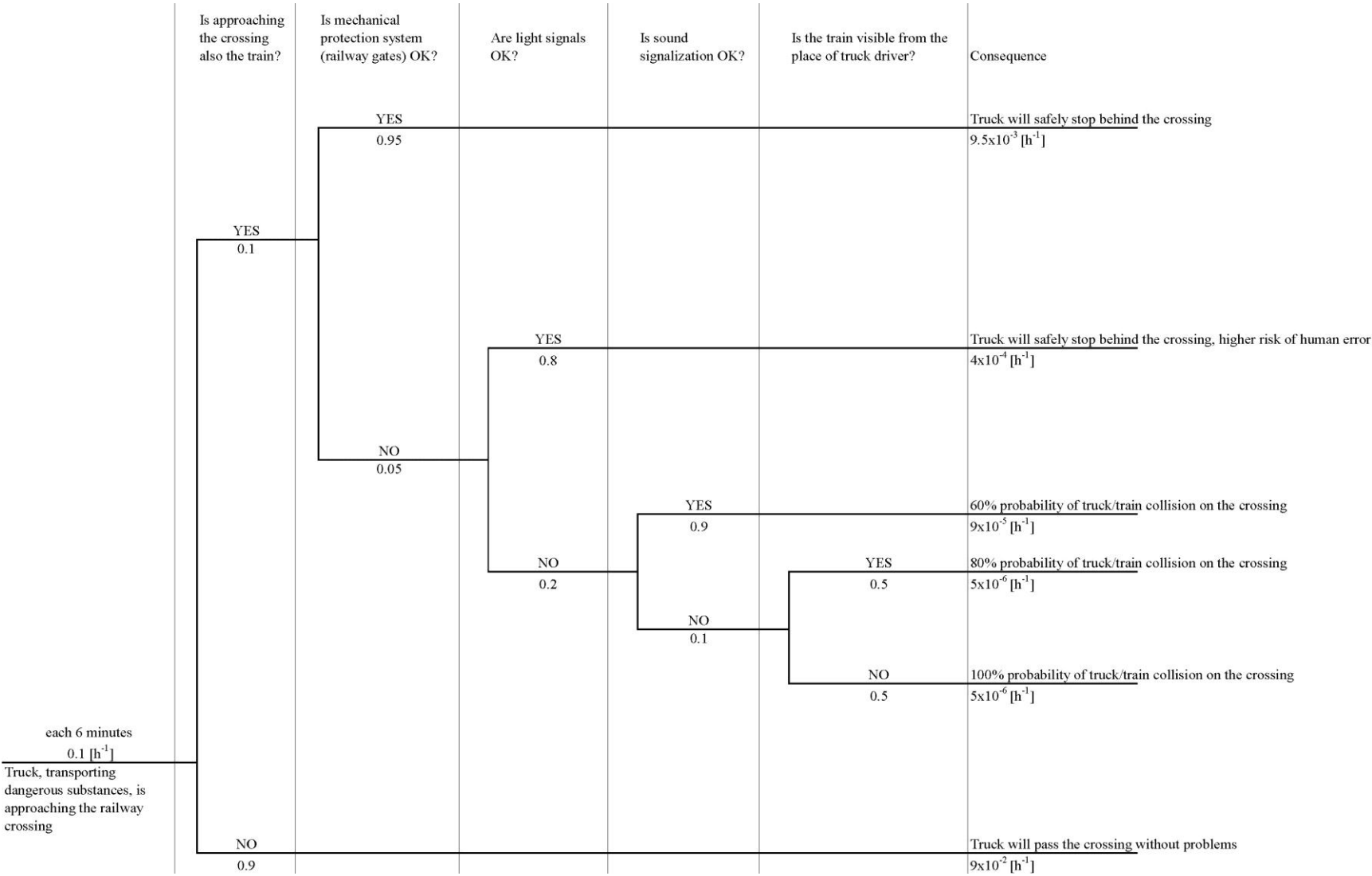


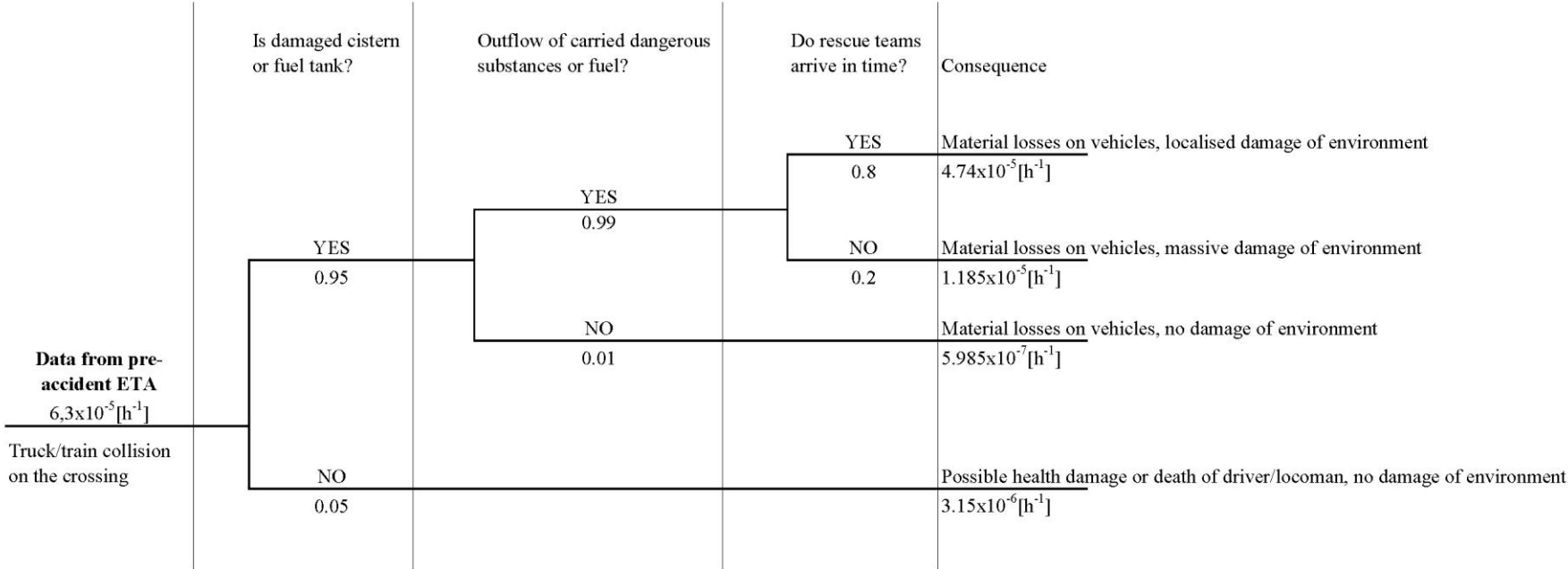
Figure 4: Event tree analysis graphical representation [3]

3.7 Annex D - ETA application

Example 1 – Pre-accidental Event Tree Analysis



Example 2 – Post-accidental Event Tree Analysis



4 Failure Modes and Effect Analysis (FMEA)

4.1 Introduction

Failure Modes and Effect Analysis (FMEA) is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance (performance of the immediate assembly and the entire system or a process). Here, the term system is used as a representation of hardware, software (with their interaction) or a process.

4.2 Terms and definitions

For the purposes of Failure Modes and Effect Analysis the terms and definitions given in IEC 60812 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) [4] are applied.

4.3 General description

A thorough FMEA is a result of a team composed of individuals qualified to recognize and assess the magnitude and consequences of various types of potential inadequacies in the product design that might lead to failures. Advantage of the team work is that it stimulates thought process, and ensures necessary expertise.

FMEA is considered to be a method to identify the severity of potential failure modes and to provide an input to mitigating measures to reduce risk. In some applications however, FMEA also includes an estimation of the probability of occurrence of the failure modes. This enhances the analysis by providing a measure of the failure mode's likelihood. The basic approach of FMEA/FMECA is described in the figure 5.

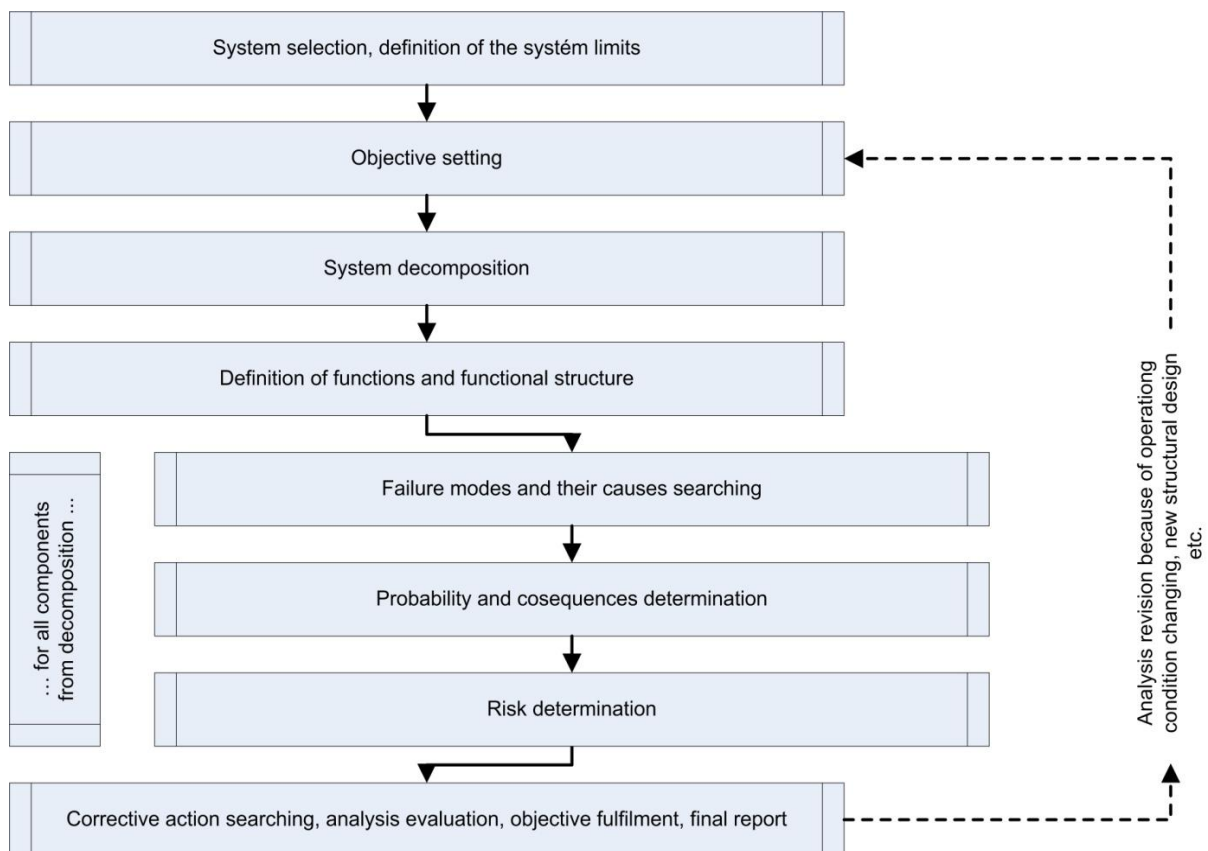


Figure 5: The basic FMEA/FMECA approach

FMECA (Failure Modes, Effects and Criticality Analysis) is an extension to the FMEA to include a means of ranking the severity of the failure modes to allow prioritization of countermeasures. This is done by combining the severity measure and frequency of occurrence to produce a metric called criticality. FMEA is a flexible tool that can be tailored to meet specific industry or product needs. Specialized worksheets requiring specific entries may be adapted for certain applications.

4.4 Annex E - FMECA application

Example – Application of FMECA on Railway Crossing

Component	Failure mode / unwanted event	Causes	Consequences	Failure probability (by MTBF)	Time to repair	Consequences probability (by failure rate)	Risk
light signaling	the lamp is not shining	ordinary wear and tear	without consequences - components in parallel connection, FMECA doesn't work with more failures at the same time	1 year	2 days	0 h ⁻¹	without risk
	impossible to see light signaling	meteorological situation, non-transparent hood		3 days	1 hour		
	relay is not switching	ordinary wear and tear		10 years	2 days		
tone bleep	impossible to hear a tone	ordinary wear and tear		10 years	1 week		
crossing gate	the crossing gate are not going down	ordinary wear and tear		10 years	1 day		
	the crossing gate are not going down	ordinary wear and tear		10 years	1 day		
	mechanical damage	ordinary wear and tear, vandalism	4 years	1 day			
alarm system sensor	garbled signal of incoming train	ordinary wear and tear	without consequences - safe failure	2 years	1 day	2,00E-08 h ⁻¹	slight
	no signal of incoming train	ordinary wear and tear	possibility of crash train and ADR road tank, leakage of danger substances with environment damage and lethal injuries	20 years	1 day		
alarm system power supply	no power	ordinary wear and tear		6 months	1 day	1,00E-06 h ⁻¹	medium
ADR road tank	no possibility of moving on grade crossing	ordinary wear and tear, insurable cheat		50 years	30 minutes	6,00E-07 h ⁻¹	low

Bibliography

- [1] IEC 61882:2001 Hazard and operability studies (HAZOP studies) – Application guide
- [2] IEC 61025:2006 Fault tree analysis (FTA).
- [3] IEC 62502:2010 Analysis techniques for dependability – Event tree analysis (ETA).
- [4] IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)