Review of Hazard Analysis Methods and Their Basic Characteristics

Vladimir Popović
Teaching and Research Assistant
University of Belgrade
Faculty of Mechanical Engineering

Branko Vasić
Associate Professor
University of Belgrade
Faculty of Mechanical Engineering

We live in the world comprised of systems and risks. With systems and technology there also comes the exposure to mishaps because systems can fail or work improperly which results in damage, injury and deaths. The possibility that a system fails and results in death, injury, damage and the like is referred to as mishap risk. The key to system safety and effective risk management is the identification and mitigation of hazards. To successfully control hazards, it is necessary to understand hazards and know how to identify them. The purpose of this paper is to better understand hazards and the tools and techniques for identifying them, so that they can be effectively controlled during the development of a system.

Keywords: *hazard analysis methods, types and techniques.*

1. INTRODUCTION

Due to the fact that there are various definitions and interpretations for the same thing in the terminology used in the given area, it was necessary, especially in the introductory part, to provide clarification for specific terms that have been used, and consider the dilemmas each analyst, dealing with the given area, faces. The English language itself, on one hand, contains many synonyms, and on the other, different experts operate with different or even contradictory terms for the same concepts. Another problem arises when these terms are to be introduced into our language [1,2]. In order to resolve the above mentioned misgivings, we have provided a short review of terms and definitions, most frequently used.

Fault: *The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources* (JUS IEC 50). A fault is hence a state resulting from failure.

Failure: *The event when a required function is terminated (exceeding the acceptable limits)* (JUS IEC 50).

Error: *A discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition* (JUS IEC 50).

An error is (yet) not a failure because it is within the acceptable limits of deviation from the desired performance (target value). An error is sometimes referred to as an incipient failure.

The term failure is sometimes confused with the terms fault and error. The distinction between failure (or fault) and error is essential in failure analysis, because this describes the borderline between what is a failure and what is not. The relationship between these terms is illustrated in Figure 1.

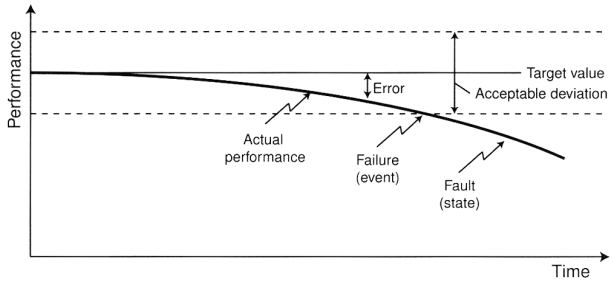

Figure 1. Illustration of the difference between failure, fault and error [3]

Mishap: *An unplanned event or series of event resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment Accident* (MIL-STD-882C). Note the last word "accident" in the definition.

Hazard: *Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment* (MIL-STD-882D).

A hazard is a potential condition that can result in a mishap or accident, given that the hazard occurs. This means that mishaps can be predicted via hazard identification. And, mishaps can be prevented or controlled via hazard elimination, control, or mitigation measures. This viewpoint provides a sense of control over the systems we develop and utilize. We can also say that hazard is a condition that is a prerequisite for an accident. A hazard is comprised of the following three basic components [4]:

- *Hazardous Element (HE)* – This is the basic hazardous resource creating the impetus for the hazard, such as a hazardous energy source such as explosives being used in the system.
- *Initiating Mechanism (IM)* – This is the trigger or initiator event(s) causing the hazard to occur. The IM causes actualization or transformation of the hazard from a dormant state to an active mishap state.
- *Target and Threat (T/T)* – This is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. This is the mishap outcome and the expected consequential damage or loss.

Received: November 2008, Accepted: December 2008
Correspondence to: Dr Vladimir Popović
Faculty of Mechanical Engineering,
Kraljice Marije 16, 11120 Belgrade 35, Serbia
E-mail: vpopovic@mas.bg.ac.rs

© Faculty of Mechanical Engineering, Belgrade. All rights reserved

The three components of a hazard form what is known in system safety as the hazard triangle. The hazard triangle illustrates that a hazard consists of three necessary and coupled components, each of which forms the side of a triangle. All three sides of the triangle are essential and required in order for a hazard to exist. Remove any one of the triangle sides and hazard is eliminated because it is no longer able to produce a mishap (i.e., the triangle is incomplete).

Hazard is a deterministic entity with its own structure, components, characteristics and features. If the hazard cannot be eliminated, its risk can be limited (diminished or controlled), namely by reducing the probability of hazard occurrence and/or the severity of accident effects, through project techniques. When the hazard arises, its outcome is almost always fixed and unchangeable. For this reason, it is very hard to reduce the severity of effects (they usually remain the same even after dealing with the hazard); it is much easier though, to reduce the probability of hazard occurrence to a reasonable level.

Risk: *An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence* (MIL-STD-882D). *The possibility of incurring misfortune or loss … danger, gamble, peril, hazard* (Collins Dictionary and Thesaurus). *To take a risk: to proceed … without regard to the possibility of danger …* (Collins Dictionary and Thesaurus).

The term risk is derived from the Greek word "ριζα", which signifies the danger to be avoided at sea. Risk is a much misunderstood and sometimes misused word. This is not surprising; in its common usage in English, it can also mean chance or gamble. The meaning of the word can therefore change with the context, and with the background of the people using the word. The word risk has a negative connotation; you do not often hear of the risk of winning the jackpot, while you may run the risk of failing an examination. Risk has two aspects. The quantitative (or normative) aspect can be calculated if we know the probability and consequence of an event. The qualitative (or descriptive) aspect relates to people's perception and depends on the emotional state and feelings. Both aspects of risk are important, but their relative importance can differ from case to case. The following research is interesting: Faced with a situation where there is a 50 % chance of gaining 100 $, or a sure gain of 50 $, most people will go for the second option. As opposed to this, if there is a 50 % chance of losing 100 $ against a sure loss of 50 $, most people will opt for the first option. In all these cases the risked value of the loss is the same [5].

Safety: *Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property* (MIL-STD-882D).

This definition has caused considerable controversy [3]. A number of alternative definitions have therefore been proposed. The main controversy is connected to the term "freedom from". Most activities involve some sort of risk and are never totally free from risk. In most of the alternative definitions safety is defined as an acceptable level of risk. The concept safety is mainly used related to random hazards, while the concept security is used related to deliberate actions.

2. HAZARD CAUSAL FACTORS

There is a difference between why hazards exist and how they exist. The basic reasons why hazards exist are: (1) They are unavoidable because hazardous elements must be used in the system, and/or (2) they are the result of inadequate design safety consideration. Inadequate design safety consideration results from poor or insufficient design or the incorrect implementation of a good design. This includes inadequate consideration given to the potential effect of hardware failures, sneak paths, software glitches, human error, and the like. HCFs are the specific items responsible for how a unique hazard exists in a system.

Figure 2 depicts the overall HCF model [4]. This model correlates all of the factors involved in hazard-mishap theory. The model illustrates that hazards create the potential for mishaps, and mishaps occur based on the level of risk involved (i.e., hazards and mishaps are linked by risk). The three basic hazard components define both the hazard and the mishap. The three basic hazard components can be further broken into major hazard causal factor categories, which are: (1) hardware, (2) software, (3) humans, (4) interfaces, (5) functions, and (6) the environment. Finally, the causal factor categories are refined even further into the actual specific detailed causes, such as a hardware component failure mode.

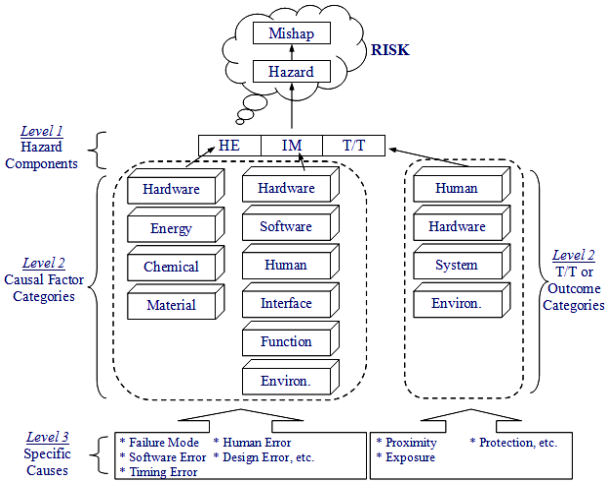

Figure 2. Hazard causal factor model

Figure 2 illustrates how hazard HCFs can be viewed at three different levels:

- *Level 1 – Top Layer:* The three hazard components (HE, IM, T/T),
- *Level 2 – Midlevel:* The HCF categories (hardware, software, human system integration (HSI), environment, functions, interfaces) and
- *Level 3 – Bottom Level:* The detailed specific causes (failure modes, errors, etc.).

3. HAZARD ANALYSIS TYPES AND TECHNIQUES

Hazard analyses are performed to identify hazards, hazard effects, and hazard causal factors. Hazard analyses are used to determine system risk and thereby

ascertain the significance of hazards so that safety design measures can be established to eliminate or mitigate the hazard. Analyses are performed to systematically examine the system, subsystem, facility, components, software, personnel, and their interrelationships.

There are two categories of hazard analyses: *types* and *techniques*. Hazard analysis type defines an analysis category (e.g., detailed design analysis), and technique defines a unique analysis methodology (e.g., fault tree analysis). The type establishes analysis timing, depth of detail, and system coverage. The technique refers to a specific and unique analysis methodology that provides specific results. System safety is built upon seven basic types, while there are well over 100 different techniques available. In general, there are several different techniques available for achieving each of the various types. The overarching distinctions between type and technique are summarized in Table 1.

Table 1. Hazard analysis type vs. technique

Type	Technique
• Establishes where, when, and what to analyze • Establishes a specific analysis task at specific time in program life cycle • Establishes what is desired from the analysis • Provides a specific design focus	• Establishes how to perform the analysis • Establishes a specific and unique analysis methodology • Provides the information to satisfy the intent of the analysis type

Hazard analysis type describes the scope, coverage, detail, and life-cycle phase timing of the particular hazard analysis. Each type of analysis is intended to provide a time- or phase-dependent analysis that readily identifies hazards for a particular design phase in the system development life cycle. Since more detailed design and operation information is available as the development program progresses, so in turn more detailed information is available for a particular type of hazard analysis. The depth of detail for the analysis type increases as the level of design detail progresses. Each of these analysis types defines a point in time when the analysis should begin, the level of detail of the analysis, the type of information available, and the analysis output. The goals of each analysis type can be achieved by various analysis techniques. The analyst needs to carefully select the appropriate techniques to achieve the goals of each of the analysis types.

There are seven hazard analysis types in the system safety discipline [4]:

- *Conceptual design hazard analysis type (CD-HAT)*;
- *Preliminary design hazard analysis type (PD-HAT)*;
- *Detailed design hazard analysis type (DD-HAT)*;
- *System design hazard analysis type (SD-HAT)*;
- *Operations design hazard analysis type (OD-HAT)*;
- *Health design hazard analysis type (HD-HAT)* and
- *Requirements design hazard analysis type (RD-HAT)*.

An important principle about hazard analysis is that one particular hazard analysis type does not necessarily identify all the hazards within a system; identification of hazards may take more than one analysis type (hence the seven types). A corollary to this principle is that one particular hazard analysis type does not necessarily identify all of the hazard causal factors; more than one analysis type may be required. After performing all seven of the hazard analysis types, all hazards and causal factors should have been identified; however, additional hazards may be discovered during the test program.

Figure 3 conveys the filter concept behind the seven hazard analysis types. In this concept, each hazard analysis type acts like a filter that identifies certain types of hazards. Each successive filter serves to identify hazards missed by the previous filter. The thick dark arrows at the top of the filter signify hazards existing in the system design. When all of the hazard analysis types have been applied, the only known hazards remaining have been reduced to an acceptable level of risk, denoted by the smaller thin arrows. Use of all seven hazards analysis types is critical in identifying and mitigating all hazards and reducing system residual risk.

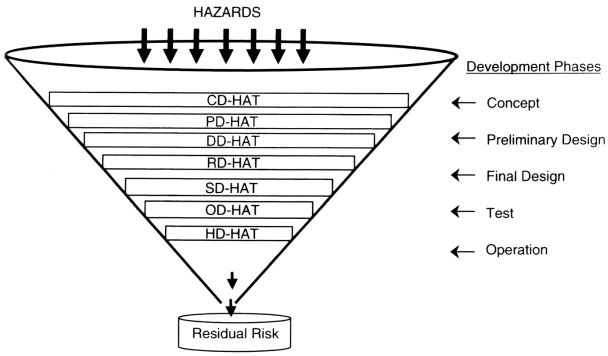

Figure 3. Hazard filters

Each hazard analysis type serves a unique function or purpose. For a best practice system safety program (SSP), it is recommended that all seven of these hazard analysis types be applied; however, tailoring is permissible. If tailoring is utilized, the specifics should be spelled out in the system safety management plan (SSMP) and/or the system safety program plan (SSPP).

Figure 4 depicts the relationship between hazard types and techniques. In this relationship, the seven hazard analysis types form the central focus for SSP hazard analysis. There are many different analysis techniques to select from when performing the analysis types, and there are many different factors that must go into the hazard analysis, such as the system life-cycle stages of concept, design, test, manufacture, operation, and disposal. The system modes, phases, and functions must be considered. The system hardware, software, firmware, human interfaces, and environmental aspects must also be considered.

3.1 Timing of hazard analysis types

Figure 5 contains a consolidated view of the time period over which the hazard analysis types are typically performed [4]. This schedule shows the most typical

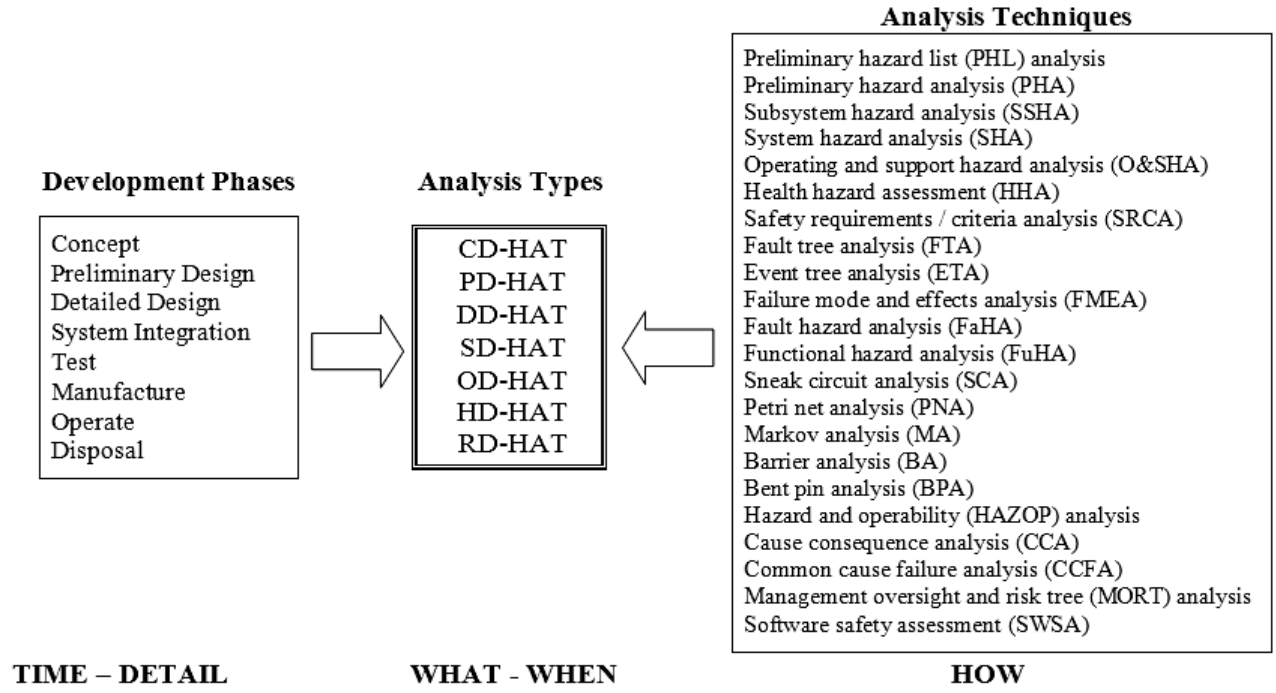

Figure 4. Type-technique relationship

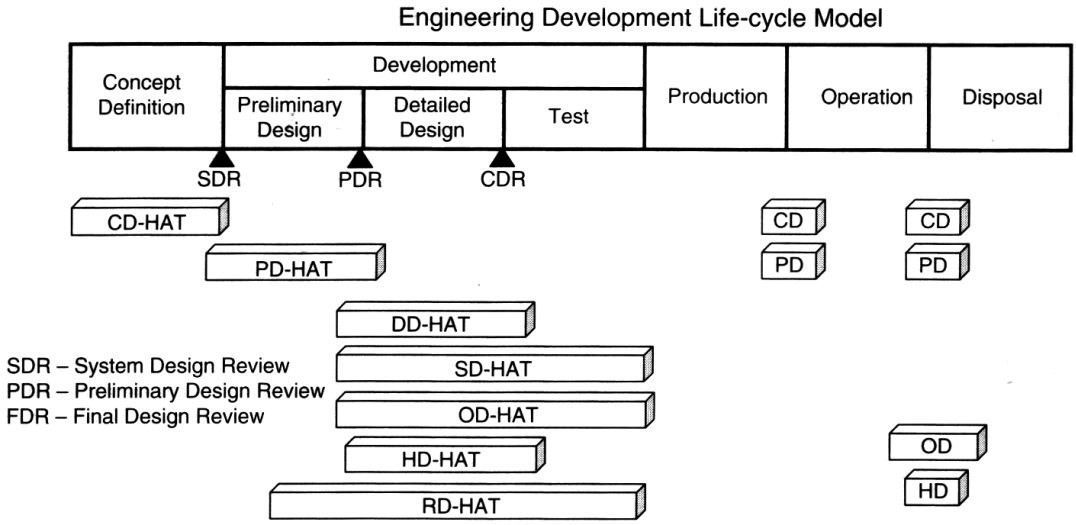

Figure 5. Overall timing of hazard analysis types

timing that has been found practical through many years of trial and error. The system development phases shown are from the standard engineering development life-cycle model. Note how each of the hazard analysis types correlates very closely to its associated development phase. Also, note that some of the analysis types should be performed in a later development phase if that phase was not specifically covered by the original analysis.

The time period for performing the hazard analysis is not rigidly fixed but is dependent on many variables, such as size of the system and project, safety criticality of the system, personal experience, common sense, and so forth. The time period is shown as a bar because the analysis can be performed at nay time during the period shown. Specifying the time period for a hazard analysis is part of the safety program tailoring process and should be documented in the SSPP. Each of the hazard analysis types has a functional time period when it is most effectively applied to achieve the desired intent and goals.

3.2 Hazard analysis techniques

Hazard analysis technique defines a unique analysis methodology (e.g., fault tree analysis). The technique refers to a specific and unique analysis methodology that is performed following a specific set of rules and provides specific result. As previously mentioned, there are over 100 different hazard analysis techniques in existence, and the number continues to slowly grow. Many of the techniques are minor variations of other techniques. And, many of the techniques are not widely practiced. We have pointed out to 22 techniques most commonly used by system safety practitioners. Each of these hazard analysis techniques is important enough to justify the fact it is mentioned in this paper. The system safety engineer/analyst should be thoroughly familiar with each of the analysis techniques considered in this paper. They form the basic building blocks for performing hazard and safety analysis on any type of system.

Technique attributes. Hazard analysis techniques can have many different inherent attributes, which makes their utility different. The appropriate technique to use can often be determined from the inherent attributes of the technique. Table 2 contains a list of the most significant attributes for a hazard analysis methodology. Table 3 summarizes some of the select attributes for the analysis techniques presented in this paper.

Table 2. Major attributes of analysis techniques

	Attribute	Description
1.	qualitative/ quantitative	analysis assessment is performed qualitatively or quantitatively
2.	level of detail	level of design detail that can be evaluated by the technique
3.	data required	type and level of design data required for the technique
4.	program timing	effective time during system development for the technique
5.	time required	relative amount of time required for the analysis
6.	inductive/ deductive	technique uses inductive or deductive reasoning
7.	complexity	relative complexity of the technique
8.	difficulty	relative difficulty of the technique
9.	technical expertise	relative technical expertise and experience required
10.	tools required	technique is standalone or additional tools are necessary
11.	cost	relative cost of the technique
12.	primary safety tool	technique is a primary or secondary safety tool

Table 3: Summary of select attributes for analysis techniques

Technique	Type	Identify hazards	Identify root causes	Life-cycle phase	Qualitative/quantitative	Skill	Level of detail	I/D
PHL	CD-HAT	yes	no	CD-PD	qual.	SS	min.	I
PHA	PD-HAT	yes	partially	CD-PD	qual.	SS	Mod.	I/D
SSHA	DD-HAT	yes	yes	DD	qual.	SS, Eng, M&S	in-depth	I/D
SHA	SD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
O&SHA	OD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
HHA	HD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
SRCA	RD-HAT	partially	no	PD-DD	qual.	SS	in-depth	–
FTA	SD-HAT DD-HAT	partially	yes	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
ETA	SD-HAT	partially	partially	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
FMEA	DD-HAT	partially	partially	PD-DD	qual./quant.	SS, Eng, M&S	in-depth	I
FaHA	DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	in-depth	I
FuHA	SD-HAT DD-HAT	yes	partially	CD-PD-DD	qual.	SS, Eng, M&S	Mod.	I
SCA	SD-HAT DD-HAT	partially	yes	DD	qual.	SS, Eng, M&S	Mod.	D
PNA	SD-HAT DD-HAT	partially	no	PD-DD	qual./quant.	SS, Eng, M&S	in-depth	D
MA	SD-HAT DD-HAT	partially	no	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
BA	SD-HAT	yes	partially	PD-DD	qual.	SS, Eng	Mod.	I
BPA	DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	in-depth	D
HAZOP	SD-HAT DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	Mod.	I
CCA	SD-HAT DD-HAT	yes	partially	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
CCFA	SD-HAT DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	Mod.	D
MORT	SD-HAT DD-HAT	yes	partially	PD-DD	qual./quant.	SS, M&S	Mod.	D
SWSA	SD-HAT DD-HAT	yes	partially	CD-PD	qual.	SS, Eng, M&S	Mod.	–

CD – conceptual design; PD – preliminary design; DD – detailed design; T – testing; SS – system safety; Eng – engineering electrical/mechanical/software; M&S – math & statistics; Mod. – moderate to in-depth.

Inductive and deductive techniques. System safety hazard analysis techniques are quite often labelled as being either an inductive or deductive methodology. For example, a failure mode and effects analysis (FMEA) is usually referred to as an inductive approach, while an FTA is referred to as a deductive approach [6]. Understanding how to correctly use the terms inductive and deductive is often confusing and even sometimes incorrectly applied. The question is: What do these terms really mean, how should they be used, and does their use provide any value to the safety analyst?

The terms deductive or inductive refer to forms of logic and reasoning [2,6]. Deductive reasoning is a logical process in which a conclusion is drawn from a set of premises and contains no more information than the premises taken collectively. The truth of the conclusion is dependent upon the premises; the conclusion cannot be false if the premises on which it is based are true. Inductive reasoning is a logical process in which a conclusion is proposed that contains more information than the observation or experience on which it is based. The truth of the conclusion is verifiable only in terms of future experience, and certainty is attainable only if all possible instances have been examined.

Two additional terms that are confusing to system safety analysts are top-down analysis and bottom-up analysis. In general, top-down analysis means starting the analysis from a high-level system viewpoint, for example, a missile navigation system, and continually burrowing into deeper levels of detail until the discrete component level is reached, such as a resistor or diode. A bottom-up analysis moves in the opposite direction. It begins at a low system level, such as the resistor or diode component, and moves upward until the system top level is reached. These definitions are illustrated in Figure 6.

Some system safety practitioners advocate that a deductive analysis is always a top-down approach and that an inductive analysis is always a bottom-up approach. This may be a good generalization but is likely not always the case. Table 4 summarizes some of the characteristics of inductive and deductive analysis techniques [7].

The bottom line is that in the long run it does not really matter to the safety analyst if a hazard analysis technique is inductive or deductive. An analyst does not select an analysis technique based on whether its methodology is inductive, deductive, top-down, or bottom-up. What is important is that there are various techniques available for identifying hazards and hazard causal factors and that the safety analyst knows how to correctly use and apply the appropriate techniques. An analyst is more concerned with the actual task of identifying and mitigating hazards.

Table 4. Inductive and deductive analysis characteristics

	Inductive	Deductive
Methodology	• What – if • Going from specific to the general	• How – can • Going from general to the specific
General characteristics	• System is broken down into individual components • Potential failures for each component are considered (what can go wrong?) • Effects of each failure are defined (what happens if it goes wrong?)	• General nature of the hazard has already been identified (fire, inadvertent launch, etc.) • System is reviewed to define the cause of each hazard (how can it happen?)
Applicability	• Systems with few components • Systems where single-point failure (SPFs) are predominant • Preliminary or overview analysis	• All sizes of systems • Developed for complex systems • Designed to identify hazards caused by multiple failures
Potential pitfalls	• Difficult to apply to complex systems • Large number of components to consider • Consideration of failure combinations becomes difficult	• Detailed system documentation required • Large amount of data involved • Time consuming
Examples	• Failure mode and effects analysis (FMEA) • Hazard and operability (HAZOP) analysis	• Fault tree analysis (FTA) • Event tree analysis (ETA) • Common cause failure analysis (CCFA)

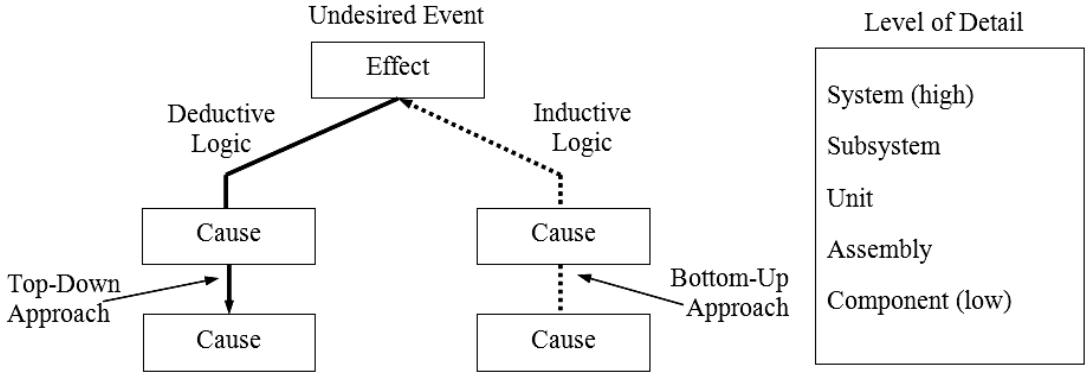

Figure 6. Inductive and deductive analysis relationship

Qualitative and quantitative techniques. System safety analysts are often in a quandary as whether to use a qualitative analysis technique or a quantitative analysis technique. Understanding which analysis type to use, and when, often seems more of an art than a science. The qualitative-quantitative factor is one of the basic attributes of a hazard analysis technique. Table 5 identifies some of the attributes that can be used to judge the strengths and weaknesses of qualitative and quantitative approaches. The system safety discipline primarily uses the qualitative risk characterization approach for a majority of safety work.

Table 5. Differences between qualitative and quantitative techniques

	Attribute	Qualitative	Quantitative
1.	numerical results	no	yes
2.	cost	lower	higher
3.	subjective/objective	subjective	objective
4.	difficulty	lower	higher
5.	complexity	lower	higher
6.	data	less detailed	more detailed
7.	technical expertise	lower	higher
8.	time required	lower	higher
9.	tools required	seldom	usually
10.	accuracy	lower	higher

4. CONCLUSION

Taking into account the previous considerations, we have come to the following conclusion:

- A hazard analysis type defines the analysis purpose, timing, scope, level of detail, and system coverage; it does not specify how to perform the analysis;
- A hazard analysis technique defines a specific and unique analysis methodology that provides a specific methodology and results;
- There are seven hazard analysis types in the system safety discipline that, together, help ensure identification and resolution of system hazards. There are over 100 different analysis techniques that can be used to satisfy the analysis type requirements and
- One particular hazard analysis type does not necessarily identify all the hazards within a system; it may take more than one type, and usually all seven types.

REFERENCES

[1] Popovic, V., Vasic, B. and Curovic, D.: Failure modes, effects and risks analysis – FMERA, Journal of Institute for Research and Design in Commerce & Industry, Vol. 6, No. 20, pp. 33-42, 2008, (in Serbian).

[2] Todorovic, J.: *Maintenance Engineering of Technical Systems*, Institute for Research and Design in Commerce & Industry and Faculty of Mechanical Engineering, Belgrade, 2006, (in Serbian).

[3] Rausand, M. and Høyland, A.: *System Reliability Theory – Models, Statistical Methods and Applications*, John Wiley & Sons, New Jersey, 2004.

[4] Ericson, A.C.: *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, New Jersey, 2005.

[5] Narayan, V.: *Effective Maintenance Management: Risk and Reliability Strategies for Optimizing Performance*, Industrial Press, New York, 2004.

[6] Zelenovic, D. and Todorovic, J.: *Effectiveness of Mechanical Systems*, Science Book, Belgrade, 1990, (in Serbian).

[7] Popovic, V., Vasic, B. and Stanojevic, N.: Contribution to development of new failure analysis methods, in: *Proceedings of the 18th EuroMaintenance Congress/3rd World Congress of Maintenance*, 20-22.06.2006, Basel, Switzerland, pp. 155-160.

ПРЕГЛЕД МЕТОДА АНАЛИЗЕ ОПАСНОСТИ И ЊИХОВИХ ОСНОВНИХ КАРАКТЕРИСТИКА

Владимир Поповић, Бранко Васић

Живимо у свету који чине системи и ризици. Уз системе и технологију, неизбежно долази и до изложености несрећама, пошто системи могу отказати или радити непрописно, што доводи до штете, повреда и смрти. Вероватноћа да систем откаже и доведе до смрти, повреда, штете и слично, зове се ризиком од несреће. Кључни моменат када је реч о безбедности система и ефикасном управљању ризиком, је уочавање и умањење опасности. Да би се успешно контролисала опасност, потребно ју је размотрити, као и знати како је уочити. Циљ овог рада је боље разумевање опасности, као и алата и техника за њено уочавање, да би се иста могла успешно контролисати током развоја система.