IOP Conf. Series: Materials Science and Engineering **252** (2017) 012046 doi:10.1088/1757-899X/252/1/012046

A comparative critical study between FMEA and FTA risk analysis methods

G Cristea[1] and DM Constantinescu[1]

[1]University POLITEHNICA of Bucharest, Romania

E-mail: gabriel.cristea@upb.ro

Abstract. Today there is used an overwhelming number of different risk analyses techniques with acronyms such as: FMEA (Failure Modes and Effects Analysis) and its extension FMECA (Failure Mode, Effects, and Criticality Analysis), DRBFM (Design Review by Failure Mode), FTA (Fault Tree Analysis) and and its extension ETA (Event Tree Analysis), HAZOP (Hazard & Operability Studies), HACCP (Hazard Analysis and Critical Control Points) and What-if/Checklist. However, the most used analysis techniques in the mechanical and electrical industry are FMEA and FTA. In FMEA, which is an inductive method, information about the consequences and effects of the failures is usually collected through interviews with experienced people, and with different knowledge i.e., cross-functional groups. The FMEA is used to capture potential failures/risks & impacts and prioritize them on a numeric scale called Risk Priority Number (RPN) which ranges from 1 to 1000. FTA is a deductive method i.e., a general system state is decomposed into chains of more basic events of components. The logical interrelationship of how such basic events depend on and affect each other is often described analytically in a reliability structure which can be visualized as a tree. Both methods are very time-consuming to be applied thoroughly, and this is why it is oftenly not done so. As a consequence possible failure modes may not be identified. To address these shortcomings, it is proposed to use a combination of FTA and FMEA.

1. Introduction

The ability to predict the reliability of components and systems is important in technical design. Reliability prediction is designed to prevent malfunctions, for example through planned maintenance. The reliability of the individual components is superior to the corresponding system reliability [1].

Optimizing the reliability analysis process requires the use of appropriate quality control tools such as Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). Through these analyzes it is possible to examine the critical parameters of the analyzed process.These are the two commonly used methods for failure analysis.

The first method is failure mode and effects analysis (FMEA). According to MIL-STD-1629 REV.A Standard [2] its definition is “The Failure Mode, Effects and Criticality Analysis (FMECA) is a reliability evaluation/design technique which examines the potential failure modes within a system and its equipment, in order to determine the effects on equipment and system performance. Each potential failure mode is classified according to its impact on mission success and

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

personnel/equipment safety." It is a bottom-up method, starting at the component level, which is used to find failure modes and to identify their effects. By adding a criticality analysis, qualitative FMEA becomes quantitative FMECA (failure mode, effects and criticality analysis).

The second method for failure analysis is Fault Tree Analysis (FTA), which is a top-down method used to identify relationships between events, such as subsystem failures and their causes. According to SAE ARP4761 Standard [3] its definition is "Fault Tree Analysis (FTA) is a deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, a Fault Tree Analysis is a "top-down" system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated."

Both methods are very time-consuming to be applied thoroughly, and this is why it is oftenly not done so.

2. Failure and risk analysis methods

Generally, risk represents the possibility of occurrence of some undesirable events that trigger different types of failures. Risk analysis is used to find the causes of failures and to prevent these failures from occurring in the future. The results of risk analysis can be used to optimize processes.

Risk analysis has two complementary branches:

1. Qualitative.
2. Quantitative.

The task of qualitative analysis is to identify the risk areas of a process, the types of risks and the factors that cause the risks. This is done by an expert through brainstorming. Quantitative analysis allows you to quantify the effect level for each type of risk.

2.1. Basic risk analysis methods

The basic methods for risk analysis are as follows:

1. Analogy.
2. Methods of expertise.
3. Statistical methods.
4. Modeling.

The analogy method focuses on examining analogies between data from a range of sources. Methods of expertise are used to collect the opinions of qualified specialists. A statistical approach to risk analysis uses different types of statistical methods for the processing of data obtained experimentally. The simulation is based on calculating different types of models and testing on these models in different situations.

Among the most commonly used risk analysis methodologies are [4]:

1. Failure modes and effects analysis (FMEA).
2. Fault tree analysis (FTA).
3. Structured What-If Technique (SWIFT).

2.2. Failure mode and effects analysis

FMEA (Failure Mode and Effects Analysis) is an inductive and bottom-up method to identify failure modes, effects and causes of technical systems [5]. The analysis starts at the component level where the possible component failure modes are identified and it is examined what the consequences are on a higher level. FMEA analysis typically involves a diverse team of people with different backgrounds (eg mechanical design, software, production, maintenance), as this increases the probability that all failures will be identified and the effects will be estimated correctly [6].

The FMEA can be extended to FMECA (Failure Mode, Effects and Criticality Analysis) by adding a criticality analysis. In this way, the purely qualitative FMEA can be made quantitative.

In FMECA, the criticality of each failure mode is quantified by the risk priority number (RPN). The risk priority number is the product of three indicators: (a) severity indicator (S), (b) occurrence indicator (O) and (c) detection indicator of a failure (D).

These indicators are usually rated on a scale from 1 to 10 [6]. Standards that provide guidelines for the assessment of each indicator are available, see, e.g., [2].

The severity (S) of a failure refers to the seriousness of the effect or impact of a certain failure. The severity indicator is rated from low impact (e.g., 1 on a scale 1 to 10) to very high impact (e.g., 10 on the same scale).

The occurrence (O) indicator of a failure refers to its failure frequency. The occurrence indicator should be rated from unlikely to occur to almost inevitable.

Finally, the detectability (D) indicator refers to the likelihood that the failure is not detected before it induces major subsequent effects (e.g., by means of process controls, procedures or operator detectability). The detectability indicator should be rated from almost sure detection to almost sure non-detection.

The risk priority number (RPN) represents the entire risk for the system user and serves as a decision criteria for the introduction of optimization actions.

As a matter of principle:

• The larger the RPN is, the greater the priority that the risk is lowered with the help of design and quality assuring actions;

• Likewise, individual values for S, O, and D that are greater than 8 should be more closely observed;

• The product O x D gives information concerning the remaining probability that defective undetected parts will reach the hands of the customer.

The risk assessment is conducted for actions, which have already been implemented. In order to lower the risk even more, additional actions are mostly required.

The observation of the absolute value of the risk priority number (the product S x O x D) is not always sufficient in many cases to find the starting points for optimization actions. Likewise, it is not reasonable to define a "fixed RPN" as a company wide action limit (e.g. optimization conducted for all RPN $\geq$ 250), since the circumstances of the assessment standards may differ for each FMEA and the observation of smaller risk priority numbers could be neglected.

Optimization actions are to be taken for high RPNs and high individual assessment values. Firstly, the calculated risk priority numbers are ranked according to their values. The optimization begins with the failure cause with the greatest RPN and should be ended at a certain lower limit (e.g. RPN = 125), depending on the scope of the analysis.

High individual assessment values must also be observed along with the RPN. A value of O > 8 means that a failure occurs most of the time. Naturally, this must be remedied. A severity value of S > 8 points to serious function impairment or to a serious safety risk. These cases must also be looked at more closely. Failures can be detected with difficulty for values of D > 8. For this reason the danger that these can reach the hands of the customer is increased.

2.3. Fault tree analysis

FTA is a very powerful systematic way which is widely used for estimating process quality. Starting from the top event, the fault-tree method uses a Boolean algebra and a deductive logical modeling to make a graphical representation of the relations among various failure events at different levels of the process.It enables the root causes of the failure events of a process to be found. This type of logic helps to establish a detailed scheme of relationships between the events in the process that can affect its quality.

The advantages of fault trees are as follows:

• Allows potential failure parts of the process to be seen in detail.
• Helps identify failures deductively.
• Enables a qualitative or quantitative analysis of the process to be made.
• The method can focus on individual parts of the process, and can extract specific failures.
• It clearly represents the behavior of the process.

The main advantage of the fault tree (in comparison with other methods) is that the analysis is limited to identify only those events of the process which lead to a specific process failure.

The disadvantages of fault trees are:

• Implementation of the method requires considerable inputs, because more process details lead to a geometric increase in the analyzed area, and the number of influencing events grows correspondingly.

• A fault tree is a Boolean logic diagram, which shows only two states: work and fail.

• It is difficult to estimate the state of partial failure of the process parts, because use of the method generally indicates that the process is either in good condition or in a faulty state.

• It requires a reliability specialist with deep knowledge of the process.

2.4. Combination of FMEA and FTA methods

Both methods are very time-consuming to be applied thoroughly, and this is why it is oftenly not done so. As a consequence possible failure modes may not be identified. To address these shortcomings, it is proposed to use a combination of FTA and FMEA.

Two options can be identified: (a) perform both an FMEA as well as an FTA separately or (b) use a mixed approach.

Concerning the first option, some authors [5] argue that this may expand the number of failure modes found due to the different starting points of both methods: bottom-up in FMEA, versus top-down in FTA. However, performing both analyses would be time consuming and may lead to a loss of focus on the most critical parts of the system, which the failure analysis typically aims to identify.

Concerning the second option, some authors [7] propose a mixed approach in which the FMEA is guided by a FTA. In their proposed approach, the analysis starts with the definition of a system failure event and continues with the construction of a fault tree for a particular system as a whole. Finally, each basic event is analyzed further with FMEA to identify the underlying failure modes of each component.

2.5. Variation mode and effects analysis

The ability to predict reliability of components and systems is important in engineering design. By predicting reliability it is possible to prevent failures. There are several methods for improving the prediction of reliability.

Today, many failures are caused by variations (strength, loads, manufacturing tolerances, etc.), resulting in expensive reclamations and dissatisfaction that may lead to loss of customers [8]. Therefore, a method called Variation Mode and Effect Analysis (VMEA), a relatively new methodology, which is a deductive method of identifying and managing sources of variation, has been developed. The VMEA method has been decomposed into three different levels [9]: Basic VMEA, Enhanced VMEA and Probabilistic VMEA.

1. Basic VMEA is used in the early design stages, where information about the variation is vague and the aim is to compare and evaluate different concepts.

2. Enhanced VMEA is used later in the design stages, where more information about the sources of variation is known.

3. Probabilistic VMEA is used in late design stages, where detailed and statistical information about sources of variation is available.

Product characteristics that are of particular interest from a variation standpoint are selected and are usually referred to as Key Product Characteristics (KPCs). The KPC can be compared to the top event in a fault tree. Each KPC is decomposed into a number of sub-KPCs that are affected by variations.

2.6. Shortcomings of presented methods

FMEA and FTA methods possess shortcomings. First, both methods distinguish only between two levels:

(1) system level and (2) component level. Second, the importance of the level of detail in a failure analysis is not treated with much emphasis. Third, the methods do not possess a feature which enables

to focus the analysis on the most critical elements of a machine. For this kind of analyses, one may want to concentrate on the most critical parts of the system and allocate more attention to these parts. This is related to the efficiency of the analysis, i.e. the required effort to perform the analysis versus the gained knowledge of failure behaviour.

3. Conclusions

Both FMEA and FTA can be used to identify the causes of failures. The result of this approach is a reliability analysis performed through the interaction between the FMEA and FTA reliability tools. Each of these risk analysis methods has advantages that allow for clearer investigation and observation of the process from different points of view.

The FMEA method is generally a library of all possible potential failures and their consequences, while the FTA allows for a detailed analysis of the logical and temporal relationships that lead to a failure taken from the top of the tree. Applying these two complementary methods provides deeper information than the separate application of the methods.

The FMEA method is often used to identify fault modes, to assess the consequences of specific malfunctions and to subjectively infer a risk and a priority number. The VMEA method is used instead to identify, evaluate, and manage unwanted variations to increase system reliability.

Acknowledgments

Mr. Gabriel Cristea acknowledges the PhD student scholarship given by the Ministry of National Education from Romania through the contract no. 06.16/2015 which made possible the present researches. He wishes to thank Professor Cristian Andreescu for the financial support given throughout this research.

References

[1] O'Connor P 2002 *Practical Reliability Engineering* ed John Wiley and Sons (Chichester) p 513
[2] MIL-STD-1629A, Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis -http://everyspec.com/MIL-STD/MIL-STD-1600-1699/
[3] SAE ARP4761 Standard - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment - http://standards.sae.org/wip/arp4761a/
[4] Vose D 2008 *Risk Analysis: A Quantitative Guide* ed John Wiley and Sons (London) p 735
[5] Bertsche B 2008 *Reliability in Automotive and Mechanical Engineering: Determination of Component and System Reliability* ed Springer Berlin (Heidelberg) p 492
[6] Tinga T 2013 *Principles of Loads and Failure Mechanisms: Applications in Maintenance, Reliability and Design* ed Springer (London) p 307
[7] Yu S, Liu J, Yang Q and Pan M 2011 *Proc. of 9th Int. Conf. on Reliability, Maintainability and Safety* pp 954-60
[8] Johansson P 2006 Variation mode and effect analysis: A practical tool for quality improvement *Quality and Reliability Engineering International* **8** 865-76
[9] Johannesson P 2009 Variation mode and effect analysis: An application to fatigue life prediction *Quality and Reliability Engineering International* **2** 167-79