ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering

Tome XII [2014] – Fascicule 4 [November]
ISSN: 1584-2673 [CD-Rom, online]

a free-access multidisciplinary publication
of the Faculty of Engineering Hunedoara

[1.] Ferenc FARKAS

DEVELOPING OF RISK ANALYSIS METHODOLOGIES

[1.] University of Szeged, Faculty of Engineering, Technical Department, Szeged, 7 Mars sq, HUNGARY

Abstract: Generally, risk is the possibility of the occurrence of certain undesirable events that initiate various types of failures. Risk analysis is used to find causes of failures and to prevent the occurrence of these failures in the future. The results of risk analysis can be used for process optimization. Risk analysis is divided into two complementary types: Qualitative and Quantitative. The task of qualitative analysis is to identify the risk areas in a process, types of risks, and the factors causing the risks. This is done in various ways, for example, by an expert, by brainstorming and so on. Quantitative analysis enables the level of effect to be quantified for each type of risk. Basic methods for risk analysis are as follows: 1. Analogies, 2. Expert methods, 3. Statistical methods, 4. Modeling, etc.
Keywords: types of failures, risk analysis, methodologies

1. INTRODUCTION

The analogy approach is focused on an examination of analogies among data obtained from a range of sources. Expert methods are used to collect the opinions of qualified specialists. A statistical approach to risk analysis uses various types of statistical methods to process data that has been obtained experimentally. The simulation is based on calculating various types of models and on testing or these models in various situations.

The followings are some of the most commonly used risk analysis methodologies:

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

2. FAILURE TREE ANALYSIS (FTA)

2.1. History of FTA

FTA was developed at Bell Laboratories in 1962 by H.A. Watson. It was aimed to evaluate the Minuteman I Intercontinental Ballistic Missile. In 1966, Boeing further developed and refined procedures and began to use it in civil aircraft design. After crash of Apollo 1, FTA was performed on the whole Apollo system. Other notable usages consists of failure analysis of NPP Three Mile Island accident in 1979 and Challenger space shuttle accident in 1986.FTA has also been adopted by the automotive industry, chemical process industry, rail industry and robotics industry.

2.2. What is a Fault Tree Analysis?

A fault tree analysis (FTA) is a deductive, top-down method of analyzing system design and performance. It involves specifying a top event to analyze (such as a fire), followed by identifying all of the associated elements in the system that could cause that top event to occur.

Fault trees provide a convenient symbolic representation of the combination of events resulting in the occurrence of the top event. Events and gates in fault tree analysis are represented by symbols.

Fault tree analyses are generally performed graphically using a logical structure of AND and OR gates. Sometimes certain elements, or basic events, may need to occur together in order for that top event to occur. In this case, these events would be arranged under an AND gate, meaning that all of the basic events would need to occur to trigger the top event. If the basic events alone would trigger the top event, then they would be grouped under an OR gate. The entire system as well as human interactions would be analyzed when performing a fault tree analysis.

2.3. FTA Procedure

- ✓ Definition of the problem and the boundary conditions
- ✓ Construction of the fault tree
- ✓ Identification of minimal cut and/or path sets
- ✓ Qualitative analysis of the fault tree
- ✓ Quantitative analysis of the fault tree
- ✓ The system is considered to be functioning properly if at least one path from input to output is functioning properly.
- ✓ Give an expression for system reliability/unreliability
- ✓ Draw an equivalent fault tree model (use only AND, OR, NOT gates)

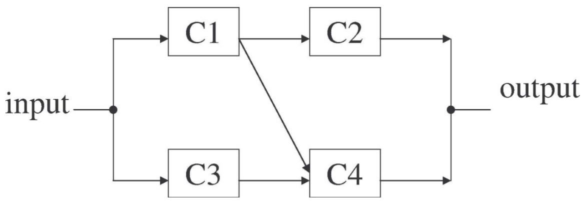

Figure 1. Example of FTA procedure

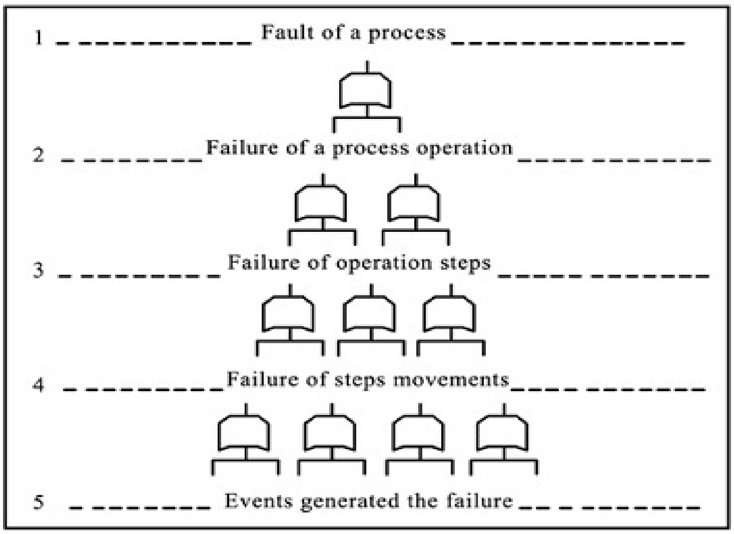

Figure 2. Structure of FTA

3. FAILURE MODE AND EFFECT ANALYSIS (FMEA)

FMEA was developed as military procedure MIL-P-1629 and published on 9. November 1949, titled Procedures for Performing a Failure Mode, Effects and Criticality Analysis. Later in 1960's it was used in aerospace and rocket industry. In 1974 FMEA become military standard Mil-Std-1629. In the late 1970's Ford Motor Company introduced FMEA to automotive industry.

3.1. Process of FMEA

FMEA consists of three main phases. In the first phase of identification, one needs to determine what can go wrong. In the second phase of analysis, one is required to identify the probability of failure, its consequences and according to this calculate the risk priority number. In the third phase one should think out how to eliminate the occurrence or reduce the severity of undesired results.

3.2. How to perform FMEA

Assemble a cross-functional team of people with diverse knowledge about the process, product or service and customer needs. Functions often included are: design, manufacturing, quality, testing, reliability, maintenance, purchasing (and suppliers), sales, marketing (and customers) and customer service.

1. Identify the scope of the FMEA. Is it for concept, system, design, process or service? What are the boundaries? How detailed should we be? Use flowcharts to identify the scope and to make sure every team member understands it in detail. (From here on, we'll use the word "scope" to mean the system, design, process or service that is the subject of your FMEA.)

2. Fill in the identifying information at the top of your FMEA form. The remaining steps ask for information that will go into the columns of the form.
3. Identify the functions of your scope. Ask, "What is the purpose of this system, design, process or service? What do our customers expect it to do?" Name it with a verb followed by a noun. Usually you will break the scope into separate subsystems, items, parts, assemblies or process steps and identify the function of each.
4. For each function, identify all the ways failure could happen. These are potential failure modes. If necessary, go back and rewrite the function with more detail to be sure the failure modes show a loss of that function.
5. For each failure mode, identify all the consequences on the system, related systems, process, related processes, product, service, customer or regulations. These are potential effects of failure. Ask, "What does the customer experience because of this failure? What happens when this failure occurs?"
6. Determine how serious each effect is. This is the severity rating, or S. Severity is usually rated on a scale from 1 to 10, where 1 is insignificant and 10 is catastrophic. If a failure mode has more than one effect, write on the FMEA table only the highest severity rating for that failure mode.
7. For each failure mode, determine all the potential root causes. Use tools classified as cause analysis tool, as well as the best knowledge and experience of the team. List all possible causes for each failure mode on the FMEA form.
8. For each cause, determine the occurrence rating, or O. This rating estimates the probability of failure occurring for that reason during the lifetime of your scope. Occurrence is usually rated on a scale from 1 to 10, where 1 is extremely unlikely and 10 is inevitable. On the FMEA table, list the occurrence rating for each cause.
9. For each cause, identify current process controls. These are tests, procedures or mechanisms that you now have in place to keep failures from reaching the customer.
10. These controls might prevent the cause from happening, reduce the likelihood that it will happen or detect failure after the cause has already happened but before the customer is affected.
11. For each control, determine the detection rating, or D. This rating estimates how well the controls can detect either the cause or its failure mode after they have happened but before the customer is affected. Detection is usually rated on a scale from 1 to 10, where 1 means the control is absolutely certain to detect the problem and 10 means the control is certain not to detect the problem (or no control exists). On the FMEA table, list the detection rating for each cause.
12. Optional) Is this failure mode associated with a critical characteristic? (Critical characteristics are measurements or indicators that reflect safety or compliance with government regulations and need special controls.) If so, a column labeled "Classification" receives a Y or N to show whether special controls are needed. Usually, critical characteristics have a severity of 9 or 10 and occurrence and detection ratings above 3.
13. Calculate the risk priority number, or RPN, which equals S * O * D. Also calculate Criticality by multiplying severity by occurrence, S * O. These numbers provide guidance for ranking potential failures in the order they should be addressed.
14. Identify recommended actions. These actions may be design or process changes tolower severity or occurrence. They may be additional controls to improve detection. Also note who is responsible for the actions and target completion dates.
15. As actions are completed, note results and the date on the FMEA form. Also, note new S, O or D ratings and new RPNs.

4. CONCLUSION

Alternatives to FTA include Dependance Diagram (DD), also known as Reliability Block Diagram (RBD) and Markov Analysis. A Dependence Diagram is equivalent to a Success Tree Analysis (STA), the logical inverse of an FTA, and depicts the system using paths instead of gates. DD and STA produce probability of success (i.e., avoiding a top event) rather than probability of a top event.

REFERENCES

[1.] McDermott, R. E., Mikulak, R. J., Beauregard, M. R. (2009) The basics of FMEA. 2nd edition. New York : Taylor & Francis Group, LLC.

[2.] Queiroz, S. R., Alvares, A. J. (2008) FMEA and FTA Analysis for Application of the Reliability Centered Maintenance Methodology: Case Study on Hydraulic Turbines. Symposium Series in Mechatronics, 3, pp. 803-812.

[3.] http://www.mtain.com/relia/relfmeca.htm

[4.] http://www.asq.org/learn-about-quality/process-analysistools/overview/fmea.html

[5.] http://www.bassengineering.com/FTA.htm

[6.] http://www.fault-tree.net/papers/ericson-fta-history.pdf

[7.] http://www.faa.gov/library/manuals/aviation/risk management/ss handbook/media/Cha p9 1200.pdf

[8.] http://syque.com/quality tools/toolbook/FTA/example.htm