University of Ljubljana

Faculty of Computer and Information Science

Failure Mode and Effects (and Criticality) Analysis Fault Tree Analysis

Report

Computer Reliability and Diagnostics

Assoc. Prof. PhD Miha Mraz

Ľuboš Slovák

2009/2010

Contents

Introduction 3

Motivation 3

Safety engineering 3

Techniques 4

Standards and history 4

Failure Mode and Effects Analysis 6

Overview 6

Types 6

Procedure 7

Ranking and scales 9

Example 11

Failure Mode, Effects and Criticality Analysis 12

Overview 12

Procedure 13

Fault Tree Analysis 14

Overview 14

Procedure 14

Examples 15

Other techniques 16

Software tools 17

Conclusion 18

Bibliography 19

Introduction

Motivation

In recent decades, the need for high-quality, reliable products have increased enormously, and such systems are more and more often part of our everyday life. Cars, personal computers, microwave ovens and other such products are used on a daily basis and their failures may often result in severe damage, loss of data or even loss of lives. On the other hand, in the fields with the highest demands for reliability (such as avionics, space programs, military, etc.) the products, systems and processes used are becoming incredibly complex, what makes it very difficult to maintain their reliability.

Usually, the desired reliability would be achieved by thorough testing of the product, or probabilistic reliability modeling, followed by fixes and appropriate changes to the product. This approach is indeed useful and may help to recognize the weak points of the product and improve the reliability by using techniques such as system and component redundancy, N-modular redundancy, backup systems, etc. However, these methods can often be used only in late changes of the development process and thus it is very expensive, time-consuming, or even impossible to achieve the required reliability.

The goal of the techniques described in this paper is to introduce the concept of reliability and/or fault-tolerance in earlier stages of the development, particularly in the design phase. This should result in better, fault-free (or at least fault-tolerant) designs needed for certain purposes.

Safety engineering

Safety engineering is an applied science studying the reliability of critical systems and ensuring that the system will behave as expected even if failures occur. Safety-engineers analyze design of a system and propose new additions to the specification or changes to an existing system which will make the system safer. In practice, however, their role is often to prove that an existing system is safe, which may not always be true, in which case the necessary corrections may be very expensive.

Techniques

This paper focuses on two perhaps most commonly used methods for analyzing and modeling potential faults in the system and their effects on it. These are:

- **Failure modes and effects analysis** (FMEA) and its extension **Failure Mode, Effects, and Criticality Analysis** (FMECA), and
- **Fault tree analysis** (FTA).

These techniques are used to exhaustively search for potential problems in any part of the system, to describe their impact on the system as a whole, to plan possible actions to reduce failures, and to evaluate the results of the actions taken. They can be used very early in the development cycle, even as soon as the design stage.

FMEA is a **bottom-up**, **inductive** analytical method which studies the effects of single component or function failures on the system or subsystem. It is useful for exhaustive listing of all potential initiating faults, but cannot analyze effects of multiple coincident failures.

FTA is basically a reverse (**top-down**, **deductive**) procedure and can be successfully used to examine events of (possibly multiple) initiating faults or external events on a complex system, but does not fit for listing all possible initiating faults.

In practice, these two methods may be (and often are) used together to achieve even better and more reliable designs.

Standards and history

There are many standards and quality systems incorporating FMEA/FMECA and/or FTA, often specifically designed for certain area, such as automotive and avionic industry, power plants (especially nuclear), space programs, etc.

The first standard which introduced the ideas of **FMEA** and **FMECA** was, however, a U.S. military standard MIL-STD-1629, published in 1949 as a procedure and standardized in 1974. Even before standardization, many industries adopted these methods in their processes. This standard was later updated by MIL-STD-1629A. Other industry standards include for instance SAE J1739 or AIAG FMEA-3.

In 1960s FMEA and FMECA began to be used in NASA and its partners and since then it was used in many NASA programs, including Apollo, Viking, Voyager and Galileo. In the same time, the civil avionic industry also started to use these techniques in designing aircraft. In 1970s it spread also to automotive industry, beginning with the Ford Motor Company.

FTA was developed in 1962 at Bell Laboratories when evaluating the Minuteman I Intercontinental Ballistic Missile Launch Control System for the U.S. Air Force Ballistics Systems Division. Around 1966 Boeing started using FTA in the design of civil aircraft. In 1970 a change in airworthiness regulations for transport aircraft led to extensive use of FTA in civil aviation. In 1975 this method found usage also within the nuclear power industry.

A general, cross-industry standard for FTA was issued by IEC under the code IEC 61025, and later adopted by European Union as EN 61025. Besides that, many industry standards for specialized uses are available, such as NRC NUREG-0492 (nuclear power industry) or SAE ARP4761 for civil aerospace.

Failure Mode and Effects Analysis

Overview

As mentioned in the Introduction, **Failure Mode and Effects Analysis** (**FMEA**) is a safety engineering technique aimed at identifying and classifying potential failure modes[1], their effects on the system and defining actions to avoid these failures. It may be performed at either the functional or piece-part level. Ideally, it should begin as early as the design stage of the system and continue throughout the whole life cycle. Its main use is to classify the effects of potential failure modes by **severity**, **occurrence** and **detection** and subsequently prioritize the actions needed to counteract or avoid these failures. This may be done by calculating the **risk priority numbers** (**RPN**) for each failure mode, though it is not necessary as the nature of certain products requires prioritizing only one or two of the characteristics.

As an essential prerequisite, an exhaustive list of potential failure modes must be compiled. While it is not possible to anticipate every possible failure mode, it is very important to do the search as thorough as possible. It is necessary for the FMEA to be conducted by a **team of experts with various views** of the product. The designer of the product is essential, but as he or she often lacks the necessary critical view of the product, experts from other fields or even the customer should be part of the team.

The output of the analysis is a **FMEA Table** which lists all the failure modes together with possible effects on the system or subsystem categorized considering the aforementioned characteristics.

Types

There are several types of FMEA distinguished by the subject of the analysis:

- **System** – aims at the whole system and its functions,
- **Design** – focuses at the components or subsystems in the design stage,
- **Process** – studies the manufacturing and assembly processes,

[1] Failure mode: The manner by which a failure is observed; it generally describes the way the failure occurs.

- **Service** – analyses services,
- **Software** – focuses on the software functions instead of hardware.

Procedure

The procedure of FMEA is straightforward and can be divided into several distinct steps.

1. As a first step, the **subject** of the analysis must be **defined** and **described** together with possible uses of the product, both intentional and unintentional, which are related to the subject.
2. A **block diagram** of the subject should be created, which shows the main components of the product, or process steps as blocks connected according to relations between them. Around these relations the FMEA can be developed. The FMEA Table worksheet should be also prepared in this step.
3. Use the diagram to **list items or functions** of the subject in the worksheet.
4. **Identify potential Failure Modes**. These should be defined as the way in which the subject may fail to satisfy the designed purpose. Examples of such failure modes may be corrosion of a component, electrical short-circuiting, deformation of the component, etc. Failures should be listed in technical terms and for each component or process step, as a failure mode in one component or process step may become a cause of failure mode in another.
5. **Determine Failure Effects** – results of a failure mode on the subject as perceived by the user. These may include noise, degraded performance or even inoperability of the product, injuries or even loss of lives. Classify the effects according to their severity by giving them a **severity number** or **category** and using a chosen scale. This is later used to prioritize the failure modes and determine which actions have to be taken to avoid potential faults.
6. **Identify** all possible **Failure Causes** for each failure mode listed in step 4. A failure cause is "design weakness that may result in a failure“[2]. They should be defined in technical terms as well. Examples may include improper operating conditions, erroneous algorithms, excessive loading, etc.

[2] http://www.qcinspect.com/article/fmea-an_overview.htm

7. The **probability of the Occurrence** of the causes should be ranked, again in some chosen scale.
8. Examine and **identify the Current Controls** – mechanisms for eliminating the causes of the failure modes or for detecting the failure before it reaches the customer. Henceforth, the testing, analysis, monitoring, and other techniques of avoiding the failure causes or detecting failures used in same or similar products/processes should be investigated.
9. The **probability of Detection** should be determined and ranked. This should reflect the likelihood of the Current Controls detecting the Failure Cause or the Failure Mode itself.
10. The **Risk Priority Numbers (RPN)** are computed as a simple product of the Severity, Occurrence and Detection ratings:

    $$RPN = (Severity)x\ (Occurrence)x\ (Detection)$$

    This value may then be used to prioritize the failure modes that require a corrective action. In some areas, however, the individual ratings may be given different significance.
11. A list of **Recommended Actions** to improve the system and its design should be compiled, addressing the most important potential problems according to the previous step. These may include inspection, testing, redesigning of the product/process, replacing individual components, adding redundancy to the system or its components, scheduling preventive maintenance, etc.
12. The **responsibility and completion dates** for these actions must be set to be able to track the improvement process.
13. Point out the **Actions Taken**, determine the new Severity, Occurrence and Detection ratings of the subject, revise the RPN, and assess the results. Determine if the actions satisfied the expectations or whether further actions are needed.
14. Continue to **update FMEA** anytime the product or process changes.

Ranking and scales

Though the scales for ranking severity, probability of occurrence and probability of detection may be chosen arbitrarily at the beginning of the FMEA, there are few commonly used scales which simplify data and result reusability or compatibility across different software tools (see section Software).

One of these scales rates all the characteristics to numbers between 1 and 10 in the following way:

- **Severity**: 1 – no effect or danger; 10 – very severe or catastrophic effects.
- **Occurrence**: 1 – not likely to occur, 10 – almost inevitable.
- **Detection**: 1 – almost certain to detect, 10 – almost impossible to detect the failure.[3]

Another scale is one defined by the MIL-STD-1692A standard. However, this standard defines no scale for Detection probability, which is also omitted from the computations. These scales are further updated and specified in another U.S. military standard – MIL-STD-882D which is often used today in many military and commercial operations (see Figures 1 and 2).

[3] Detailed information may be found here: http://www.fmeainfocentre.com/examples/fmeadev.pdf

- **Severity**

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Figure 1 - Severity levels according to MIL-STD-882D[4]

- **Occurrence**

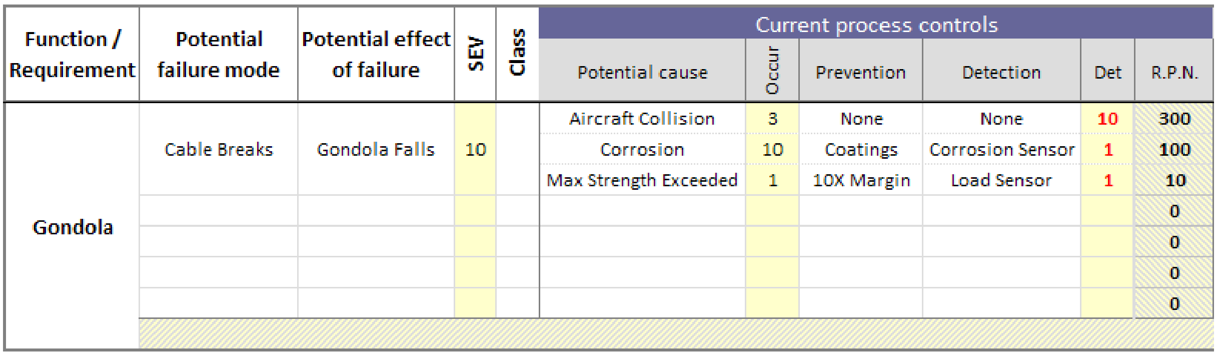
Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Figure 2 - Occurence probability levels according to MIL-STD-882D[5]

[4] MIL-STD-882D, p. 18, obtained on 30th March 2010 from http://www.safetycenter.navy.mil/instructions/osh/milstd882d.pdf

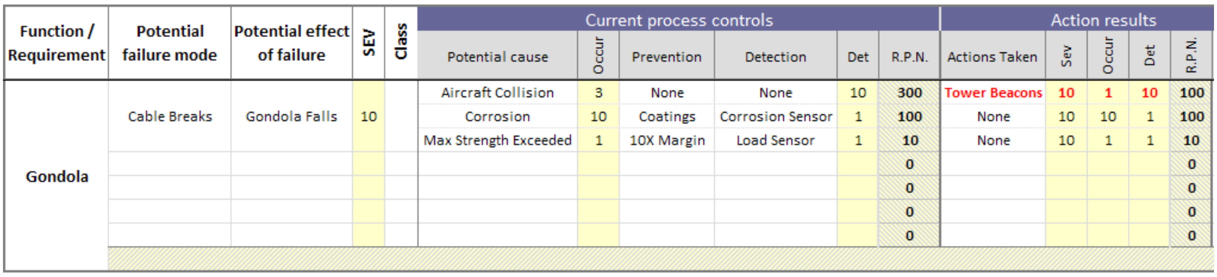
Example

Here is an example of a filled FMEA table examining the potential failure modes of a gondola (a cableway) and the same table filled after the action has been taken to address these possibilities.



Function / Requirement	Potential failure mode	Potential effect of failure	SEV	Class	Current process controls					
					Potential cause	Occur	Prevention	Detection	Det	R.P.N.
Gondola	Cable Breaks	Gondola Falls	10		Aircraft Collision	3	None	None	10	300
					Corrosion	10	Coatings	Corrosion Sensor	1	100
					Max Strength Exceeded	1	10X Margin	Load Sensor	1	10
										0
										0
										0
										0

Figure 3 - FMEA Table of a gondola (cableway)[6]



Function / Requirement	Potential failure mode	Potential effect of failure	SEV	Class	Current process controls						Action results				
					Potential cause	Occur	Prevention	Detection	Det	R.P.N.	Actions Taken	Sev	Occur	Det	R.P.N.
Gondola	Cable Breaks	Gondola Falls	10		Aircraft Collision	3	None	None	10	300	Tower Beacons	10	1	10	100
					Corrosion	10	Coatings	Corrosion Sensor	1	100	None	10	10	1	100
					Max Strength Exceeded	1	10X Margin	Load Sensor	1	10	None	10	1	1	10
										0					0
										0					0
										0					0
										0					0

Figure 4 - FMEA Table of a gondola (cableway) after taking preventive actions[7]

[5] As above, p. 19

[6] Source: http://www.sigmazone.com/gondola_lift_fmea.htm, obtained on 30th March 2010

[7] Source: http://www.sigmazone.com/gondola_lift_fmea.htm, obtained on 30th March 2010

Failure Mode, Effects and Criticality Analysis

Overview

As already mentioned, **FMECA** extends FMEA by introducing the notion of **criticality** into the analysis. All aforementioned characteristics of FMEA are applicable to FMECA as well. In addition a **criticality analysis** is performed as part of the procedure. We may distinguish two basic types of criticality analysis, according to MIL-STD-1692A standard:

- **Qualitative** – this approach is very similar to computing of the risk priority numbers (RPNs), but only severity and occurrence are taken into account. Failure modes are compared according to the **Criticality Matrix** which has severity levels on the horizontal axis and occurrence on the vertical axis[8].
- **Quantitative** – this type of criticality analysis computes **modal criticality numbers** (C_m) for each failure mode of each item and **item criticality numbers** (C_r) for each item using this formulas:

  $$\boldsymbol{C_m = \lambda_p \alpha \beta t}$$

  $$\boldsymbol{C_r = \sum_{n=1}^{N} (C_m)_n}$$

  Where:

  - λ_p is the basic failure rate of a item
  - α is the failure mode ratio, i.e. "the fraction of the part failure rate (λ_p) related to the particular failure mode under consideration …"[9]
  - β is "the conditional probability that the failure effect will result in the identified criticality classification, given that the failure mode occurs" [10]
  - t is the duration of the mission phase or simply the operating time
  - N is the number of failure modes related to the analyzed item.

[8] See MIL-STD-1629A, Figure 102.2, p. 102-7

[9] MIL-STD-1629A, p. 102-3, obtained on 29th March 2010 from http://www.sre.org/pubs/Mil-Std-1629A.pdf

[10] As above

Procedure

The procedure of FMECA is similar to the procedure of FMEA (see p. 4 – 5) with additional steps performed approximately after step 10 of FMEA. These include:

a. Do the **criticality computations** and rank the failure mode criticality using either qualitative or quantitative approach (see above).
b. Determine **critical items** in the system.

The recommended actions are then suggested according to the criticality of the failure modes, which becomes the main classifying characteristic.

Fault Tree Analysis

Overview

As already mentioned in the Introduction, **Fault Tree Analysis** (**FTA**) is a **deductive**, **top-down** method of failure analysis. It studies one failure event at a time by constructing a **fault tree** with the studied event as a root and all possible causes of the failure represented as a series of logic expressions. A sample fault tree may be seen in Figure 5.

The terms **Cut Set** and **Minimal Cut Set** are often used to describe the route between the fault (root) and the cause of the event, and the shortest such route respectively.

Procedure

As with the FMEA/FMECA techniques, the basic procedure of FTA can be summarized into few steps:

1. **Identify possible failures** to be studied by the FTA. The list of potential failures may be obtained using the FMEA, or just simply by studying the system. These failures will be used as roots for the failure trees developed in the following steps.
2. Taking one potential failure at a time, **list all possible immediate causes** of this failure and connect them to the failure node (the root node) using logical gates to represent the relationships. [11]
3. Use similar **top-down** process **recursively** to identify causes of the previous (higher level) events while possible, i.e. while the **root causes** for the failures are not identified.
4. The **probabilities of failure** should be determined and assigned to the leaf nodes of a fault tree (the root causes) and using Boolean equations the probability of the top event (the studied failure) should be computed.
5. Possible **countermeasures are proposed and developed.**

[11] A fairly exhaustive list of possible gates and primary event blocks may be found here: http://www.weibull.com/basics/fault-tree/index.htm

Examples

In the following figure, a simple fault tree may be seen that studies a failure of a spacecraft. Only basic AND and OR gates are used for this tree.

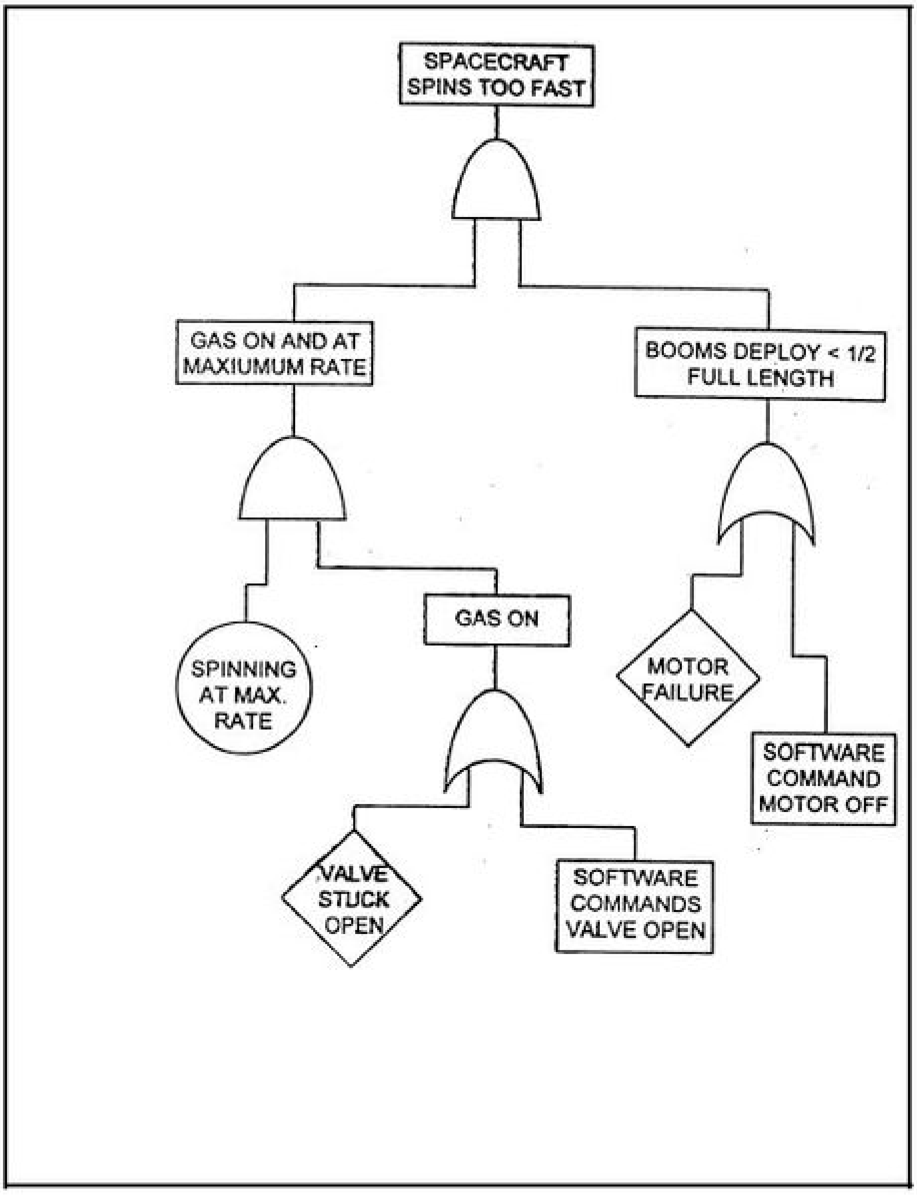

SPACECRAFT SPINS TOO FAST
GAS ON AND AT MAXIUMUM RATE
BOOMS DEPLOY < 1/2 FULL LENGTH
SPINNING AT MAX. RATE
GAS ON
MOTOR FAILURE
SOFTWARE COMMAND MOTOR OFF
VALVE STUCK OPEN
SOFTWARE COMMANDS VALVE OPEN

Figure 5 - Example of a fault tree[12]

[12] Source: http://www.hq.nasa.gov/office/codeq/doctree/871913.pdf, obtained on 30th March 2010

Other techniques

There are several other techniques which may be used to analyze potential failures of a system or its components, or to study the reliability of a system design. Alternatives include **Dependence Diagram**, which is more commonly known as **Reliability Block Diagram** (**RBD**)[13]. **Success Tree Analysis** (**STA**) is basically equivalent to RBD and represents a logical inverse of an FTA. However, constructing a success tree may be significantly more demanding.

[13] See http://en.wikipedia.org/wiki/Reliability_block_diagram

Software tools

There are many tools available that can aid the implementation of FMEA/FMECA or FTA, either in form of specialized standalone applications, or as various plug-ins and modules to a more general application. However, basic FMEA/FMECA or FTA can be easily carried out using general tools like spreadsheet software (for the former) or some diagram/flowchart software (for the latter).

The leading specialized software tools, which can be used for FMEA/FMECA include:

- **Xfmea** by ReliaSoft. Reliasoft is a U.S. company specialized in developing reliability engineering software tools and in providing training and services in this field.
- **Fault Tree Analysis, ITEM ToolKit Module** by ITEM Software is a module to the ITEM ToolKit, a general and comprehensive reliability analysis and safety software tool.
- **RAM Commander** by Advanced Logistics Development which contains a module for FMEA/FMECA as well as for the FTA.
- **Byteworks FMEA Software** by Byteworks which is currently used by the Ford Motor Company.

When using FTA, one can find the following applications useful:

- **BlockSim** by Reliasoft is aimed at supporting both Reliability Block Diagrams and Fault Tree Analysis.
- **Fault Tree Analysis, ITEM ToolKit Module** by ITEM Software (see above).
- **OpenFTA** by Formal Software Construction Limited – an open-source software tool specialized in FTA.

Conclusion

In this paper we described the basics of two probably most used techniques of safety engineering aimed at analyzing potential failures of a product or process which are useful in designing high-quality, reliable and fault-tolerant products or processes.

These techniques – Failure **Mode and Effects (and Criticality) Analysis** (**FMEA / FMECA**) and **Fault Tree Analysis**, were introduced by reviewing the history of their emergence and spreading into all kinds of industry areas, together with listing of some important standards which formalize them.

In the following sections we described all three methods in more detail, providing step-by-step instructions for implementing them as well as some examples from practice. We explained the differences between these techniques which implies also their potential usage.

We also outlined a few alternatives which may be used in the field of safety engineering as well, but which were not the focus of this paper.

Bibliography

Department of Defense, United States of America. (1980). *Procedures for Performing a Failure Mode, Effects and Criticality Analysis, Military Standard (MIL-STD-1629A).* (Also available on http://www.sre.org/pubs/Mil-Std-1629A.pdf as of 27 March 2010)

Department of Defense, United States of America. (2000). *Standard Practice for System Safety, Military Standard (MIL-STD-882D).* (Also available on http://www.sre.org/pubs/Mil-Std-1629A.pdf as of 29 March 2010)

Failure Modes, Effects and Criticality Analysis. ReliaSoft. http://www.reliasoft.com/newsletter/3q2002/fmea.htm (accessed 27 March 2010).

Failure Mode, Effects and Criticality analysis. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Failure_Mode,_Effects,_and_Criticality_Analysis (accessed 27 March 2010).

Failure mode and effects analysis. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis (accessed 27 March 2010).

Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA). Weibull.com. http://www.weibull.com/basics/fmea.htm (accessed 29 March 2010).

Fault Tree Analysis. Weibull.com. http://www.weibull.com/basics/fault-tree/index.htm (accessed 29 March 2010).

Fault tree analysis. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Fault_tree_analysis (accessed 27 March 2010).

FMEA: An Overview. QC Inspeciton Services, Inc. http://www.qcinspect.com/article/fmea-an_overview.htm (accessed 27 March 2010).

Mayfield, P. *FMEA Tutorial.* SigmaZone.com. http://www.sigmazone.com/gondola_lift_fmea.htm (accessed 29 March 2010).

NASA Software Safety Guidebook, NASA Techical Standard. (2004) (also available on http://www.hq.nasa.gov/office/codeq/doctree/871913.pdf as of 29 March 2010).

Safety engineering. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Safety_engineering (accessed 27 March 2010).

What is Failure Mode and Effects Analysis? Resource Engineering, Inc. http://www.reseng.com/overviews/fmea_overview.htm (accessed 29 March 2010).