"Rethinking Risk and Failure Analytics"

"…seeing they may see and not perceive…"
Bible, Isaiah 6:9; Mark 4:12
"No risk, no fun…if there is no Risk Management"
Bluvband, 2002

SUMMARY

Sense of management lies in a permanent decision-making, wherein every decision is characterized by taking (and even facing) risks: “blindfold” ones if missed, or well expected – foreseen, analyzed, evaluated, and prepared for.

The purpose of this paper is to review, analyze and compare the popular and more-or-less standard Risk and Failure Analysis Instruments (RFAI), carefully reflect and explore their typical usage, pitfalls, problems and possible remedies.

The paper starts with necessary definitions and then presents a multidimensional toolbar of well-known and newly introduced RFAIs, possible mistakes and failures in those tools’ application.

1 INTRODUCTION

All business decisions are made under conditions of risk, and one primary objective in Product/Process/Organization management is elimination or mitigation of a risk - the risk of product or process failure.

Remark. Kume (1985) describes tree more error-handling principles in addition to Elimination and Mitigation: Detection, Replacement and Facilitation.

From the organization's perspective, elimination of failures is the most desirable principle.

Decisions must be taken on how to prepare the system or process to prevent the most damaging errors, faults and failures and implement recovery processes after failures occur (Bluvband, 1999) (see figure 1).

The purpose of a failure analysis is to eliminate the causes of failures identifying Preventive engineering actions that eliminate the cause of potential failures or define contingent actions that may mitigate effects of failure mechanisms that cannot be eliminated.

This action must take multiple viewpoints from the customer, design, process and product perspectives.

However, this is not always a feasible goal in the industry and services, where business and trade considerations, such as capturing a larger market share, minimizing Time-To-Market, demonstrating innovations, etc. drive software and hardware manufacturers to introduce new products / new services based on their products, before run-up, testing, fixing and de-bugging has been completed.

Therefore, one should be prepared for Detection, Replacement, Facilitation and Mitigation which are the more conventional ways of error handling in software, hardware and process engineering.

2 DEFINITIONS

This paragraph will introduce and define some terms, which are in use throughout the paper.

First, consider a model of defects focused upon the idea of their preventing, isolating and detecting.

Let's begin with some definitions of Error (Flaws), Fault and Failure (in accordance with definitions from IEEE Standard 1044-1993).

Considering these FFF (**"three F's")**: **F**law, **F**ault, **F**ailure, one can use the term **"defect"** to refer to any abnormality, irregularity, inconsistency, or variance from expectations. It is important to mention that in practice, i.e. in field we are experiencing the Failures as "showstoppers", unless very high level of testability is achieved and even Faults or yet Flaws are timely detected and appropriately reacted (stop the activity; fix - go ahead; go ahead – fix later: in case of redundancy or low severity of possible Failure; etc.).

It may be used to refer to a condition or an event, to an appearance or a behavior, to a form or a function)

- **Flaws (Errors)** are **defects** in the human thought process or, as a result, in manufacturing, made while trying to understand given information, to solve problems, or to use certain initial methods and tools.
- **Faults** are actual manifestations of flaws within the product/process.
  The relationship here is "many-to-many":
  One flaw may cause several faults, and various flaws may cause the same fault.
- **Failures** are departures of the operational system/process behavior from the expected requirements.

A particular failure may be caused by several faults, one fault may cause several failures, and some faults may never cause a failure.

Remark. This provides some insight into the reliability:

The system may contain faults but if those faults will never be executed, it is reliable.

- **Failure Cause (FC)** - is defined as the circumstances during design, manufacture or use which have led to a failure (BSI, BS 4778-3.2, 1991).
- **Failure Mode (FM)** - is defined as the physical or functional manifestation of a failure (IEEE Std-610.12, 1991).
- **End Effect (EE)** - is defined as the consequence(s) of a failure mode for the operation, function, or status of the highest indenture level (MIL-Std-1629, 1980). For all practical purposes, this definition can be extended to include system/equipment availability.
  End Effect is linked to the definition of Risk.
- **Risk** - may be defined as **the effect of uncertainty on objectives (ISO 31000)**. Risks originate from a variety of sources: they can come from uncertainty in markets, and unwanted results of project/process/product failures, originating as an flaw or fault (see below) at any phase (research, design, development, production, or field usage) expressed in legal liabilities, credit hazards, accidents, natural causes and disasters.

  Sometimes the risk comes from deliberate moves by competitors, and events that have uncertain or unpredictable root-cause.

However, risk is also a function of the adequacy of our objectives. It increases if we only look at one aspect of our objective – the achievement of a positive function and do not consider in a real way how to avoid the negative aspects of performance.

Risk may be classified according to its origin as hazardous risk, uncertainty risk or opportunity risk.

- Hazardous risks: potential negative events that will result in catastrophic product failure - and the potential liability for damages to consumers.
  The business goal is to eliminate or mitigate hazardous risks.
- Uncertainty risks: the risk that comes from natural variation in anticipated business outcomes (product wear-out, production waste, obsolescence, efficiency, etc.) The business goal is to manage in such a way as to mitigate or minimize uncertainty risk.
  Engineering managers must manage these uncertainty risks.
- Opportunity risks: the risks implicit in the relationship between risk, growth, and return. Opportunity risk is event-driven based on the market. The business goal is to manage opportunity risk to maximize return.

Business managers are responsible for managing opportunity risks.

While there are many specific types of risk to be addressed by managerial decisions, this paper focuses on those risks (not necessary mutually exclusive ones) that tend to dominate the application of a product or service in the ultimate user's environment:

- **Technological** risk: ability to perform to expectations over time
- **Performance** risk: ability to consistently deliver the customer performance expectation
- **Safety** risk: ability to prevent injury or accident during customer operation as a result of FFF.
- **Security** risk: ability to prevent injury or accident during customer operation as a result of deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.
- **Quality** risk: ability to prevent FFF during production
- **Logistics** risk: ability to deliver the system and support its operation
- **Liability** risk: ability to avoid any product liability concerns from a producer perspective

3 RISK and FAILURE ANALYSIS INSTRUMENTS

Over the years, many approaches, tools and instruments were developed for Risk and Failure Analysis (RFA). These Instruments can be distinguished by categorization using the following dimensions:

In following paragraphs the thorough examination of the RFAI will be presented, getting the clues and recommendations for RFAI prioritization: how and what to use in different applications, possible usages and for variety of users.

4 Direction, Visibility, Correctness and Completeness of the Analysis.

All RFAI can be divided into two parts: Inductive (FMECA, FMEA, ETA), Deductive (CED, FTA), and Bidirectional (Bounced FA, Model-Based)

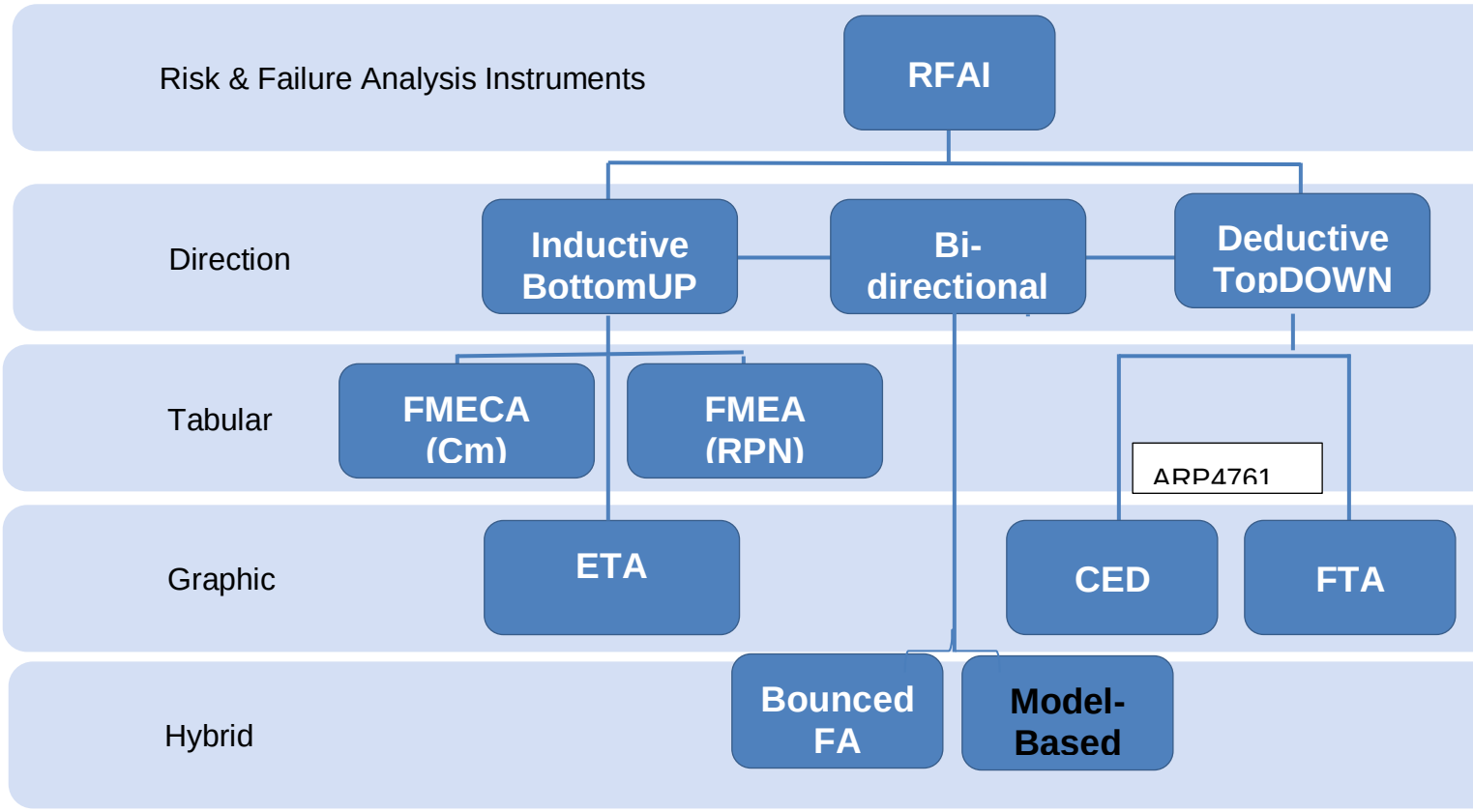


Fig.1 RFAI Chart

1.1 Direction, Visibility and Correctness

In an inductive approach the examiner starts with lowest possible level items, applying known statistical or hypothetical/theoretical data: failure modes, causes, rates and possible local effects, and then moves from those particular experiences to a more general set of consequent next level effects, accumulating those influences as Next Level Effects. In other words, considering, for example, product tree, the investigation moves step-by-step accumulating and integrating from lower level, through all the next higher levels, up to the top product level, estimating the EE of the whole product/process. Figure 2 "Inductive FA" outlines the steps involved with an inductive approach of the FMEA.

FMEA is a classic tool of what we refer to as "Disciplined Engineering" - a systematic framework considered as a tool to reduce potential errors, prevent common mistakes, and improve the consistency of the engineering work.

The purpose of FMEA is to examine possible failure modes and determine the impact of these failures on the product (FMECA or more contemporary Design FMEA – DFMEA) and the process (Process FMEA - PFMEA):

- FMECA and DFMEA are used to analyze product designs before they are released to production. It focuses on potential failure modes associated with the functions of the product and caused by design deficiencies;
- PFMEA is used to analyze the new or existing processes. It focuses on the potential failure modes associated with process safety / effectiveness / efficiency, and problems with the functions of a product caused by the problems in the process.

The main advantage of the FMEAs is the mentioned above systematic analysis and tabular presentation. Primarily, the FMEA tables present the qualitative description of the shin: failure cause, failure mode, Local/Next level/EE.

Nevertheless the Quantitative assessment is very important for the Risk evaluation. Traditionally, in order to quantify and assess the failure mode consequence and risk, FMECA uses Criticality matrix approach presenting the Failure Mode Criticality Cm for every Failure Mode:

$$C_m = \beta \bullet \alpha \bullet \lambda \bullet p \bullet Q \bullet d \bullet t,$$

Where: β = Conditional probability of occurrence of EE assuming the given FM.,
α = Failure mode ratio,
λp = Part failure rate,
t = Duration of applicable mission phase,
d = duty Cycle,
Q = Quantity.

The only drawback of this approach is lack of Severity contribution to the FM Criticality **quantitative** evaluation.

FMECA uses **tabular Criticality Presentation** – Criticality Matrix (see Fig. 2):

Criticality	**Criticality No. Thresholds**	**Severity**			
		IV	**III**	**II**	**I**
A – Frequent	21497.0*E-9				
B – Reasonably Probable	10748.5*E-9				
C – Occasional	1074.8*E-9				
D – Remote	107.5*E-9				
E – Extremely unlikely					
Total					

Fig. 2 Criticality Matrix with restricted zone (in red)

Overcoming this disadvantage, the Automotive FMEA [9] team ranks the Severity (S) of the failure, the probability of its Occurrence (O) and the probability of detecting the failure cause or mode, i.e. Detectability (D).

Risk assessment is determined via RPN (Risk Priority Number), which is calculated by multiplying the ranking values of Severity, Occurrence and Detectability and obtaining one categorization number for each possible cause of each failure using the following equation:

$$RPN = O \bullet S \bullet D.$$

Once all items under consideration have been analyzed and the estimated RPN values assigned, corrective actions can be planned for the RPN values in descending order.

The ultimate goal of a corrective action is to achieve an appropriate reduction in the severity, occurrence and/or detection rankings in order to obtain "acceptable" RPNs.

Is Ranking Procedure so clear and simple?

The answer is: “No”!

There is a Pitfall in Use of Irrelevant Statistics [Bluvband FA of FMEA]. After the failure effects have been identified, Severity (S), Occurrence (O) and Detectability (D) should be evaluated. One possible method is the use of the conventional ranking procedure to rank these risk components on a ‘1’ (Best Case) to ‘10’ (Worst Case) ordinal scale that appears on standard FMEA forms [9].

A comprehensive FMEA team discussion on a specific item can result in a wide spread of ranks raising the question of how to resolve this situation.

Drop Outliers? Calculate average rank? Define as highest rank (Worst Case Approach)?

Conventional FMEA does not provide any guidelines for this eventuality. Typically, such problems are resolved by applying the arithmetic mean value.

In some cases more sophisticated specialists calculate the standard deviation of the proposed values and then, using Normal distribution approximation, apply all kinds of statistical sensitivity analyses. This is a mistake!

The RPN components are evaluated on the **Ordinal Scale**. This scale uses so-called Non-Parametric Statistics! Such measures as mean, standard deviation, etc. are absolutely irrelevant to the Ordinal Scale because the distance between ranks is meaningless.

Remedy. The following is a short list of proven guidelines that could be useful for FMEA teams:

- Team members could decide not to participate in the ranking of a given item or given component due to lack of relevant knowledge or experience
- A wide rank spread indicates some problem (usually due to the heterogeneity of the team). Nonetheless, we always try to obtain consensus. On the other hand, zero difference of ranks could indicate total indifference by team members towards the item under discussion.
- Outliers should be considered. Maybe they represent true estimates proposed by “process experts”! Maybe these outliers are the result of some misunderstanding or irrelevant experience!
- Either the Median or Mode (certainly not the Mean!) should be used as the team’s rank estimate!

Remark. Actually, even the RPN calculation obtained by multiplying the Ordinal Scale values (1) is a kind of pitfall, which is, unfortunately, regulated by the Automotive Industry Action Group (AIAG) Standards [9]! As a result, this case needs to be dealt as well. The situation can be improved by using some alternative scales, considering RPN as an illustration of the Pareto Priority Index PPI [1]. For example, one could use 'Rational Scales' for RPN components evaluation, such as Failure Rate for Occurrence, Probability of misdetection for Detectability and the Failure Cost for Severity.

1.2 PPA (Potential problem analysis)

There is an opinion [Greg] that the Detection component of the RPN is redundant.

A **Potential Problem Analysis** is a systematic process very similar to FMEA for uncovering and dealing with potential problems that are reasonably likely to occur. This approach also uses criticality analysis (**dropping RPN's use of detectability** as a primary driver in the assessment of risk: it is considered to be useful as a follow-on mitigating methodology (at the product and process levels) to be applied only after the possibility of an initial engineering elimination of the failure mode and the reduction of severity at the level of the specification of the requirements and design of the system have failed).

On the one hand right: FFF Detection (followed by FFF Isolation and Repair) is usually considered important for Maintainability and Logistics only, but on the other hand: **Timely Detection** of the FFF (just before irreversible happens) gives the operator (or the automated system) timely to change the mission or the operation conditions in order to succeed without or with **much lower** Risk, even if Severity and Occurrence are high! For example, it is well known that a "brake fluid leak" leads to brake failure (catastrophic). Ignoring the Detection component, the Risk of "brake lines damage" (leading to low brake fluid level and then to brake failure) will be assessed equally for a system with and without an indicator of brake fluid level (not distinguishing whether the fault is visible or not to the driver). Such detection prevents the drive (which will be interrupted anyway by a catastrophe) and therefore prevents the Catastrophic failure, lowing the Risk. Nevertheless, for the "Reliability" FMEA (see also in this paper the para 2.2) does not meter if the failure mode is detectable or latent, will detection be incorporated or not) the mission will not be accomplished and **from Reliability point of view one may omit the detection D** as a component in the RPN: sooner or later the system will stop …

1.3 COMPLETENESS OF THE ANALYSIS

Is FMEA the ideal tool for FA being systematic, exhaustive and all inclusive?

How can we assure the thoroughness of the failure modes in the analysis?

The pitfall in Failure Modes Identification is obvious: **Missing Failure Modes**.

Indeed, the first step of the FMEA 'Step by Step' procedure is compiling a list of system/process functions or system equipment items and identifying the failure modes of each item.

One of the main problems besetting the FMEA process is the omission of Failure Modes because the brainstorming session is not sufficiently comprehensive.

One of the causes of this problem is inherent in the well-known classical definition of failure: "The inability of an item, product or service to perform required functions on demand due to one or more defects" [11].

Unfortunately, this definition is too narrow and, therefore, does not cover all possible aspects of failure analysis.

Remedy. Paper [10] proposes a checklist of 10 types of Failures Modes that can be utilized by the FMEA team as a basis for defining the customized list of failures associated with any given activity or item.

This check list is based on the Key Question "What Can Go Wrong?":

1. The intended function (mission) is not performed.
2. The intended function (mission) is performed, but there is some safety problem or a problem in meeting a regulation requirement (for example, ecological) associated with the intended function (mission) performance.
3. The intended function (mission) is performed, but at a wrong time (availability problems).
4. The intended function (mission) is performed, but at a wrong place.
5. The intended function (mission) is performed, but in a wrong way (efficiency problems).
6. The intended function (mission) is performed, but the performance level is lower than planned.
7. The intended function (mission) is performed, but its cost is higher than planned (unscheduled maintenance or repair, higher consumption of required resources, etc.).
8. An unintended (unplanned) and (or) undesirable function (mission) is performed.
9. Period of intended function (mission) performance (life time) is lower than planned (reliability problem).
10. Support for intended function (mission) performance is impossible or problematic (maintenance, repairability, serviceability problems).

1.4 COMPLEMENTARY APPROACH

To ensure the completeness of the analysis, the above 10 rules are not enough: after completing the bottom-up (inductive) FMEA, one should accomplish the analysis with a top-down (deductive) approach.

The most simplified and well-known tool for **deductive** RFA is Cause-Effect Diagram (CED) Fishbone Diagram (Ishikawa, 1950), used for the systematical analysis of possible FC.

Looking on CED, one can see that this analysis is just particular case of the most comprehensive, graphical deductive tool Fault Tree Analysis (FTA): “FTA with OR-gates only”.

The main advantages of CED vs FTA is Simplicity (appropriate for line workers) and Order in focusing on possible FC direction: MMMMME (Man-Method-Material-Measurement-Machine-Environment)…

But the CED, like the FMEA, does not consider combinations of events. Therefore,

trying to accomplish the analysis, one should take the advantage of the most powerful deductive RFA instrument which is, no doubts, FTA (see Fig.4).

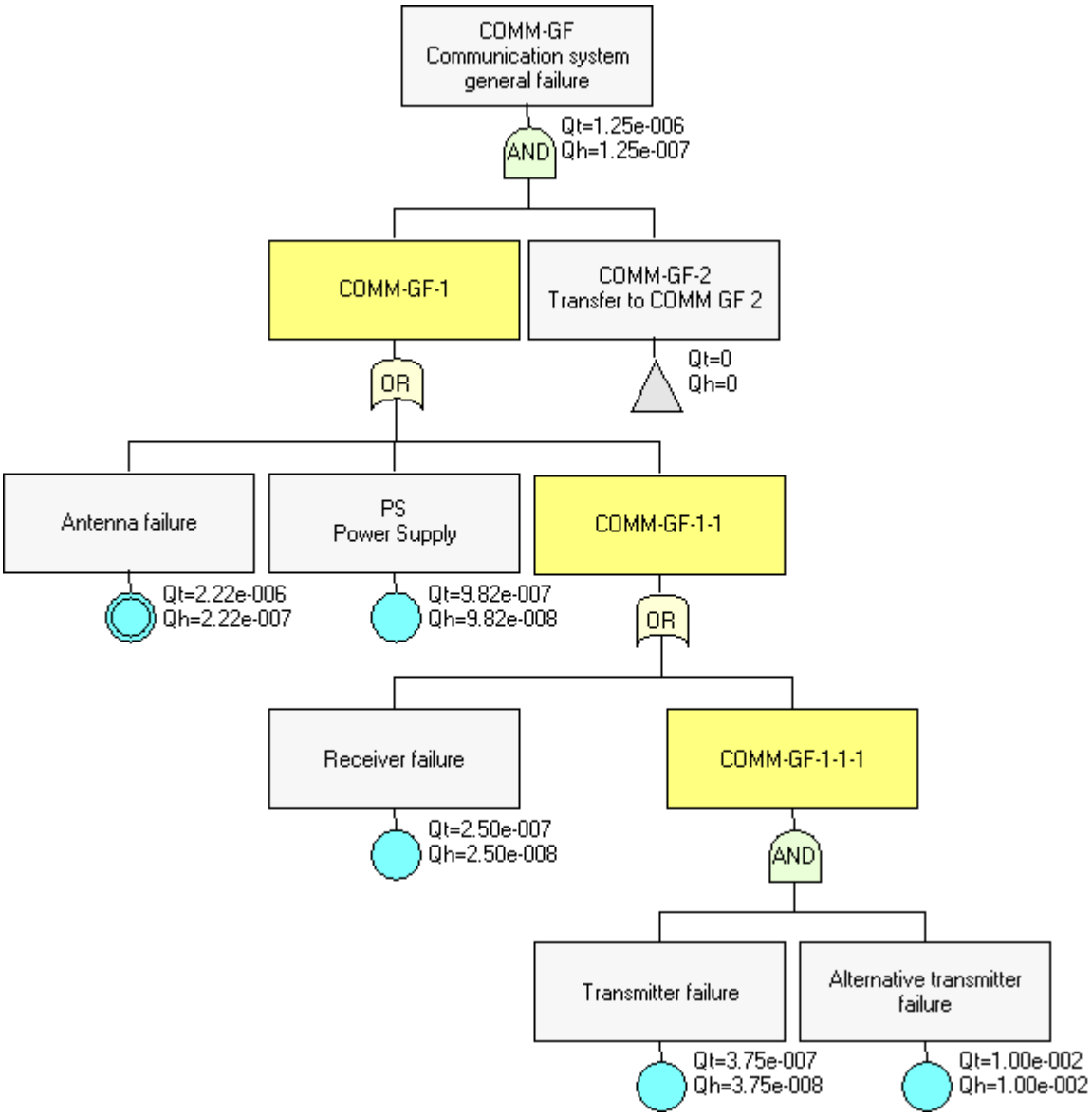


Fig.3

By taking into account combinations of failures, FTA avoids the obvious shortcomings of FMEA. However, being heavily dependent on personal experience and knowledge, even "fine art" of a performer-analyst, FTA has a tendency to miss some of failure modes (FM) or FM combinations.

Fig. 4 presents four main attributes which are actually the four main differences between the FMEA and FTA.

	Attribute	**FMEA**	**FTA**
1.	Boundaries of the analysis	Single point failures	Combinations of failures
2.	Direction of analysis	Bottom-Up	Top-Down
3.	Predefined indenture levels	Product/Process tree is a "skeleton" of a bottom-up	Structure/Skeleton is not predefined, just a logic

	Attribute	FMEA	FTA
		structure	tree as a framework
4.	Presentation of the analysis process and results	Tabular	Graphical

Fig. 4 FMEA and FTA four main differences

1.5 BOUNCING FA and MODEL-BASED FA

Paper [14] suggests Bouncing Failure Analysis (BFA) and implies the usage of the combination of tabular analysis (FMEA-style) and graphical analysis (FTA-style). Both types of analyses require the deep understanding of the System/Process Under Analysis (SUA) behavior: System End Effects and Failure Modes. Such understanding is essential for decomposition of the system and compilation of complete End Effects and Failure Modes lists/libraries where each FM or combination of FMs causes one or more End Effects. The way to define the End Effects list is to investigate the SUA functional requirements, i.e. "What the system is required to do" (F1, F2 … Fj), as well as SUA safety requirements, i.e. "What the system is required not to do" (Fj+1, …, Fk). For example, for a communication system with functions: F1=Receiving, F2=Transmitting, …, Fk = Dangerous level of radiation. The function F1 will have the following End Effects: EE11=No Signal, EE12=Signal Distortion, EE13=Noisy Signal, etc. Therefore, setting up the End Effects list is the first important step of the BFA procedure.

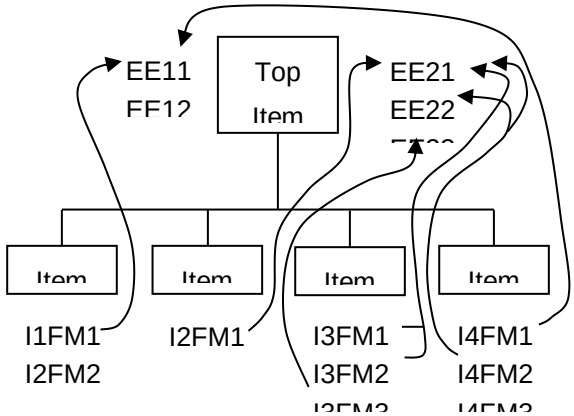


Fig. 4a EEs vs FMs

Following is the step-by-step description of the BFA methodology.

1. Define all possible End Effects (EE), i.e. the effects at the top system level. In most cases the EE list can be derived from the list of the functional requirements for the System Under Analysis (SUA). In our example "Function 1" has two possible End Effects: EE11 and EE12.
2. Assign the appropriate Severity to each EE, subject to the SUA improper operation consequences.

3. Define all possible failure modes on the bottom level. Failure modes for the bottom (component) level are usually well known and can be found in the existing failure modes databases (see Fig. 4a), i.e. “Item 3” has three Failure Modes: I3FM1, I3FM2, and I3FM3.
4. Use the single-point FMEA as a basis for the failure analysis of a higher order: double-point failures, triple-point failures, n-point failures.
5. Look for double, triple, etc. combinations of failures building Interaction Matrices (see [14] example on Fig. 4b).

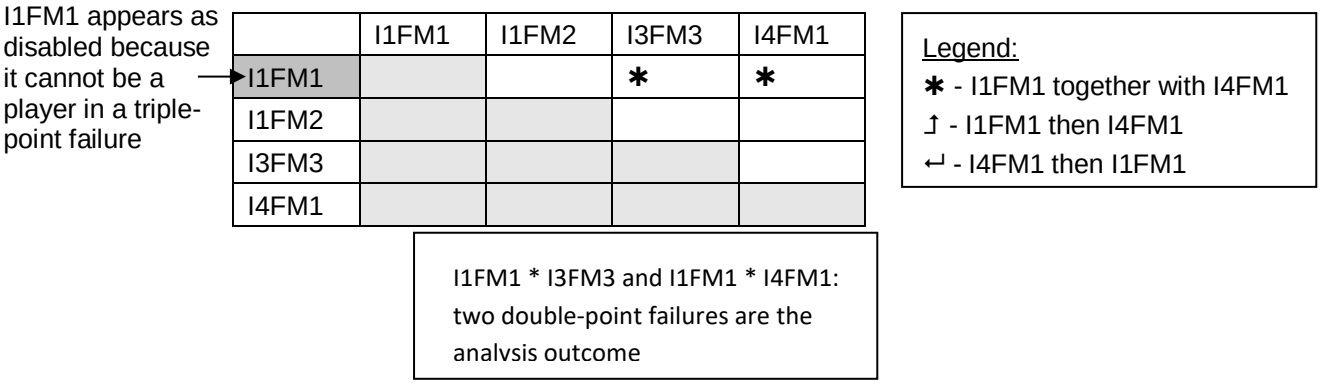


Fig. 4b Shortened Interaction Matrix: Double-Point Failure

Selection of FMs in the matrix is accompanied by an additional background process - all FMs that cannot be a part of the triple-point failure will be disabled automatically.

Then one should continue to the triple-point failure investigation by drilling down to the desired failure mode, enabled in the double-point matrix. Our investigation results in the selection of a failure mode together with its operator (can be “*” or “↥”) and creation of a shortened matrix. Applying the same technique used for the double-point failures, we select a cell of the matrix that will now present a triple-point failure. (See Fig. 4b).

Generally, both FMEA and FTA include many elements of intuition and subjective engineering judgment.

When a major risk issue, such as safety of a commercial aircraft or of a nuclear power plant, is discussed, there is a natural desire to eliminate human errors in the analysis to the most possible extent and to make it as "automatic" and "fool proof" as possible.

This is the main motivation for the approach of Model Based Safety Analysis (MBSA) [13] – the approach which has been introduced about 10 years ago, but hasn't yet gain global popularity and has not yet received recognition for formal tasks, such as certification of commercial aircraft.

The main idea behind MBSA is “**precise model of a system behavior**, **both in normal and given FFF mode of operation**. On basis of such a model additional automatic tools will be able to perform safety analysis, providing all desired outputs, such as probability of a failure, combinations of events leading to failure etc. This step of analysis can be totally automated, without any need in human interpretation of the model or data processing "by hand". Thus, if the model is precise, the outputs of safety analysis shall be complete, consistent, error free and independent of any individual perception of the factors involved.

System level Failure can occur due to failures of components (system Fault), incorrect outputs, corrupted messages, or improper functioning of software in the absence of failures. A fault model captures information about the various ways in which the components of the system (both the digital controller and the mechanical system) can malfunction. It defines the behavior of common failure modes, such as non-deterministic, inverted, stuck-at, etc. The fault model also specifies the fault triggers that activate the component failures and their duration. We distinguish between transient faults (those that last for a short period of time) and permanent faults (those that last forever). The fault model can also specify more complex fault behaviors, such as fault propagations, dependent faults, etc. It can also specify fault hierarchies, in which the user can define the failure mode of a component as a function of its subcomponents or as an abstraction of the underlying fault behavior.

Depending on the system model, we can chose to model different types of digital faults, mechanical faults, timing faults, etc. The digital faults are those that relate to the digital component of the system - both hardware and software. For example, a digital fault could be inverting an output on a hardware chip. One would also like to be able to describe situations in which software fails to perform as expected (i.e. software faults) but it is still unclear how such faults can be described and modeled. Some software faults can be simulated by introducing failure modes on outputs, such as an inverted or non-deterministic, etc., but these failure modes do not closely match our intuitive notion of software faults and additional research is necessary to further explore this issue.

Mechanical faults are those that occur in the mechanical components of the system outside the digital controller. These are entirely dependent on the environment of the system in question, and could include electrical or hydraulic problems, network upsets, communications failures, and a variety of other kinds of problems.

Another useful step on the way to MBSA is the concept of "Full Integration of FTA".

At present, Fault Tree Analysis for an Aircraft is usually conducted on the level of a separate system, not integrated at the entire Aircraft level. Certainly, this approach does not represent physical reality of the aircraft, because there is considerable interdependence between the systems. The source of interdependence can be supply of energy (electrical or hydraulic), signals etc. Thus, Fault Trees for the systems of an aircraft, necessarily include "external events", which in a fact represent events which happen in another system. In practice, these "external events" are usually processed manually or semi-manually, and this highly increases risk of mistakes in the processing of the Fault Trees.

Main sources of the mistakes are:

1. Since "external events" are usually represented as very simple models (single event, without the underlying Fault Tree), after any change in the input data (failure rates, operation profile etc.), Fault Trees must be manually recalculated. Since there is no automatic mechanism of searching for all the trees that require recalculation, mistakes are common.
2. For the same reason, internal mutual dependence or even common basic events in the trees, describing internal and external events, can be missed. This can lead to severe errors in calculation of hazard probabilities.
3. In many cases, a safety engineer is working on integrated Aircraft level and analyses the Fault tree maximum on the LRU level.

In order to overcome these obstacles and make Fault Tree Analysis of the systems much more robust, the principle of Full “System of Systems” Integration has been employed in the advanced analysis tools, like ALD Safety Commander. It means that the data bases

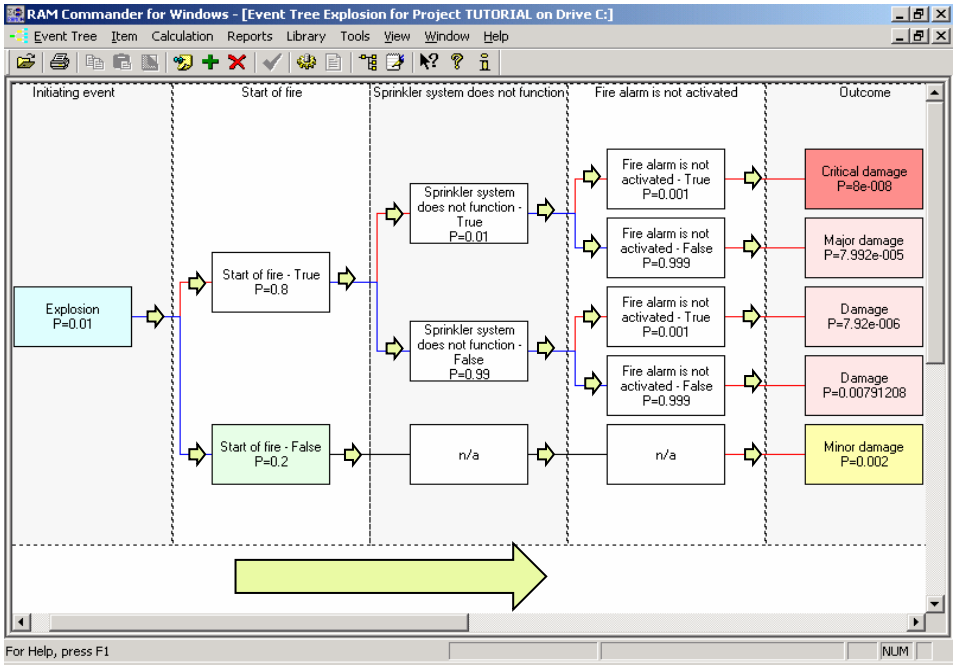
for all systems of the aircraft are fully integrated, and this makes possible detailed and risk-free FTA for all aircraft systems and for the whole Aircraft. Full System Integration can be seen as an important step to creation of a comprehensive model of system logic, which will serve a basis for Model Based Safety Analysis.

1.6 Dynamic types of analysis: ETA and DFTA

Event Tree Analysis

Event Trees are one of the most widely used methods in system risk analysis. It is an inductive failure analysis performed to determine the consequences of single failure for the overall system risk or reliability. ETA uses similar logic and mathematics as Fault Tree Analysis, but the approach is different FTA uses deductive approach and ETA uses the inductive approach (from basic failure to it's consequences).

An Event Tree itself is a visual representation of single failure sequences, **limited to the effects of the initiating event.**



Dynamic fault tree with a plurality of aircraft items' failure conditions and may include both static gates and dynamic gates (AND, OR, "K out of N", PAND, SEQ, SPARE, etc.), items with failure times distributed normal, log-normal, exponentially, Weibull, etc.

For safety catastrophic events the case of a rare-event estimation is very often, then the importance sampling method may be applicable [15]. The most essential problem in this method is how to select an appropriate reference probability distribution. Unfortunately, well-known approaches for reference distribution selection (scaling, translation) are not applicable for dynamic fault trees analysis. So the methodology described in the patent [15] is the solution for this important FA case.

2 Standpoints of the Events.

2.1 Perspectives for assessing opportunities for potential failure

FA should distinguish three different perspectives for assessing the opportunities for potential failures:

- **System level failure** must be analyzed **"outside-in"** using a customer's perspective of symptoms, failure modes, and the potential causes.
  From the FFF perspective, user as a rule experiences the System Level Failures only - as EE of the System. Flaws and Faults are the part of potential cause assessments.
- **Process level failure** must be analyzed **"inside-out"** using work process detail to establish a perspective of symptoms, failure modes, and potential causes.
  In the automotive industry [9], the Potential Failure Mode is defined as the manner in which the process could potentially fail to meet the process requirements and/or design intent.
- **Product/Design level failure** must be analyzed **"end-to-end"** across the full process using the production cycle from delivery of the initial raw material through installed application doing the job that that the customer requires in order to establish a perspective of symptoms, failure modes, and potential causes.
- The analyst must understand what perspective is under investigation!

2.2 End Effect Impact Point of view

During Risk and FA, it is very important what type of risks the investigator is interesting in.

Just let's consider the two basic characteristics of a System: Reliability and Safety [1]

Engineers routinely assume that the more reliable a system is, the safer it is, and vice versa. This assumption is sometimes somewhat erroneous and sometimes very erroneous and leads to a lot of confusion in systems failure analysis. Actually, it is often true that the safer the system, the less reliable it is.

Consider an elevator: The maximum level of safety provides an inoperative elevator — its doors won't shut on you or your dog; pressing buttons won't cause anything unsafe to happen. Enter the inoperative elevator, stay inside as long as you wish, exit it — you are 100% safe. What about reliability? As the inoperative elevator is functionally ineffective, it's absolutely unreliable in getting you up and down to different floors of the building— its reliability is zero.

To improve the safety of a reliable (moving) elevator, designers add elements and controls that limit the probability of its adequate operation. For example, they may add a sensor that indicates proper door closure. If the sensor is out of order, the elevator won't move: reliability decreases while safety improves.

This trivial example demonstrates that in some cases there is an apparent contradiction between safety and reliability.

Those who performed FMEA for complicated systems know that the Critical EE from Reliability point of view (and as a consequence its Failure Cause), maybe negligible from point of view of Safety! Moreover, Failure Modes negligible from Safety and Reliability may be Critical from Security point of view [17] S vs S (Dov)

The referenced paper [3] Bluvband, Friedman "FMECA-what about the `quality assurance' task? " shows very clearly that FMECA should be performed additionally for Production Quality assessing influence of the Failure Modes and Preventive actions in manufacturing process (in addition to field usage Reliability and Safety considerations).

For example, usual practice [AIAG, MIL-STD-169, etc.] if to define a

Catastrophic failure as “A failure which may cause death or system loss (e. g., aircraft, launching system, mission control)“.

Critical failure as "Failures that may cause severe injury, major property damage or system damage that will result in loss of the intended mission"

Major failure as “A failure which may cause (1) minor injury, minor property damage, or minor system damage that will result in delay, (2) loss of availability of asset, (3) loss of mission operating margin without significant degradation in a probability of mission success”.

From Reliability point of view, for a new system developed with substantial investment in order to increase its Reliability, “loss of intended mission” may be defined as “Catastrophic” (actually may concur with the previous definition if some of the Managers will be fired – i.e. will be **lost** for the organization), see also para 1.2 .

Same logic was applied when in the relatively new standard [8] the LSA FMEA is introduced and actually required. The fact that different failure modes may cause the same maintenance activities brings us to the idea to group such failure modes in direction to the Logistic FMEA.

Logistic FMEA main purposes are:

- Systematic identification of maintenance tasks (from intrinsic failures of the equipment)
- Identification and analysis of
  - Failure detection means,
  - Localization means,
- Requirements for Troubleshooting procedures

The LSA FMEA is generally coincident with, but not identical to, the Design-oriented or the Process-oriented FMECA. The main difference between Design FMECA and LSA FMEA is that different failure modes from a design perspective can be grouped in the same failure mode for LSA FMEA because they lead to the same maintenance action. Other maintainability, maintenance or safety analyses use data from LSA FMEA or derived from FMECA, e.g., Level of Repair Analysis (LORA), Reliability-Centered Maintenance (RCM) and Scheduled Maintenance Analysis (SMA). In order to take full benefit of existing works and to avoid useless duplication of works, these other activities must be tightly interfaced and coordinated with FMECA and LSA FMEA.

3 CONCLUSIONS

1. FA should be performed not "generally", but in accordance with the type of Risk i.e. understanding what perspective is under investigation (Safety, Reliability, Quality, ILS, Security, Business, etc.).
2. Risk assessment should be done in accordance with the EE impact point of view, for every type of Risk, and given several risk types, then harmonized for Decision Making.
3. The analyst should use and choose the advanced proven and new methods and models to achieve high-level of completeness, visibility and correctness of the FA.

4 References

1. Bluvband Z., Quality's Greatest Hits: Classic Wisdom from the Leaders of Quality, ASQ Quality Press, 2002
2. Kume H., Statistical Methods for Quality Improvement, Productivity Press, 1987.
3. Bluvband Z., Friedman A., "FMECA-what about the `quality assurance' task?" Reliability and Maintainability Symposium, 1989, Proceedings.
4. IEEE Standard Classification for Software Anomalies, 1044-1993, 1994.
5. BSI, BS 4778-3.2, 1991 BS 4778-3.2:1991, IEC 60050-191:1990, Quality vocabulary. Availability, reliability and maintainability terms. Glossary of international terms.
6. IEEE-Std-610.12-1990-IEEEStandardGlossaryofSoftwareEngineering Terminology
7. ISO 31000:2009, Risk management -- Principles and guidelines
8. AIA/ASD S3000L, Logistic Support Analysis (LSA), ASD, 2014
9. Automotive Industry Action Group (AIAG) Standards
10. Bluvband Z., Grabov P,“ Failure Analysis of FMEA”, RAMS, 2009
11. Quality Glossary, ASQ, http://asq.org/glossary/f.html
12. Ishikawa, Kaoru, Introduction to Quality Control. J. H. Loftus (trans.). Tokyo: 3A Corporation,1990
13. Anjali Joshi. Mike Whalen. Mats P.E. Heimdahl, Model-Based Safety Analysis, Final Report, NASA, 2006
14. Bluvband Z., Polak R., Grabov P., Bouncing Failure Analysis (BFA). The Unified FTA-FMEA Methodology, RAMS, 2005
15. Bluvband Z., Porotsky S., Methods, apparatus and systems for performing dynamic fault tree analysis, US Patent US8832497 B2.
16. MIL-STD-1629, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, U.S. Department of Defense. 1979
17. Shirtz D., Bluvband Z., Elovici Y., Shoval P., Computer Systems & Information SSR: a Unified Approach to Decision Making, RAMS, 2007
18. Bluvband Z., Grabov P., Nakar O., Expanded FMEA (EFMEA), RAMS, 2003.
19. PFMEA, RAM Commander RAMC 7.2 New Features, *ALD WEB Site*, www.aldservice.com
20. Jeff A. Estefan, Survey of Model-Based Systems Engineering (MBSE), INCOSE MBSE Focus Group, May 25, 2007