FMEA and FTA

Vít Hampl

FMEA - Failure mode and effects analysis

FMEA is a bottom-up technique used to identify, prioritize, and eliminate potential failures from the system, design or process before they reach the customer.

History

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.

Types

There are several types of FMEA according to the stage in which they are used:
Concept FMEA, which is used to analyze concepts in the early stages
before hardware is defined. It focuses on potential failure modes associated with the proposed functions of a concept proposal. This type includes the interaction of multiple systems and interaction between the elements of a system at the concept stages. CFMEA helps select the optimum concept alternatives, or determine changes to design specifications, identifies potential failure modes caused by interactions within the concept, increases the likelihood all potential effects of a proposed concept's failure modes are considered. It also identifies system level testing requirements and helps determine if hardware system redundancy may be required within a design proposal
Design FMEA, which is used to analyze products before they are released to production. It focuses on potential failure modes of products caused by design deficiencies. DFMEAs are normally done at three levels – system, subsystem, and component levels. This type of FMEA is used to analyze hardware, functions or a combination. DFMEA aids in the objective evaluation of design requirements and design alternatives, in the initial design for manufacturing and assembly requirements. It increases the probability that potential failure modes and their effects have been considered in the design/development process, provides additional information to help plan thorough and efficient test programs. Develops a list of potential failure modes ranked according to their effect on the customer. It also establishes a priority system for design improvements, provides an open issue format for recommending and tracking risk reducing actions and future reference to aid in analyzing field concerns.
Process FMEA, which is normally used to analyze manufacturing and assembly processes at the system, subsystem or component levels. This type of FMEA focuses on potential

failure modes of the process that are caused by manufacturing or assembly process deficiencies. PFMEA identifies potential product related process failure modes. assesses the potential customer effects of the failures, identifies the potential manufacturing or assembly process causes and identifies process variables on which to focus controls or monitoring. It develops a ranked list of potential failure modes, establishing a priority system for corrective action considerations, documents the results of the manufacturing or assembly process and identifies process deficiencies. It also identifies confirmed critical characteristics and/or significant characteristics and operator safety concerns. PFMEA feeds information on design changes required and manufacturing feasibility back to the designers.

Service FMEA, which is used to analyze services and their design. Analyzes service industry processes before they are released to impact the customer.

Software FMEA, which is used to analyze software products. This type of FMEA is used to analyze software in combination with hardware.

Usage of FMEA

FMEA should be used in these situations:

- When a process, product or service is being designed or redesigned, and after quality function deployment.
- When an existing process, product or service is being applied in a new way.
- Before developing control plans for a new or modified process.
- When improvement goals are planned for an existing process, product or service.
- When analyzing failures of an existing process, product or service.
- Periodically throughout the life of the process, product or service

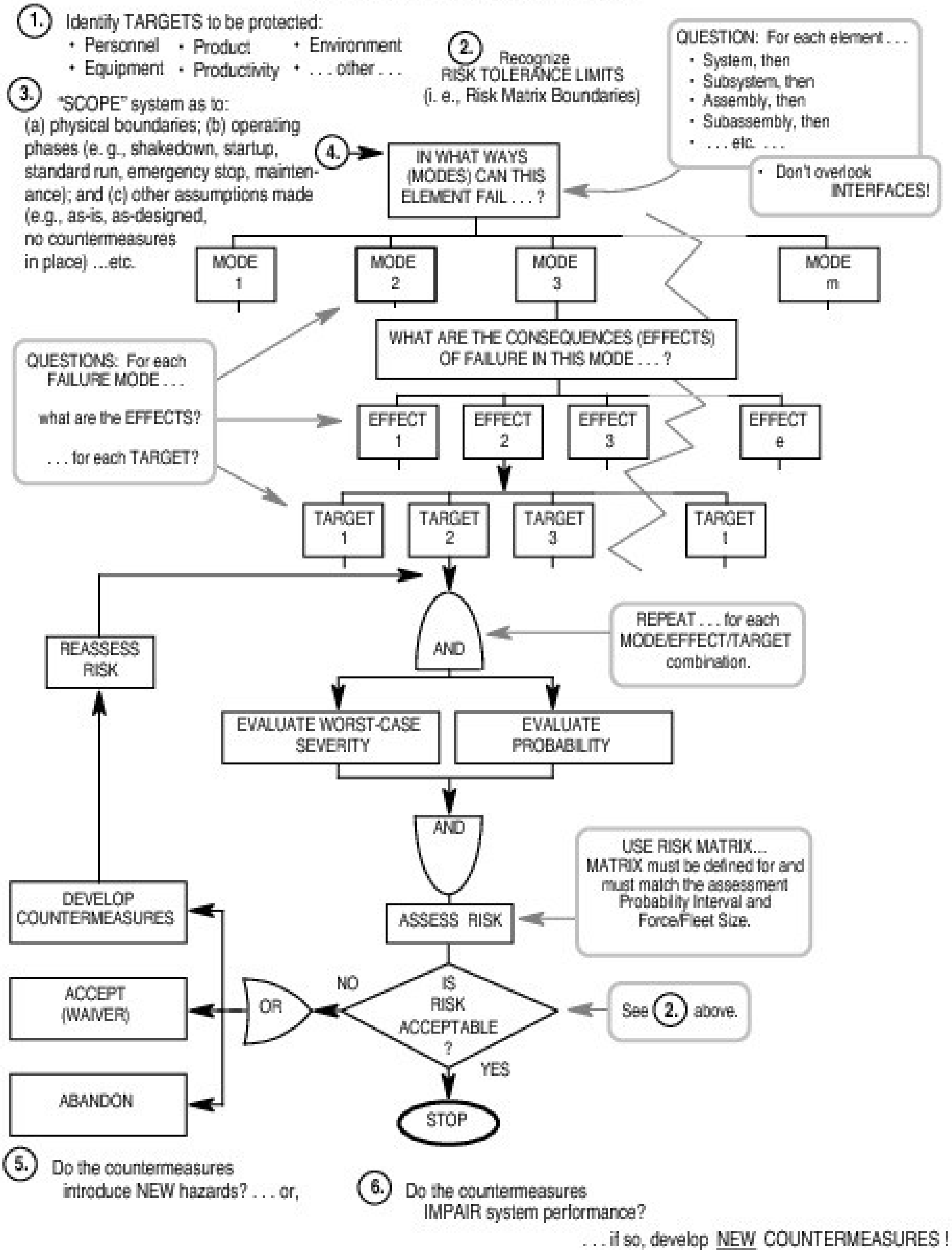
FMEA should be used to identify:

- critical or hazardous conditions.
- potential failure modes
- need for fault detection.
- effects of the failures.

In long term view, FMEA:

- aids in producing block-diagram reliability analysis
- aids in producing diagnostic charts for repair purposes and maintenance handbooks.
- is used to design a built-in test (BIT), failure detection & redundancy.
- helps in analysis of testability.
- is used for retention as formal records of the safety and reliability analysis, which are to be used as evidence in product safety law-suit.

FMEA Process Flow



1. Identify TARGETS to be protected:
- Personnel
- Product
- Environment
- Equipment
- Productivity
- . . . other . . .

2. Recognize RISK TOLERANCE LIMITS (i. e., Risk Matrix Boundaries)

3. "SCOPE" system as to: (a) physical boundaries; (b) operating phases (e. g., shakedown, startup, standard run, emergency stop, maintenance); and (c) other assumptions made (e.g., as-is, as-designed, no countermeasures in place) ...etc.

4.

QUESTION: For each element . . .
- System, then
- Subsystem, then
- Assembly, then
- Subassembly, then
- . . . etc. . . .

- Don't overlook INTERFACES!

QUESTIONS: For each FAILURE MODE . . .

what are the EFFECTS?

. . . for each TARGET?

REPEAT . . . for each MODE/EFFECT/TARGET combination.

USE RISK MATRIX... MATRIX must be defined for and must match the assessment Probability Interval and Force/Fleet Size.

See 2. above.

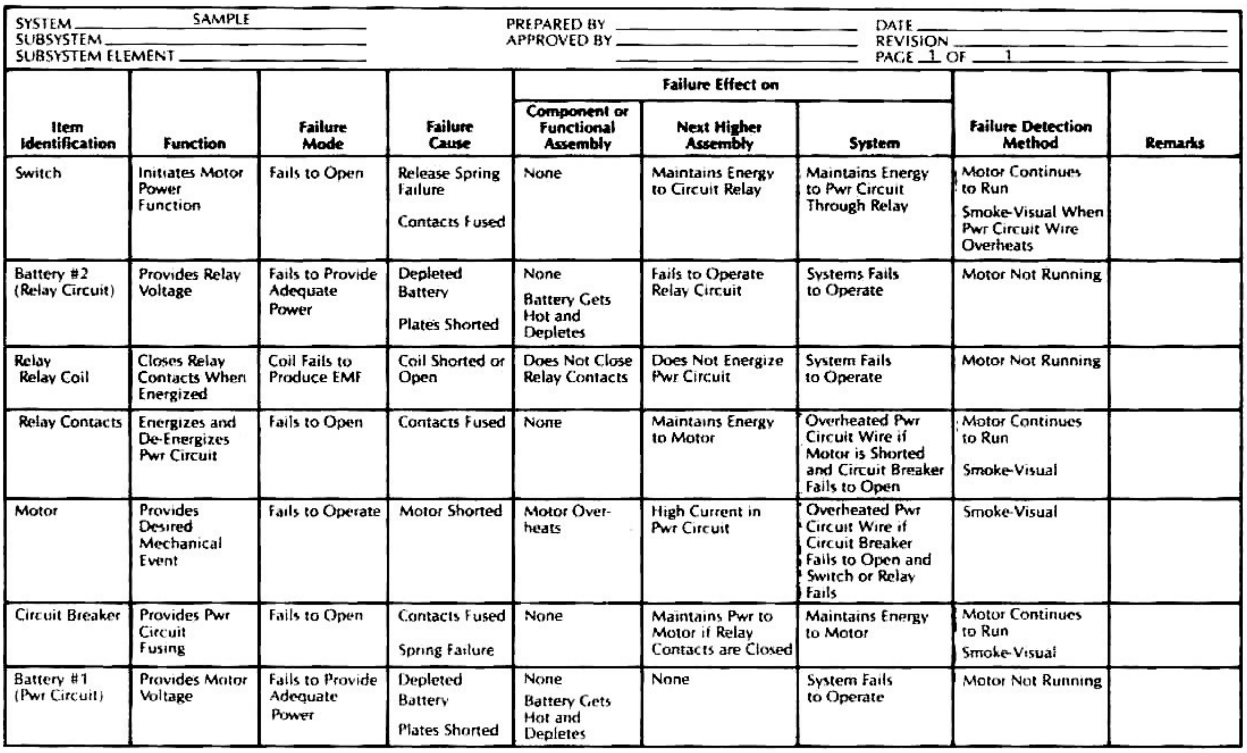
5. Do the countermeasures introduce NEW hazards? . . . or,

6. Do the countermeasures IMPAIR system performance?

. . . if so, develop NEW COUNTERMEASURES !

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.



SYSTEM SAMPLE
SUBSYSTEM
SUBSYSTEM ELEMENT

PREPARED BY
APPROVED BY

DATE
REVISION
PAGE 1 OF 1

Item Identification	Function	Failure Mode	Failure Cause	Failure Effect on			Failure Detection Method	Remarks
				Component or Functional Assembly	Next Higher Assembly	System		
Switch	Initiates Motor Power Function	Fails to Open	Release Spring Failure Contacts Fused	None	Maintains Energy to Circuit Relay	Maintains Energy to Pwr Circuit Through Relay	Motor Continues to Run Smoke-Visual When Pwr Circuit Wire Overheats	
Battery #2 (Relay Circuit)	Provides Relay Voltage	Fails to Provide Adequate Power	Depleted Battery Plates Shorted	None Battery Gets Hot and Depletes	Fails to Operate Relay Circuit	Systems Fails to Operate	Motor Not Running	
Relay Relay Coil	Closes Relay Contacts When Energized	Coil Fails to Produce EMF	Coil Shorted or Open	Does Not Close Relay Contacts	Does Not Energize Pwr Circuit	System Fails to Operate	Motor Not Running	
Relay Contacts	Energizes and De-Energizes Pwr Circuit	Fails to Open	Contacts Fused	None	Maintains Energy to Motor	Overheated Pwr Circuit Wire if Motor is Shorted and Circuit Breaker Fails to Open	Motor Continues to Run Smoke-Visual	
Motor	Provides Desired Mechanical Event	Fails to Operate	Motor Shorted	Motor Over-heats	High Current in Pwr Circuit	Overheated Pwr Circuit Wire if Circuit Breaker Fails to Open and Switch or Relay Fails	Smoke-Visual	
Circuit Breaker	Provides Pwr Circuit Fusing	Fails to Open	Contacts Fused Spring Failure	None	Maintains Pwr to Motor if Relay Contacts are Closed	Maintains Energy to Motor	Motor Continues to Run Smoke-Visual	
Battery #1 (Pwr Circuit)	Provides Motor Voltage	Fails to Provide Adequate Power	Depleted Battery Plates Shorted	None Battery Gets Hot and Depletes	None	System Fails to Operate	Motor Not Running	

Example of filled FMEA sheet

FMEA measurements

Ease of Detection

A – Easy Immediately detected and alarmed

B – Limited Detected with delay or needs observation

C – Difficult No detection available

Frequency of Occurrence

A – Operational events More than once per year

B – Likely events 1/y ~ 10-2/y

C – Unlikely events 10-2 ~ 10-4/y

D – Extremely unlikely events Less than 10-4/y

Risk Potential

I – Normal Operational caution required

II – Danger Limited function

III – Minor hazard	Immediate halt and repair
IV – Major hazard	Accident, damage of facility
V – Extreme	Possible environmental effect

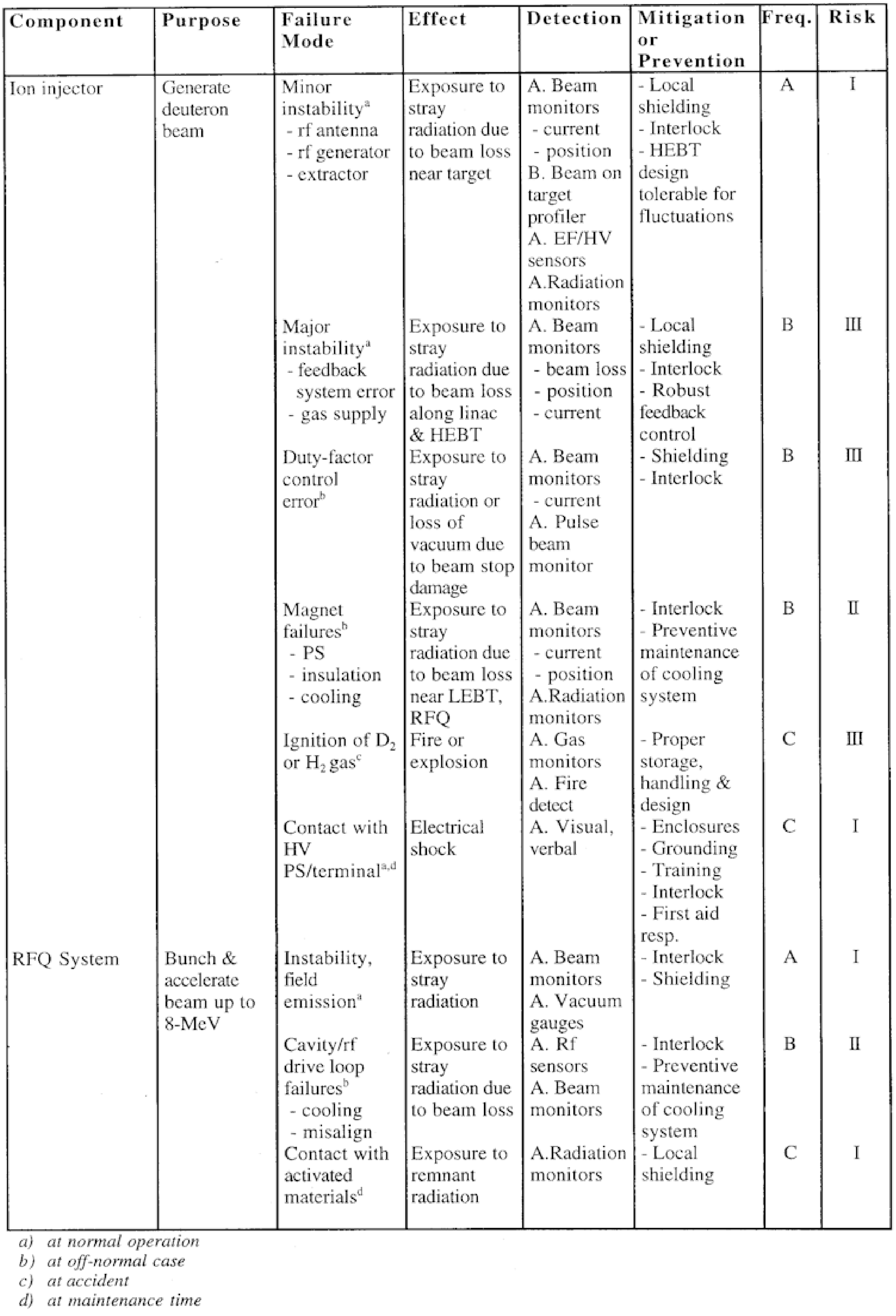
Alternative risk potential categories:

Category I - Catastrophic: A failure which may cause death or weapon system loss (i.e., aircraft, tank, missile, ship, etc...)

Category II - Critical: A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.

Category III - Marginal: A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.

Category IV - Minor: A failure not serious enough to cause injury, property damage or system damage, but which will result in unscheduled maintenance or repair.



Component	Purpose	Failure Mode	Effect	Detection	Mitigation or Prevention	Freq.	Risk
Ion injector	Generate deuteron beam	Minor instability[a] - rf antenna - rf generator - extractor	Exposure to stray radiation due to beam loss near target	A. Beam monitors - current - position B. Beam on target profiler A. EF/HV sensors A.Radiation monitors	- Local shielding - Interlock - HEBT design tolerable for fluctuations	A	I
		Major instability[a] - feedback system error - gas supply	Exposure to stray radiation due to beam loss along linac & HEBT	A. Beam monitors - beam loss - position - current	- Local shielding - Interlock - Robust feedback control	B	III
		Duty-factor control error[b]	Exposure to stray radiation or loss of vacuum due to beam stop damage	A. Beam monitors - current A. Pulse beam monitor	- Shielding - Interlock	B	III
		Magnet failures[b] - PS - insulation - cooling	Exposure to stray radiation due to beam loss near LEBT, RFQ	A. Beam monitors - current - position A.Radiation monitors	- Interlock - Preventive maintenance of cooling system	B	II
		Ignition of D_2 or H_2 gas[c]	Fire or explosion	A. Gas monitors A. Fire detect	- Proper storage, handling & design	C	III
		Contact with HV PS/terminal[a,d]	Electrical shock	A. Visual, verbal	- Enclosures - Grounding - Training - Interlock - First aid resp.	C	I
RFQ System	Bunch & accelerate beam up to 8-MeV	Instability, field emission[a]	Exposure to stray radiation	A. Beam monitors A. Vacuum gauges	- Interlock - Shielding	A	I
		Cavity/rf drive loop failures[b] - cooling - misalign	Exposure to stray radiation due to beam loss	A. Rf sensors A. Beam monitors	- Interlock - Preventive maintenance of cooling system	B	II
		Contact with activated materials[d]	Exposure to remnant radiation	A.Radiation monitors	- Local shielding	C	I

a) at normal operation
b) at off-normal case
c) at accident
d) at maintenance time

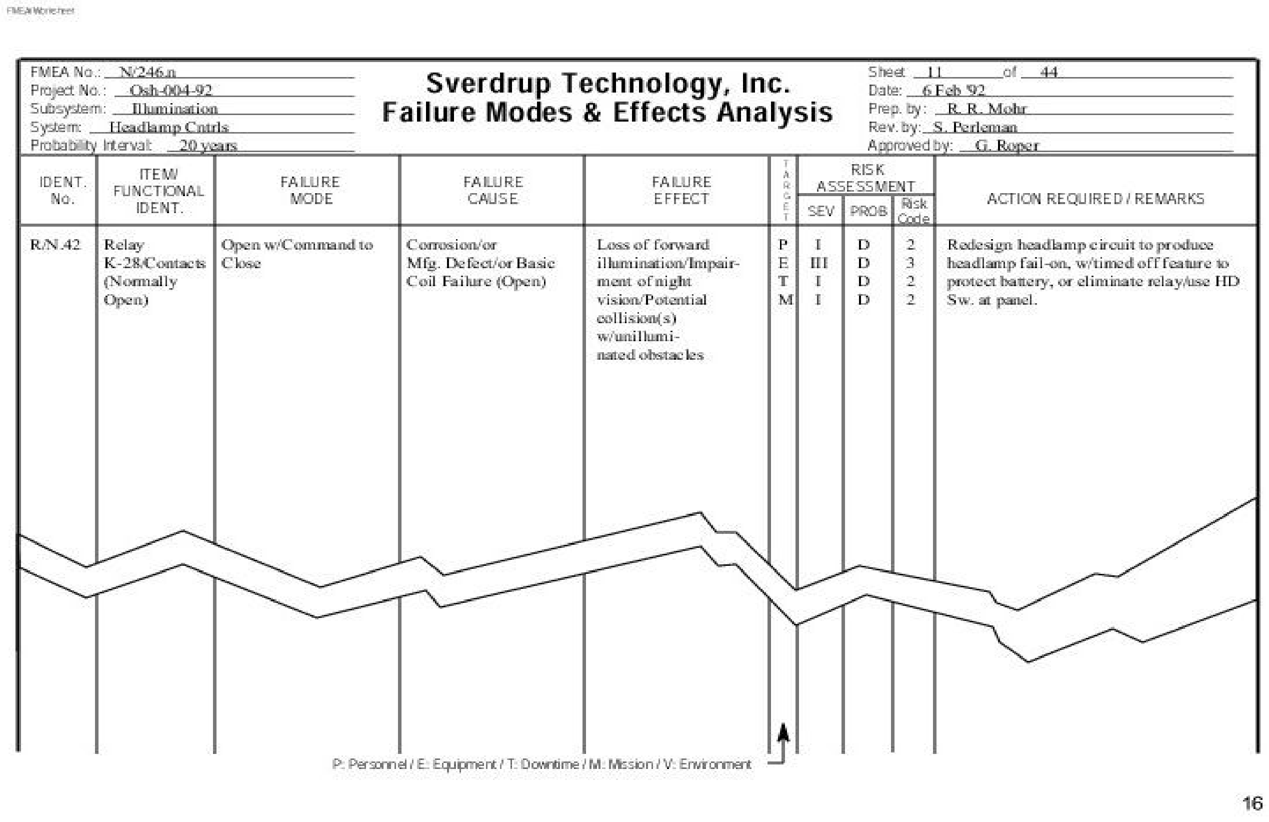
Example of FMEA worksheet with categorization

How to perform FMEA (by asq.org)

1. 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.

2. 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.)

3. 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.



FMEA Worksheet

FMEA No.: N/246.n
Project No.: Osh-004-92
Subsystem: Illumination
System: Headlamp Cntrls
Probability Interval: 20 years

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis

Sheet 11 of 44
Date: 6 Feb 92
Prep. by: R. R. Mohr
Rev. by: S. Perleman
Approved by: G. Roper

IDENT. No.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED / REMARKS
						SEV	PROB	Risk Code	
R/N.42	Relay K-28/Contacts (Normally Open)	Open w/Command to Close	Corrosion/or Mfg. Defect/or Basic Coil Failure (Open)	Loss of forward illumination/Impairment of night vision/Potential collision(s) w/unilluminated obstacles	P E T M	I III I I	D D D D	2 3 2 2	Redesign headlamp circuit to produce headlamp fail-on, w/timed off feature to protect battery, or eliminate relay/use HD Sw. at panel.

P: Personnel / E: Equipment / T: Downtime / M: Mission / V: Environment

16

Example of a FMEA worksheet

4. 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.

5.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.

6. 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?"

7. 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.

8. 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.

9. 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.

10. 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. 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 to

lower 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.

FMECA – FMEA with Criticality Analysis

The purpose of the Criticality Analysis is to rank each failure mode as identified in the FMEA, according to each failure mode's severity classification and its probability of occurrence. MIL-STD-1629 is an excellent data source for the implementation of a Criticality Analysis. The result of the Criticality Analysis will leads itself to the development of a Criticality Matrix. The failure mode criticality number for each specific failure mode (Cm) is calculated as follows: $C_m=\beta\alpha\lambda_p t$, where
C_m is failure mode criticality number
β is conditional probability of failure effect
α is failure mode ratio
λ_p is part failure rate per million hours
t is duration of relevant mission phase

The resulting FMECA analysis will enable a criticality matrix to be constructed. The criticality matrix displays the distribution of all the failure mode criticality numbers according to the severity category and referring to the criticality scale. According to Mil-Std-1629 the scale is divided into five levels:
Level A - Frequent. The high probability is defined as a probability which is equal or bigger than 0.2 of the overall system probability of failure during the defined mission period.
Level B - Reasonable probable. The reasonable (moderate) probability is defined as probability which is more than 0.1 but less than 0.2 of the overall system probability of failure during the defined mission period.
Level C - Occasional probability. The occasional probability is defined as a probability, which is more than 0.01 but less than 0.1 of the overall system probability of failure during the defined mission period.
Level D - Remote probability. The remote probability is defined as a probability, which is more than 0.001 but less than 0.01 of the overall system probability of failure during the defined mission period.

Level E - Extremely unlikely probability. The extremely unlikely probability is defined as probability which is less than 0.001 of the overall system probability of failure during the defined mission period.

Compiled from following sources:
http://www.asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html
http://www.fmeainfocentre.com/presentations/SFMEA-IIE.pdf
http://www.mtain.com/relia/relfmeca.htm

FTA – Fault Tree Analysis

FTA is a top-down failure analysis used for discovering the root causes of failures or potential failures. It uses boolean logic to combine a series of lower-level events.

The symbols used in a single FTA Logic Diagram are called Logic Gates and are similar to the symbols used by electronic circuit designers. A FTA is a status driven analysis where the inputs to a Logic Gate represent the status of a part and/or other factor being included in the analysis. Other factors can include such things as training, tools, safety equipment, supervision etc. The output from a Logic Gate is a logic state that represents a condition that exists in the system. An event occurs when the output of a Gate changes state.

If a part or other factor is functioning correctly, the state is TRUE. If the part or other factor is malfunctioning, the state is FALSE. When a logic statement is TRUE it is assigned a Boolean logic value of one (1). When a logic statement is FALSE it is assigned a Boolean logic value of zero (0). The FTA Logic Diagrams included in this analysis use the symbols listed in attached Logic Symbol Diagram. All Boolean Algebra rules are applicable.

An FTA is performed by systematically determining what happens to the system when the status of a part or other factor changes. The minimum criteria for success is that no single failure can cause injury or an undetected loss of control over the process. Where extreme hazards exist or when high value product is being processed, the criteria may be increased to require toleration of multiple failures.

An FTA requires consideration of both positive and negative events. The logic tree segments leading to a Negative Event, such as an accident, defines all of the things that could go wrong to cause the negative event. Logic tree segments for negative events usually use more OR gates than AND gates, except for redundant safeguards.

The logic tree segment leading to a positive event defines all of the things that must work together for the machine to operate or to complete a successful mission. Logic trees for positive events generally use more AND gates than OR gates, except for redundancy. Maintenance troubleshooting trees are a good examples of logic trees for positive events. Inverting the output of a positive event converts it into a negative event.

NAND and NOR gates are used primarily to define countermeasures that, if true, will allow the system to tolerate conditions that would otherwise result in safety hazards or machine failure. Bass Associates Inc. combines Positive Events, Negative Events and Countermeasures into the FTA Logic Diagram to provide a comprehensive system analysis.

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.

Standardization

FTA standardized in several industry and government standards, including NRC NUREG–0492 for the nuclear power industry, an aerospace-oriented revision to NUREG–0492 for use by NASA, SAE ARP4761 for civil aerospace, MIL–HDBK–338 for military systems for military systems. IEC standard IEC 61025 is intended for cross-industry use and has been adopted as European Norme EN 61025.

FTA procedure (by faa.org)

1. Assume a system state and identify and clearly document state the top level undesired event(s). This is often accomplished by using the PHL or PHA. Alternatively, design documentation such as schematics, flow diagrams, level B & C documentation may reviewed.
2. Develop the upper levels of the trees via a top down process. That is determine the intermediate failures and combinations of failures or events that are the minimum to cause the next higher level event to occur. The logical relationships are graphically generated as described below using standardized FTA logic symbols.
3. Continue the top down process until the root causes for each branch is identified and/or until further decomposition is not considered necessary.
4. Assign probabilities of failure to the lowest level event in each branch of the tree. This may be through predictions, allocations, or historical data.
5. Establish a Boolean equation for the tree using Boolean logic and evaluate the probability of the undesired top level event.
6. Compare to the system level requirement. If it the requirement is not met, implement corrective action. Corrective actions vary from redesign to analysis refinement.

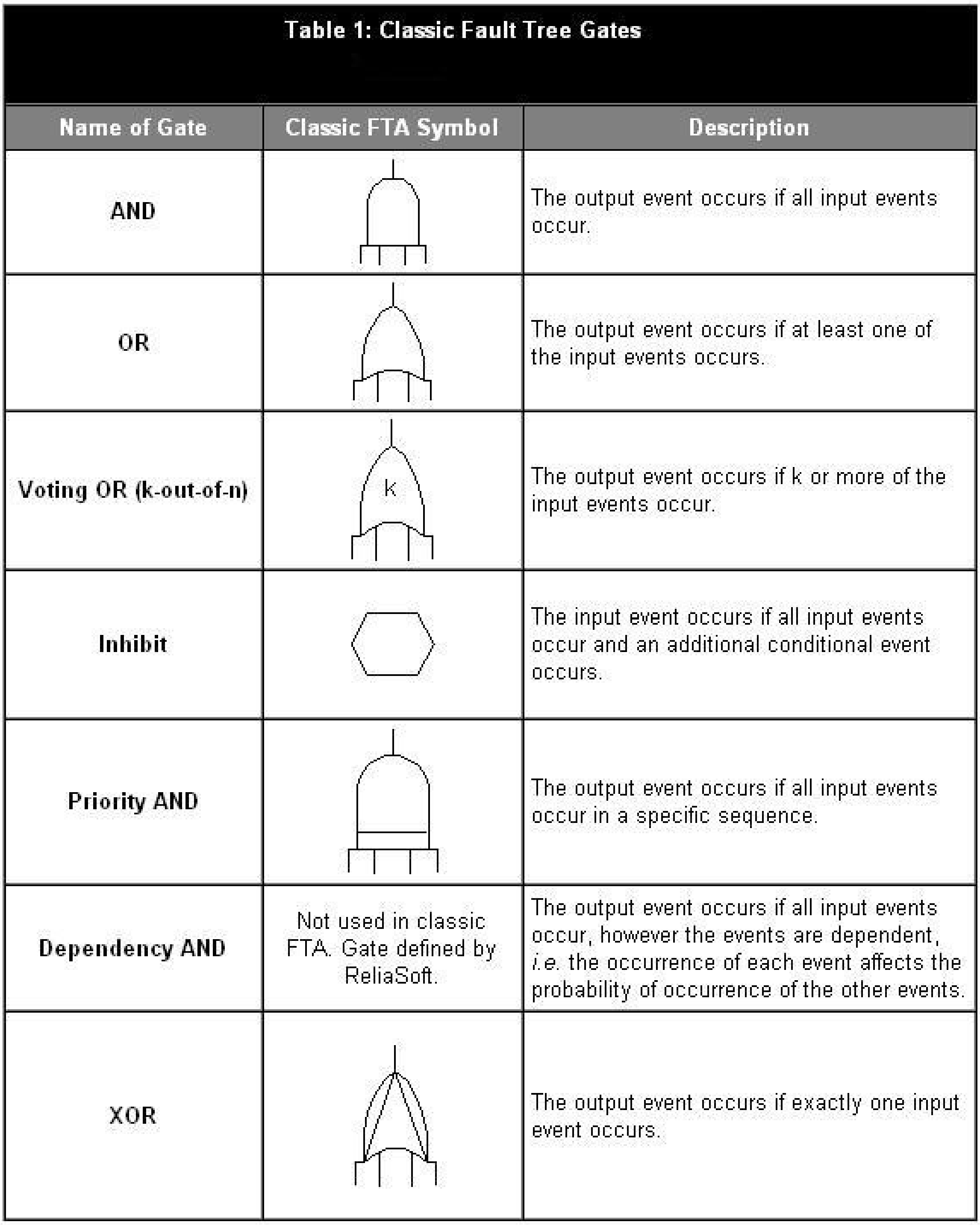


Table 1: Classic Fault Tree Gates

Name of Gate	Classic FTA Symbol	Description
AND		The output event occurs if all input events occur.
OR		The output event occurs if at least one of the input events occurs.
Voting OR (k-out-of-n)	k	The output event occurs if k or more of the input events occur.
Inhibit		The input event occurs if all input events occur and an additional conditional event occurs.
Priority AND		The output event occurs if all input events occur in a specific sequence.
Dependency AND	Not used in classic FTA. Gate defined by ReliaSoft.	The output event occurs if all input events occur, however the events are dependent, *i.e.* the occurrence of each event affects the probability of occurrence of the other events.
XOR		The output event occurs if exactly one input event occurs.

Based on available data, probabilities of occurrences for each event can be assigned. Algebraic expressions can be formulated to determine the probability of the top level event occurring. This can be compared to acceptable thresholds and the necessity and direction of corrective action determined.

The FTA shows the logical connections between failure events and the top level hazard or event. "Event," the terminology used, is an occurrence of any kind. Hazards and normal or abnormal system operations are examples. For example, both "engine overheats" and "frozen bearing" are abnormal events. Events are shown as some combination of rectangles, circles, triangles, diamonds, and "houses." Rectangles represent events that are a combination of lower level events. Circles represent events that require no further expansion. Triangles reflect events that are dependent on lower level events where the analyst has chosen to develop the fault tree further. Diamonds represent events that are not developed further, usually due to insufficient information. Depending upon criticality, it may be necessary to develop these branches further.

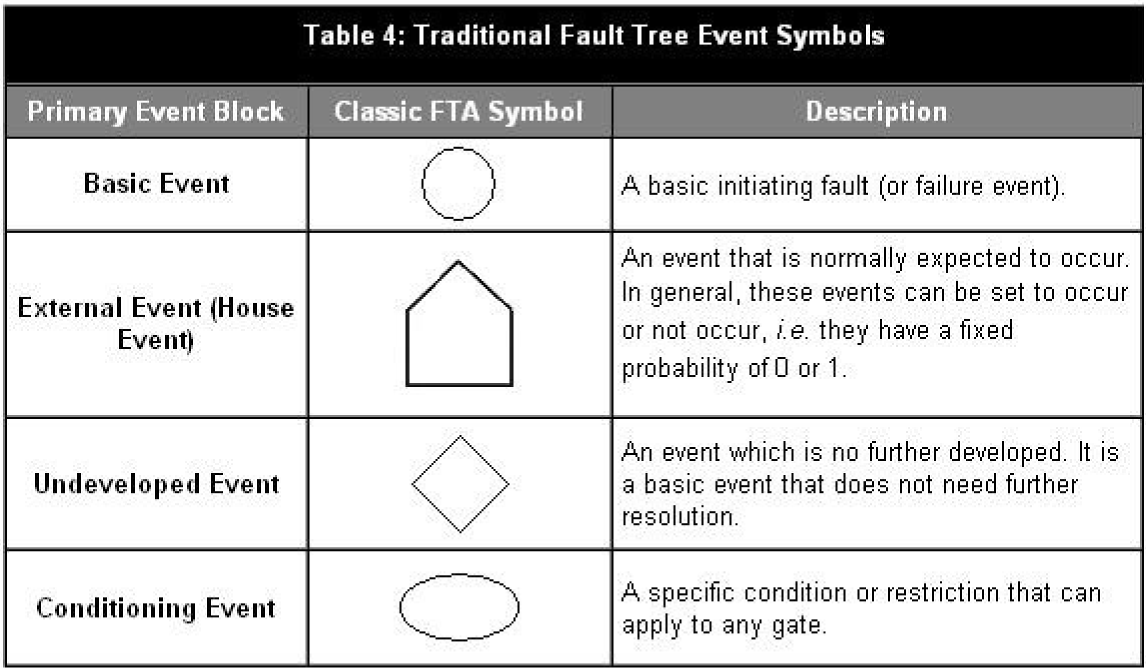


Table 4: Traditional Fault Tree Event Symbols

Primary Event Block	Classic FTA Symbol	Description
Basic Event	○	A basic initiating fault (or failure event).
External Event (House Event)	⌂	An event that is normally expected to occur. In general, these events can be set to occur or not occur, *i.e.* they have a fixed probability of 0 or 1.
Undeveloped Event	◇	An event which is no further developed. It is a basic event that does not need further resolution.
Conditioning Event	⬭	A specific condition or restriction that can apply to any gate.

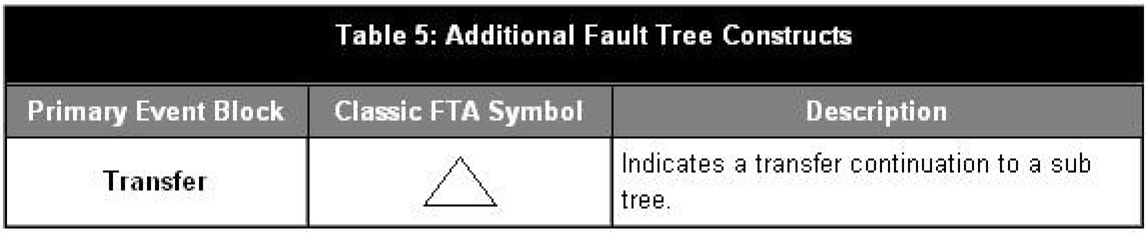


Table 5: Additional Fault Tree Constructs

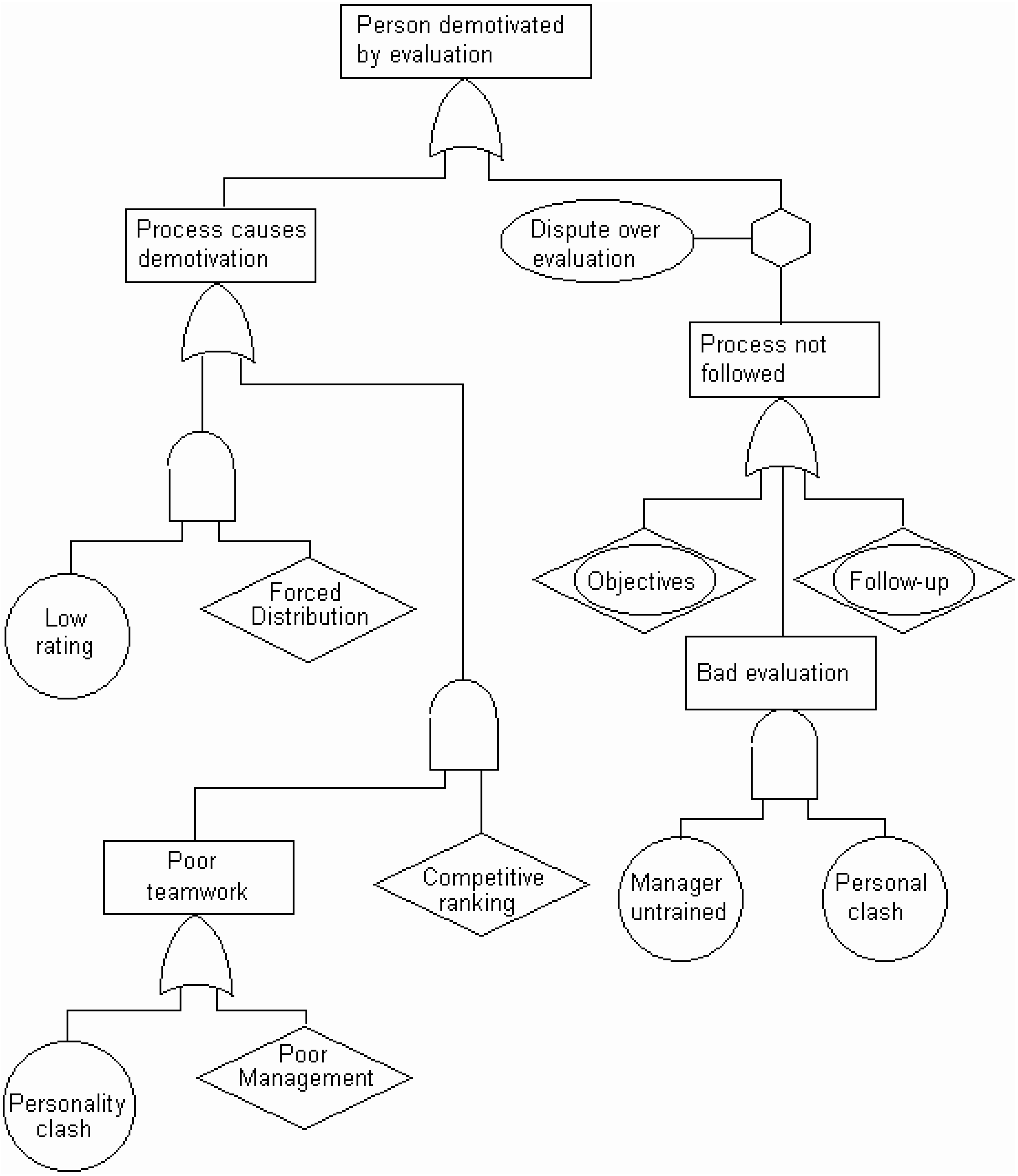
Primary Event Block	Classic FTA Symbol	Description
Transfer	△	Indicates a transfer continuation to a sub tree.

FTA symbols can depict all aspects of NAS events. The example reflects a hardware based problem. More typically, software (incorrect assumptions or boundary conditions), human factors (inadequate displays), and environment conditions (ice) are also included, as appropriate.

Events can be further broken down as primary and secondary. A primary event is a coolant pump failure caused by a bad bearing. A secondary event would be a pump failure caused by ice through the omission of antifreeze in the coolant on a cold day. The analyst may also distinguish between faults and failures. An ignition turned off at the wrong time is a fault, an ignition switch that will not conduct current is an example of failure.

Events are linked together by "AND" and "OR" logic gates. An "AND" gate is used for the ignition failure illustrating that the ignition systems are redundant. That is both must fail for the engine to fail. These logic gates are called Boolean gates or operators. Boolean algebra is used for the quantitative approach.

As previously stated, the FTA is built through a deductive "top down" process. It is a deductive process in that it considers combinations of events in the "cause" path as opposed to the inductive approach, which does not. The process is asking a series of logical questions such as "What could cause the engine to fail?" When all causes are identified, the series of questions is repeated at the next lower level, i.e., "What would prevent fuel flow?" Interdependent relationships are established in the same manner. When a quantitative analysis is performed, probabilities of occurrences are assigned to each event. The values are determined through analytical processes such as reliability predictions, engineering estimates, or the reduction of field data (when available). A completed tree is called a Boolean model.



Example of FTA graph

The probability of occurrence of the top level hazard is calculated by generating a Boolean equation. It expresses the chain of events required for the hazard to occur. Such an equation may reflect several alternative paths. Boolean equations rapidly become very complex for simple looking trees. They usually require computer modeling for solution. In addition to evaluating the significance of a risk and the likelihood of occurrence, FTAs facilitate presentations of the hazards, causes, and discussions of safety issues. They can contribute to the generation of the Master Minimum Equipment List (MMEL). The FTA's graphical format is superior to the tabular or matrix format in that the inter-relationships are obvious. The FTA graphic format is a good tool for the analyst not knowledgeable of the system being examined. The matrix format is still necessary for a hazard analysis to pick up severity, criticality, family tree, probability of event, cause of event, and other information.

Software FTA

Software fault tree analysis was developed in 1983. The process paralleled standard FTA principles, starting with a top event and working backwards through the tree, generating a path that showed the necessary hardware as well as software events that had to occur. SFTA, like FTA starts with a defined top event. This event is described through a hazard analysis and is usually a safety critical event. The process assumes, that the system has failed according to the defined event and works backwards to determine the set of possible paths that allow the event to occur. This path is made up of further decomposed events connected by hates similar to those in FTA. Events are continually expanded until either they cannot be developed further due to lack of information or insufficient consequences or they no longer require analysis. Once the tree has been fully expanded and analyzed, it can be shown that the program either allows or disallows the top event state to be reached. This information is then used to correct the program, if required, eliminating the undesired event's occurrence. Each event in the set of undesirable events is then analyzed in a similar fashion. It has been shown, that for large systems the use of partial SFTA can be effective in finding faults and in identifying critical modules that may need further analysis.

Unlike hardware fault trees where each hazard or event can be assigned a given probability of failure due to big amounts of historical data, software failures are in and of themselves logical, not lending themselves to a level of probability. The software either works or it does not. This distinction between probabilistic hardware fault trees and logical software fault trees is important in understanding the complexity involved in trying to conduct a complete software analysis.

In summary, SFTA can be used to determine software safety requirements, detect logic errors and identify multiple failure sequences involving different parts of the system that lead to hazardous events.

Competing technologies

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.

Compiled using following sources:
http://www.bassengineering.com/FTA.htm
http://www.fault-tree.net/papers/ericson-fta-history.pdf
http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/Chap9_1200.pdf
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA303377&Location=U2&doc=GetTRDoc.pdf
http://syque.com/quality_tools/toolbook/FTA/example.htm

FTA and FMEA comparison

FTA is a deductive, top-down method aimed at analyzing the effects of initiating faults and events on a complex system. This contrasts with Failure Mode and Effects Analysis (FMEA), which is an inductive, bottom-up analysis method aimed at analyzing the effects of single component or function failures on equipment or subsystems. FTA is very good at showing how resistant a system is to single or multiple initiating faults. It is not good at finding all possible initiating faults. FMEA is good at exhaustively cataloging initiating faults, and identifying their local effects. It is not good at examining multiple failures or their effects at a system level. FTA considers external events, FMEA does not. In civil aerospace the usual practice is to perform both FTA and FMEA, with a Failure Mode Effects Summary (FMES) as the interface between FMEA and FTA.