FAILURE MODES AND EFFECTS ANALYSIS

Failure Modes and Effects Analysis (FMEA) is an engineering activity that explores the effects of possible failure modes on a system and its environment. When criticality analysis is applied in FMEA, the technique is called FMECA (Failure Modes, Effects and Criticality Analysis). The expanding use of these techniques is a response to the growth in complexity, cost, and potential for catastrophic hazards in modern systems. FMEA and FMECA are often used to help prevent expensive system modifications by discovering latent design and operational deficiencies in early design and testing. FMEA and FMECA are also used to reduce failures or to support

J. Webster (ed.), *Wiley Encyclopedia of Electrical and Electronics Engineering*. Copyright © 1999 John Wiley & Sons, Inc.

maintenance by troubleshooting the design of a system after it is operational (1–4).

FMEA is a systematic method of identifying what can go wrong with each component of a system (its failure modes) and what effects each failure mode can have as it propagates through the component, the system, and the surroundings. A possible failure mode for an electrical part is "stuck open" or "short circuit." A possible effect is "no current flow," "erroneous output," or "loss of signal."

FMEA is performed on many types of systems including electrical, electronic, mechanical, avionic, space, nuclear, and hydraulic. FMEA may be quantitative or qualitative. If it is quantitative, a failure rate is determined for each failure mode. Failure rates for components can then be combined to measure system failure rates for each of the system's failure modes. Results of the FMEA can support reliability analysis and safety analysis processes.

ORIGIN

The move to production line facilities in the early twentieth century spurred interest in improving manufactured goods by reducing the number of failures, faults, rejects, or unacceptable parts. Statistical techniques allowed examination of how items were made and how to improve (or remove waste from) the methods of manufacture.

New electronic devices (RADAR) and the more sophisticated radio and avionics equipment developed during World War II prompted concerns about both efficient manufacture and continued reliability during use. These concerns grew during the late 1940s and the 1950s as the complexity of military systems increased. Systematic examination of failures was needed to improve reliability in both traditional equipment (e.g., communications, fire control, and avionics) and new military technologies (e.g., missiles, jet aircraft, and nuclear applications).

Early approaches to systems analysis and statistical analysis found sources of errors and unreliability in complex engineered systems. In addition, analyses of computer reliability began during these years. A 1955 military standard required "failure analysis" to provide for reliability control of the design of flight control systems (5). Other publications also described a technique that, by 1966, was being called by its modern name, Failure Mode and Effect Analysis (6,7). However, it took a number of years for this technique to spread beyond aerospace and the military into other applications.

Meanwhile, reliability as an engineering discipline continued to develop throughout the late 1950s. By 1960, a systems approach to reliability had been developed, and reliability issues were considered an integral aspect of engineering (8). By 1968, a published tutorial described the methodology using the FMECA label (9).

FMEA, along with reliability engineering, continued to mature throughout the 1970s, 1980s, and 1990s. During this time, use of FMEA spread from the aerospace electronics community to applications in the automotive, chemical processing, manufacturing, petroleum, and nuclear industries. In recent years, FMEA has been applied to a broad range of problems. Along with its traditional role in device design, FMEA is now used extensively in safety and logistics analysis, in medical engineering, and for improvement of process design. Stamatis reports that all major U.S. automobile companies require a FMEA program for their suppliers (4).

Software Failure Modes and Effects Analysis (SFMEA) is an extension of hardware FMEA that is used to examine the system consequences of software failure modes, such as incorrect data or incorrectly timed software activity (10). For example, a SFMEA of a particular system might identify one of its software failure modes to be "outdated data is used," the local effect of that failure mode to be "refrigerant pump is turned off," and the system-level effect to be "temperature limit is exceeded." The use of SFMEA has grown as system reliability has become more dependent on the correct functioning of the software.

PROCESS

A FMEA is a simple procedure. Although the specific language describing how to perform a FMEA differs somewhat, depending on the standard or source referenced, the process is basically the same. The required input to any FMEA activity is a clear, comprehensive description of the system/subsystem/component design. A FMEA can be conducted using the following steps:

1. Prepare a design description of the component or system.
2. Decide what type of analysis (functional or hardware) to perform.
3. Draw a block diagram and devise a coding system for identification, ensuring that all elements of the components are included.
4. Determine the functions or modules (if a functional FMEA), or piece parts and subassemblies (if a hardware FMEA) that comprise the block diagrams.

The previous steps are typically done during design regardless of whether a FMEA is going to be conducted, and are often available in a functional design document. They are essential input to the FMEA.

5. Determine the failure modes of each block. The identification of failure modes is the most difficult part of the FMEA process. For a higher-level, or functional, FMEA, an analysis of how the system could fail to achieve the required behavior yields a list of failure modes. These failure modes may address mechanical, electrical, electronic, software, environmental, and operational aspects of the system. For a lower-level, or piece-part, FMEA, a list of common failure modes (e.g., "valve failed open," "valve failed closed," etc.) is sometimes available for each component. For example, Stamatis provides a list of 88 major failure modes for semiconductors (4). Traditionally, FMEA is performed using known failure modes. Alternatively, a group of analysts with different, relevant areas of expertise will meet to brainstorm a list of ways in which the component might fail. For a FMEA at any level, industry data, project records

Table 1. FMEA Sample Standards

NASA

MSFC-SPEC-549. *Guidelines for Performing Failure Mode Effects (FMEA) on Mechanical, Electrical, and Electromechanical Components,* Base: 1977.

MSFC-SPEC-85M03885. *Guidelines for Performing Failure Mode, Effects, and Criticality Analysis (FMECA) on the Space Shuttle,* Base: 1971.

(There are 20+ NASA standards documents describing FMEA or FMECA, mostly from the Marshall Space Flight Center. These documents typically detail FMEA/FMECA processes for a specific system. MSFC-SPEC-549 and MSFC-SPEC-85M03885 are the most general and earliest of them.)

U.S. Military

MIL-F-18372, *Notice 1. Flight Control Systems: Design, Installation and Test of Aircraft (General Specification for),* 1997.

MIL-STD-1629A, *Notice 2. Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* 1984.

Industrial/International

BSI BS 5760: *Reliability of Systems, Equipment and Components, Part 5: Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FMECA),* British Standards Institution; London, 1991.

IEC Standard 812, *Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA),* International Electrotechnical Commission; Geneva, Switzerland, 1985.

SAE ARP 4761, Society of Automotive Engineers, *Aerospace Recommended Practice: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* Warrendale, PA: SAE International, 1996.

SAE J 1739—*Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual,* Recommended Practice July 1994. Society of Automotive Engineers, Warrendale, PA, 1994.

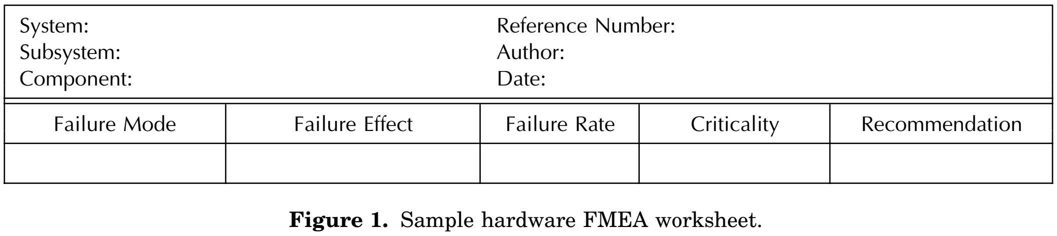
for previous, similar systems, and the analysts' knowledge are assets in determining the possible failure modes.

6. Analyze each block of the block diagram by identifying the effect of each failure mode on the component. In some application areas, a list of guidewords (e.g., "leak," "failure to isolate") can provide a baseline for the analysis. The assessment of failure effects includes both local consequences (e.g., a pipe rupturing causes leakage) as well as consequences throughout the system (e.g., the leakage contaminates an area). The effects also include any possible negative consequences on performance, safety, and functionality, as well as on humans or property.
7. Summarize the analysis for use in higher level analysis. Since FMEA uses a bottom-up approach, the effect of failure on the individual part is first identified, and then the broader effect on the system is described. FMEA may be performed at several different levels of abstraction, depending on the level of detail required. For example, FMEA from the lowest practical level may be required for innovative or safety-critical components, while only a high-level FMEA (or no FMEA) may be indicated for well-understood or noncritical components. When several levels of FMEA are performed, the effects at the lower level typically become the failure modes at the next higher level.
8. Use the FMEA results to improve the design. FMEA is often used as input to a design review, with follow-up to the FMEA involving implementation of the recommended corrective actions. For example, the FMEA process may yield a recommendation to add redundancy to avoid a single point failure. Since a quantitative FMEA is often used to predict reliability, components with low scores may be targeted for redesign, testing, maintenance, or logistics support activities. In this way, the FMEA helps identify and prioritize areas in need of additional project resources.

Combining the FMEA with a criticality analysis produces a FMECA (Failure Mode, Effect, and Criticality Analysis). A FMECA adds a classification of the failure modes in order to rank their criticality. The criticality measure is the product of the probability of the failure's occurrence and the severity of the failure's effects. The probability of piece-part failure is often available in industry data or by testing. The severity rating often refers to a standard four-tiered ranking ranging from "no effect" to "catastrophic effect."

A typical FMEA uses table-based worksheets to capture the relevant information. Standards, such as those in Table 1, as well as other references listed in the Bibliography, describe such worksheets in detail. Figure 1 is a typical worksheet for a hardware FMEA at the component or piece-part level. The third column documents the known or calculated failure rate. The right-hand column, labeled "Recommendation," refers to the role of the FMEA in proposing corrective actions. These may take the form of design changes to eliminate failure modes or to detect their presence, or of additional testing or validation procedures.

FMEA can vary somewhat in the format of the tables that are used. Figures 2 and 3 show two examples of FMEA from different industries. Each FMEA documents both the local and broader effects of the failure. Each also describes provis-



System:	Reference Number:
Subsystem:	Author:
Component:	Date:

Failure Mode	Failure Effect	Failure Rate	Criticality	Recommendation

Figure 1. Sample hardware FMEA worksheet.

VEHICLE: (Typical) SPACECRAFT
SYSTEM: ATTITUDE CONTROL

BLOCK DIAG. NO.	SYSTEM FUNCTION (MAJOR SECTION)	FAILURE TYPE	FAILURE CAUSE	EFFECT ON SYSTEM	EFFECT ON SPACECRAFT	COMPENSATING PROVISIONS	FAILURE CLASS
1.0	Helium pressurization, supply function	Leakage	Material and weld imperfection; vibration induced fatigue; loose fittings from vibration	Gradual loss of helium pressurizing gas, hence incomplete expulsion of fuel and oxidizer supply	Reduction in attitude maneuvers and duration of planned mission, depending on leak rate.	None	I (3-2-1)
		Rupture	Material or weld imperfection or micrometeoroid penetration	Complete loss of helium pressure, hence thruster engines inoperative	Immediate loss of attitude control capability, possible shrapnel damage to adjacent equipment	None	I (3-2-1)

Figure 2. Example of a functional FMEA worksheet for a spacecraft attitude control system. From Ref. 6. Copyright 1966 AIAA—Reprinted with permission.

ions for failure compensation. In addition, the FMEA in Fig. 3 describes how the failure can be detected.

AUTOMATION

The FMEA technique requires a practitioner to have extensive knowledge of the system being examined. Traditionally, FMEA is a manual, labor-intensive method. Recently, efforts to reduce the cost have focused on automation of FMEA, principally for electrical engineers in the automotive industry.

A number of programs are now available commercially and through professional organizations to assist with FMEA. Advertisements in a journal such as *IEEE Transactions on Reliability* or a search with an internet search engine provide many up-to-date sources for these programs. Software programs can ease the repetitive entry of data into the worksheets and the tedious updates of the FMEA to reflect design changes. Computer programs can calculate the needed statistics and analyze failure rate field data. Some FMEA databases contain failure rates or permit user queries.

A more important development in automating FMEA processes is programs that allow development and storage of component models in on-line libraries. These libraries allow circuit descriptions to be imported from the computer-aided design (CAD) tools used to design them and the outcomes of

SYSTEM: .... Blowout Preventer ....
INDENTURE LEVEL: .2 - Hydraulic Control Unit ....
REFERENCE DRAWING: .... XYZ123 ....
OPERATING STATE: .... Shallow drilling ....

DATE: ....
SHEET .... OF ....
ORIGINATOR: ....
APPROVED: ....

			FAILURE EFFECT					
ID	FUNCTION	FAILURE MODE	LOCAL EFFECT	SYSTEM EFFECT	FAILURE DETECTION METHOD	COMPENSATION PROVISIONS	SEVERITY	REMARKS
1.1 accumulator unit	Provide hydraulic power supply and converts electrical/ pneumatic signals into hydraulic power output	1.1/1 Loss of utility air	1. Pneumatically actuated valves fail to open	1. Control from tool-pushers panel inhibited	1. Diverter valve status lamp does not change over	1. Normal operation is from drillers pane	3	System operation degraded
			2. Loss of hydraulic pressure control	2. Hydraulic output signals inhibited	2. Hydraulic pressure alarm	2. Pressure control can be switched to customer supply	3	System operation degraded
			3. Air-driven hydraulic pump fails	3. Control from driller's and tool-pushers panels inhibited	3. Hydraulic pressure alarm	3. Electric driven pumps available	3	System operation degraded

Figure 3. Example of a FMEA worksheet with failure detection methods for an offshore safety system's hydraulic control unit. From Ref. 15. Reprinted by permission of Addison Wesley Longman Ltd.

each failure mode to be simulated (11). In some programs, libraries of failure modes are available. The reuse of models and simulation of faults cut the cost of FMEA and simplify the analysis of changes through the system's life-cycle.

EVALUATION

FMEA is a static, forward analysis method in that it searches forward in time from a failure mode to the possible effects of that failure. FMEA is limited in that it usually considers only one failure mode at a time. Analysis of the effects of multiple failures or of common-cause failures, particularly those involving timing, may be difficult (12). To compensate for these constraints, FMEA can be effectively combined with a backward analysis method, such as Fault Tree Analysis, which searches backward from a known failure mode to its contributing or root causes (3). For example, the HAZOP (Hazards and Operability Analysis) technique, widely used in the chemical industry, combines forward and backward searches to identify and analyze possible system hazards. In addition, the combination allows explicit consideration of operator actions, a frequent factor in accidents but often ignored in FMEA (12).

FMEA has also been combined with other reliability techniques that examine a different class of reliability problems. For example, FMEA has been used with Sneak Circuit Analysis (SCA), with the FMEA handling failures associated with system hardware and software, and the SCA handling unexpected behaviors resulting from circuit paths or current flows that have been designed unintentionally into a system (13).

STANDARDS

Once FMEA had been specified by the U.S. military and had matured in the aeronautical industry, it was rapidly incorporated into standards by other U.S. government organizations. The earliest organizations to set standards on the FMEA methodology were NASA in 1971 and the U.S. military in 1974. Subsequently, international standards organizations, British and German standards organizations, and the Society of Automotive Engineers issued FMEA standards. (Table 1 lists some key FMEA standards.) See Dhillon (14) for an extensive bibliography.

To summarize, FMEA is an important technique for identifying and analyzing the effects of failures in a system. FMEA is a key component of reliability analysis for a variety of applications.

BIBLIOGRAPHY

1. J. Klion, *Practical Electronic Reliability Engineering; Getting the Job Done from Requirement through Acceptance,* New York: Van Nostrand Reinhold, 1992.
2. E. E. Lewis, *Introduction to Reliability Engineering,* New York: Wiley, 1994.
3. D. Raheja, *Assurance Technologies: Principles and Practices,* New York: McGraw-Hill, 1991.
4. D. H. Stamatis, *Failure Mode and Effects Analysis: FMEA from Theory to Execution,* Milwaukee: ASQC Quality Press, 1995.
5. MIL-F-18372 *Notice 1—General Specification for Flight Control Systems: Design, Installation and Test of Aircraft,* 1997, Base: 1955.
6. H. E. Arnzen, Failure mode and effect analysis: A powerful engineering tool for component and system optimization, *Ann. Reliabil. Maintainabil.,* **5**: 355–371, 1966.
7. J. de S. Coutinho, Failure-effect analysis, *Trans. New York Acad. Sci.,* Series II, **26** (1): 564–584, 1964.
8. D. N. Chorafas, *Statistical Process and Reliability Engineering,* New York: D. Van Nostrand, 1960.
9. K. Greene and T. J. Cunningham, Failure mode, effects, and criticality analysis, *Symp. Reliabil. Proc.,* 374–384, 1968.
10. R. R. Lutz and R. M. Woodhouse, Requirements analysis using forward and backward search, *Ann. Softw. Eng.,* **3**: 459–475, 1997.
11. T. A. Montgomery et al., FMEA automation for the complete design process, *IEEE Proc. Annu. Reliabil. Maintainabil. Symp.,* IEEE Press, 30–36, 1996.
12. N. G. Leveson, *Safeware: System Safety and Computers,* Reading, MA: Addison-Wesley, 1991.
13. D. S. Savakoor, J. B. Bowles, and R. D. Bonnell, Combining sneak circuit analysis and failure modes and effects analysis, *IEEE Proc. Annu. Reliabil. Maintainabil. Symp.,* 199–205, 1993.
14. B. S. Dhillon, Failure modes and effects analysis—bibliography, *Microelectronics Reliability,* **32** (5): 719–731, 1992.
15. J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment* Essex: Addison Wesley Longman, 1993.

Robyn R. Lutz
Robert M. Woodhouse
Jet Propulsion Laboratory