Risk –Informed Regulation of Marine Systems Using FMEA

LT Robb Wilcox, P.E.
U.S. Coast Guard Marine Safety Center
Washington, D.C.

Abstract

The marine industry is recognizing the powerful techniques that can be used to perform risk analysis of marine systems. One technique that has been applied in both national and international marine regulations is Failure Mode and Effects Analysis (FMEA). This risk analysis tool assumes a failure mode occurs in a system/component through some failure mechanism; the effect of this failure is then evaluated. A risk ranking can be developed in a more detailed variant of FMEA called Failure Mode and Effects Criticality Analysis (FMECA).

1.0 FMEA Applications In Marine Regulations

Safety is an immense public concern for the maritime industry, especially in the application of relatively new marine technologies. Traditional regulation of conventional marine design has relied upon a level of risk, intuitively accepted, based on established design methods and operational history. A ship considered unsafe due to some maritime disaster or system failure, often causes regulatory change to improve safety. This form of risk management will never be totally eliminated because of the constant demand for improving safety and the fact that risk cannot be completely removed. However, other methods of risk management are being employed to provide adequate levels of safety to marine systems to avoid: the reactive approach to safety, long period of development, possible severe consequences to the public, and a high level of uncertainty about the safety performance of a new design.

The safety of a ship design is often questioned when relatively new technologies or complex systems are used that have not had a successful history of safe operation or an established engineering system. The need for a better understanding of the safety performance of new marine designs has prompted the application of established risk analysis techniques to develop an improved assessment of design safety. FMEA is one of the reliability/safety analysis tools adopted by the marine community for system safety analysis.

1.1 Title 46 Code of Federal Regulations

Title 46 Code of Federal Regulations (CFR) represents the regulatory requirements applicable to the design, construction, and operation of U.S. flagged ships. A requirement for failure analysis techniques is mentioned in 46 CFR Part

62 “Vital System Automation,” which represents the minimum requirements for vessel automated vital systems. While this regulation does not specifically require FMEA, it mandates the use of a qualitative failure analysis technique; most often FMEA is the technique applied. The above regulation requires a failure analysis to be performed on vital automation systems with the intent to assist in evaluating safety and reliability of the following systems: propulsion controls, microprocessor-based system hardware, safety controls, automated electric power management, automation required to be independent that aren’t physically separated, and any other automation that constitutes a safety hazard to the vessel or personnel. [1]

The acceptability of an automated system’s design is based on requirements for specific system monitoring, safety control requirements, and “failsafe” design. The acceptable “failsafe” states of the systems are pre-determined to require system design to levels of least critical consequence [1]. As an example, the preferred “failsafe” state for the propulsion speed control is the “as-is” condition. The performance of the design to meet these requirements is proven through design verification testing.

1.2 International Code of Safety for High-Speed Craft (HSC)

The HSC Code was adopted in 1994 to provide regulations for high-speed (low displacement) craft. The U.S. Coast Guard accepts compliance with the HSC Code as equivalent to compliance with the regulations in Subchapter K of Title 46 CFR. The Codes safety philosophy is based on the management and reduction of risks while recognizing that additional hazards exist for high-speed craft compared with a conventional ship. FMEA is a required part of the HSC Code compliance to provide an analysis of failure performance to assist in safety management. The FMEA procedure is well defined as an appendix to this reference. [2]

1.3 Guidance for Certification of Passenger Carrying Submersibles (NVIC 5-93)

Navigation Vessel and Inspection Circular (NVIC) No. (5-93) was created in 1993 to provide design guidance for the certification of passenger carrying submersibles in the U.S. The requirements of NVIC (5-93) are intended to provide an equivalent level of safety to surface craft. Included in the list of additional requirements for the submersible is the application of FMEA to all submersible systems. There is no specific format required for the FMEA, however, Mil-Std 1629A “Procedures for Performing a Failure Mode, Effects and Criticality Analysis” is stated as a reference. [3]

2.0 FMEA/FMECA Procedure

The process of conducting a Failure Mode and Effects Analysis can be examined in two levels of detail. FMEA is the first level of analysis, which consists of the identification of potential failures and the effects on systems performance by identifying the potential severity of the effect. The second level of analysis is the Failure Mode and Effects Criticality Analysis (FMECA) consisting of additional steps for calculating the risk of each failure through measurements of the severity and probability of a failure effect. Both of these methods are intended to provide information for making risk management decisions.

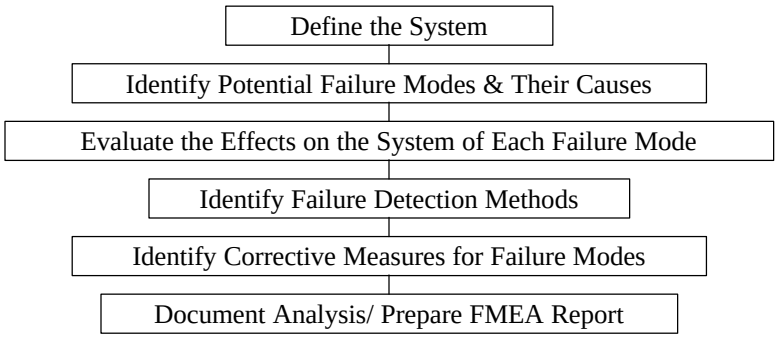

Figure 1. FMEA Procedure

2.1 FMEA

FMEA is an inductive process that examines the effect of a single point failure on the overall performance of a system through a "bottom-up approach" as shown in Figure 1[4]. This analysis should be performed iteratively in all stages of design and operation of a system, however, engineering system design should stress safety considerations early in the design process since it is more difficult and costly to rectify faults later.

2.1.1 Define the System

The first step in performing a FMEA is to organize as much information as possible about the system concept, design, and operational requirements. By organizing the system model, a rationale, repeatable, and systematic means to analyze the system can be achieved. One method of system modeling is the system breakdown structure model; a top down division of a system (e.g. ship, submarine, propulsion control) into functions, subsystems, and components. Block diagrams and fault-tree diagrams provide additional modeling techniques for describing the component/function relationships.

2.1.2 Identify Potential Failure Modes & Their Causes

The failure mode is the manner that a failure is observed in a function, subsystem, or component [1]. Failure modes of concern depend on the specific system, component, and operating environment. The past history of a component/system is used in addition to understanding the functional requirements to determine

relevant failure modes. For example, several common failure modes include: complete loss of function, uncontrolled output, and premature/late operation [2].

The cause of a failure mode is the physical or chemical processes, design defects, quality defects, part misapplication, or other methods, which are the reasons for failure [5]. It is important to note that more than one failure cause is possible for a failure mode; all potential causes of failure modes should be identified including human error. IMO HSC Code specifically mentions the need to consider the possible operator error that can occur when initiating a redundant system or the possible delay in initiating an alternative operational mode [2].

2.1.3 Evaluate the Effects on the System of Each Failure Mode

The failure effect is the severity of the consequence of the failure mode. The effect should consider conditions that influence the system performance goals of management; for regulation, the aspect of safety is most important. The effects are generally classified into three levels of propagation: local, next higher level, and end effect. The effects should be examined at different system levels in order to determine possible corrective measures for the failure [5]. The consequences of the failure mode can be identified by a severity index indicating the relative importance of the effect due to a failure mode [1]. Some common severity classifications include: I- catastrophic, II- critical, III- major, IV- minor [2].

2.1.4 Identify Failure Detection Methods/Corrective Actions

Part of the risk management portion of the FMEA is the determination of failure detection sensing methods and possible corrective actions [6]. There are many possible sensing device alternatives such as alarms, gauges, and inspection. An attempt should be made to correct a failure or provide a backup system (redundancy) to reduce the effects propagation to rest of system. If this is not possible, procedures should be developed for reducing the effect of the failure mode through operator actions, maintenance, and/or inspection. The IMO HSC Code and NVIC 5-93 both state that if the end effect is hazardous or catastrophic, a backup system and corrective operating procedure is required [2].

2.2 FMECA

Failure Mode and Effects Criticality Analysis is an extension of the FMEA process with the addition of a risk (criticality) assessment. Risk is a measure of the combination of the consequence of a failure mode and its probability of occurrence [7]. The results of the risk assessment can be prioritized to indicate high risk failure modes/items/systems that should receive risk reduction considerations.

2.2.1 Failure Probability Determination

The determination of the failure probability can be performed qualitatively or quantitatively. Quantitative analysis relies upon numeric estimation of failure

probability using data sources. Qualitative probability assessment is applied with the use of subjective estimation for probability values.

2.2.1.1 Qualitative Failure Probability Determination
Qualitative probability of failure is determined using probability categories selected by the analyst. The probability of occurrence categories often used are: A-frequent, B-moderate, C-occasional, D-unlikely, and E-extremely unlikely. [5]

2.2.1.2 Quantitative Failure Probability Determination
If the failure rate of a component is known, the probability can be evaluated from the determination of a quantitative criticality number as follows [5]:

$$C_r = \sum_{n=1}^{j} (a b l_p \mathrm{t})_n = \sum_{n=1}^{j} C_{m_n}$$

Failure mode Criticality Number (Cm) = portion of item criticality number due to one of its failure modes under a specific severity classification. Item Criticality Number (Cr) = probability of item failure of specific severity classification expected due to the items failure modes. Other variables: a = probability item will fail in a particular mode; b = conditional probability of failure effect given a specific failure mode; l_p = items failure rate; t = time; r = severity classification; n = failure modes in the items that fall under a particular criticality classification.

2.2.2 Criticality Matrix (Risk Matrix)

The risk associated with different failure modes or system components can be ranked to show the relative affects on safety. The criticality matrix is important for risk management because it provides an effective visual risk communications tool. To determine a component's risk, the probability/ item criticality number is combined with the severity classification. Those items considered to have relatively high risk should be examined to try to reduce the risk by lowering the probability or consequence of the event; acceptability depends on risk management criteria. The acceptance criteria shown in Table 1 is used as an example this may vary based on the decision of risk management. The IMO HSC Code and NVIC 5-93 both state that a single failure must not result in a catastrophic event, unless the likelihood is extremely remote.

Table 1. Risk/Criticality Matrix

	SEVERITY			
LIKELIHOOD	IV (Low)	III	II	I(High)
A (Frequent)	(3)	(2)	(1)	(1)
B	(3)	(2)	(2)	(1)
C	(3)	(3)	(2)	(1)
D	(4)	(3)	(2)	(1)

E (Unlikely)	(4)	(4)	(3)	(2)

(1) Unacceptable: should be mitigated to a (3) or lower; (2) Undesirable;
(3) Acceptable with controls ; (4) Acceptable as-is; no action necessary

3.0 Conclusion

FMEA/FMECA is an effective approach for risk analysis addressing risk assessment, risk management, and risk communication concerns. This analysis provides information that can be used in risk management decisions for system safety. FMEA has been used successfully within many different industries and has recently been applied in maritime regulations to address safety concerns with relatively new designs.

While FMEA/FMECA is a useful tool for risk management, it also has qualities that limit its application as a complete system safety approach. This technique provides risk analysis for comparison of single component failures only; avoiding such concerns as common cause failures. Other techniques for providing risk analysis should be considered for their application to specific system safety determinations. Perhaps an integrated program using various risk analysis techniques would further improve the understanding of marine system safety.

It is important to realize the strengths and weaknesses of this risk analysis technique to apply it correctly to system safety applications. With knowledge of the capabilities of this tool the risk manager can improve engineering designs with regards towards system safety.

References

1. Title 46 Code of Federal Regulations Part 62 - Vital System Automation. The Office of the Federal Register National Archives and Records Administration.
2. International Code of Safety for High-Speed Craft, International Maritime Organization, 1995, pp. 175-185
3. USCG Navigation Vessel and Inspection Circular No. 5-93, 1993
4. Andrews J, Moss T. Reliability and Risk Assessment. Longman Scientific & Technical, 1993
5. Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, 1980
6. Modarres M., What Every Engineer Should Know About Reliability and Risk Analysis, Marcel Dekker, Inc., 1993
7. Wilcox R, Karaszewski Z, Ayyub B. Methodology for Risk-Based Technology Applications to Marine System Safety. In: Ship Structure Symposium 1996