No. 138 (Dec 2014) Recommendation for the FMEA process for diesel engine control systems

1 General

1.1 Introduction

IACS UR M44 defines the documents required for the approval of diesel engines. For engine control systems, the following item and respective footnote are listed in Table 1 of UR M44:

25	FMEA (for engine control system)[5]

5. Where engines rely on hydraulic, pneumatic or electronic control of fuel injection and/or valves, a failure mode and effects analysis (FMEA) is to be submitted to demonstrate that single failure of the control system will not result in the operation of the engine being degraded beyond acceptable performance criteria for the engine. The FMEA reports required will not be explicitly approved by the classification society.

UR M44 does not define requirements for the performance of an FMEA. It is therefore the purpose of this document to give guidance on FMEA for diesel engine control systems as required in IACS UR M44. It may also be applied to the control system of dual-fuel and gas engines.

1.2 Objectives

1.2.1 The primary objective of an FMEA for the diesel engine control system is to provide a comprehensive, systematic and documented analysis, which establishes the important failure conditions and assesses their significance with regard to acceptable safety and performance criteria. As stated in UR M44, the FMEA should demonstrate that single failure of the control system will not result in the operation of the engine being degraded beyond acceptable performance criteria for the engine. Thereby, single failure is related to the consideration of only one component failure mode at a time, i.e. no combination of failure modes; however, it considers the possibility of common-cause failures.

1.2.2 General acceptable performance and safety criteria for the engine, as well as criteria specific to the engine application (see 2.1.1), should be stated in the FMEA report and all identified failure modes evaluated against these criteria. By doing so, the analysis recommended in this document is rather similar to a Failure Mode, Effects and Criticality Analysis (FMECA); however, the objective to demonstrate the compliance with acceptance criteria can efficiently be met this way.

1.2.3 This Recommendation focuses on the analysis and documentation requirements of an FMEA. The FMEA process and procedure is comprehensively documented in reference literature and recognized standards such as HSC-Code Annex 3 and Annex 4 and IMCA M 166.

1.3 System FMEA

1.3.1 The diesel engine control system FMEA should be performed as a system FMEA.

1.3.2 A system FMEA is carried out in a top-down manner, i.e. it starts from the overall system level and progresses to the next level down, or subsystem level, and further down to

No. 138 (cont)

the equipment item or component level. However, if it can be justifiably shown that at a certain level there is no further effect on the overall system if a failure occurs, then it is not necessary to continue to the next level down. In this case, it would not be necessary to continue to analyse all of the system levels down to component level.

1.3.3 The FMEA for diesel engine control systems should be based on a single-failure concept under which a subsystem or equipment item at various levels of the system's functional hierarchy is assumed to fail by one probable cause (initiating event) at a time. The effects of the postulated failure are analysed and classified according to their severity. Any failure mode which may cause an effect on the system beyond previously agreed acceptance criteria shall be mitigated by measures such as system or equipment redundancy. An exception is a “hidden failure” in which a second failure must occur in order to expose the “hidden failure”. A “hidden failure” is a special case because the failure effects are not apparent to the vessel operators under normal circumstances if the failure occurs on its own. One example would be a relief valve on a steam pipe.

1.3.4 A test programme of selected items should be drawn up to verify the assumptions and confirm the conclusions made in the FMEA.

1.4 Acronyms and definitions

For the purpose of this Recommendation, the acronyms and definitions listed in Table 1 apply.

Table 1: Acronyms and definitions

Term	Definition
CCF	Common Cause Failure. Failures of different items, resulting from a single event, where these failures are not consequences of each other.
Component	A constituent basic element or item of a system. In the context of diesel engine control systems e.g. a sensor, a processor, etc.
Design Intent	A detailed explanation of the ideas, concepts, and criteria that are defined by the designer to be important. Typically included • System requirements • Design conditions • System limitations
Essential Services	Equipment and systems necessary for the design intent and safe operation of the engine (e.g. fuel oil supply, cylinder lubrication, waste gate control, etc.)
Failure	Termination of the ability of an item or component to perform a required function under stated conditions.
Failure Effect	Immediate consequences of a failure on operation, function or functionality, or status of some item.
Failure Mode	The specific manner or way by which a failure occurs in terms of failure of the item (being a part or (sub) system) function under investigation; it may generally describe the way the failure occurs or the observed effect.
FMEA	Failure Mode and Effects Analysis. A systematic technique for failure analysis of the systems to whatever level of detail is required to identify the potential failure modes, their causes and effects on the performance of a system.
FMECA	Failure Mode, Effects and Criticality Analysis. An extension to the FMEA to include a means of ranking the severity of the failure modes to allow prioritization of countermeasures. This is done by combining the severity measure and frequency of occurrence to produce a metric called criticality.

No. 138 (cont)

Term	Definition
Function	A Function is what the system or equipment item is designed to do. Each function should be documented as a function statement that contains a verb describing the function, an object on which the function acts, and performance standard(s).
Interface	A point at which independent systems or components interact or communicate.
Redundancy	Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system.
Reliability	Reliability is the ability of an item to perform a required function for a stated period of time under stated conditions.
Safety	This is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.
Severity	The magnitude of the consequence as a result of a failure mode occurring. Severity considers the worst potential consequence of a failure mode.
System	Set of interrelated or interacting elements. In the FMEA context, a system will have a) defined purposes expressed in terms of required functions; b) stated conditions of operation use; c) a defined boundary. The structure of a system is hierarchical.
System Boundary	The system boundary forms the physical and functional interface between the system and its environment, including other systems with which the analysed system interacts. The definition of the system boundary for the analysis should correspond to the boundary as defined for design and maintenance. This should apply to a system at any level. Systems and/or components outside the boundaries should explicitly be defined for exclusion.

No. 138 (cont)

2 FMEA process

The FMEA process can be divided into several steps as shown in Figure 1. These steps are further described in the following paragraphs, as referenced in Figure 1. The FMEA report shall describe all necessary information used as input for the FMEA process as well as the assumptions and results. The FMEA report is described in section 3.

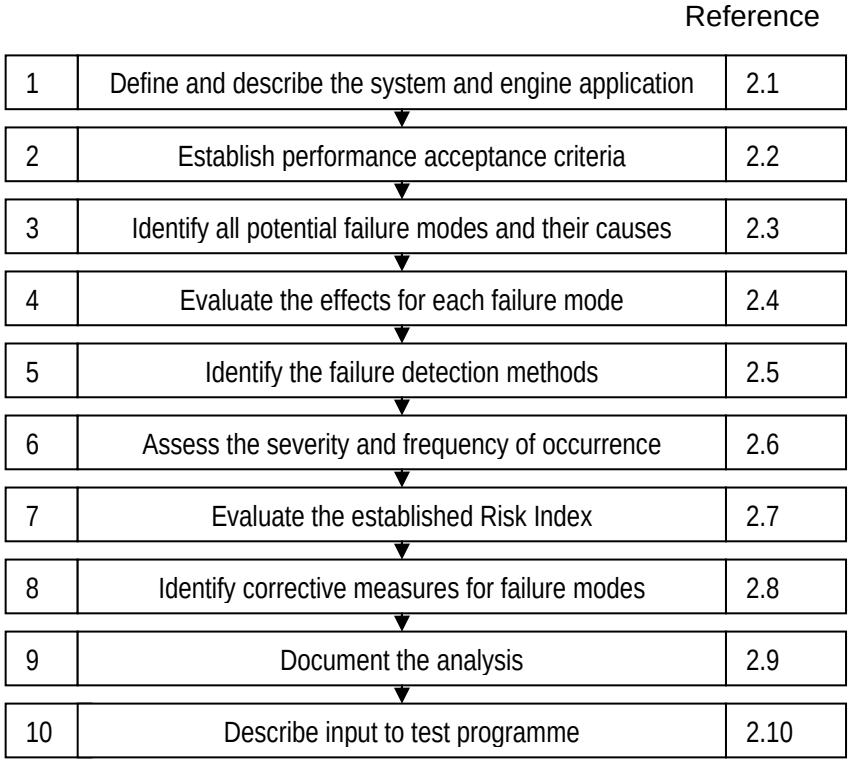

Figure 1: Diesel engine control system FMEA process

2.1 Define and describe the system and engine application

As a basis for the FMEA, the system to be analysed should be described through narrative text, use of drawings and reference to equipment manuals. The narrative description of the system, its operational modes, boundaries and functional requirements should address the following:

2.1.1 Description of the engine application (refer also to UR M44, Appendix 3, “Design”), primarily defining:

- Single main engine propulsion (and limitations of application, e.g. controllable pitch propeller only)
- Multiple engines (diesel-electric and diesel-mechanic)
- Auxiliary engine
- Emergency engine

No. 138 (cont)

2.1.2 Functional description of system operation, structure and boundaries:

- Description of system boundaries (physical, e.g. diesel engine and control system elements considered in the analysis as well as operational boundaries, e.g. performance parameters):
  - I/O signal specification, sensors and actuators
  - Interface signal specification
  - Monitoring system, including human-machine-interfaces
  - Network connection, e.g. CAN bus, Ethernet
  - Protection, e.g. galvanic isolation
  - Hardwired safety circuits
  - Power supply arrangement
  - Definitions of interactions with engine external systems (e.g. ship alarm system, gear box, controllable pitch propeller automation, power management, gas detection, exhaust, ventilation, lube oil supply, fuel supply systems)
  - Definition of limiting performance parameters influenced by the control system, e.g. temperatures, pressures, power, speed
- Design intent(s) and system operational modes for the electronic control system
  - Description of manual operation
  - Description of local/remote mode
  - Alarms/warnings
- Any interface to the engine safety system, if applicable
- Illustration of the interrelationships of functional elements of the system by means of block diagram(s)

  The block diagram(s) should provide a graphical representation of the system and its components for the subsequent analysis. As a minimum, the block diagram should contain:
  - Breakdown of the system into major sub-systems or components
  - All appropriately labelled inputs and outputs and identification numbers by which each sub-system is referenced; and
  - All redundancies, alternative signal paths and other engineering features, which provide "fail-safe" measures

  It may be necessary to develop a different set of block diagrams for each operational mode.

No. 138 (cont)

2.1.3 Functional relationships among the system elements, including:

- Listing of all component units and components within the control system boundary (part list, names, functions)
- Redundancy level and nature of the redundancies, separation, independency
- Description of multiple CPU operation from a concept/system architecture perspective
- Distributed control system architecture

2.1.4 System requirements and function with acceptable functional performance limits of the system and its constituent elements in each of the typical operational modes

- Acceptance criteria for the electronic control - and safety system performance depending on engine application

2.1.5 System constraints

2.2 Establish safety and performance acceptance criteria

Performance acceptance criteria are to be established considering

- The pertinent class and statutory requirements
- The acceptable operating criteria set by the engine designer with respect to safety and availability
- The engine application (refer to UR M44, Appendix 3, “Design”), e.g. a single engine propulsion application may have stricter acceptance criteria than a multiple engine propulsion application, for instance higher redundancy requirements and design for fault tolerance, meaning that the system can maintain safe operation in the presence of a certain number and certain types of failures

2.2.1 The acceptable performance criteria need to be stated in a manner, which enables the evaluation of each failure mode against these criteria. It is recommended to apply a risk matrix, using a severity index, reflecting the impact of a failure mode to the safety and to the engine performance, and a frequency index reflecting the frequency of occurrence of the event.

2.2.2 The assumptions made in the evaluation of the severity and frequency indices should be documented.

2.2.3 The following tables give **examples** of indices and the resulting risk matrix (Risk Index table). Depending on the specific analysis, a different scale or number of index steps may be used. The risk matrix can be divided into three areas: an area with an acceptable risk index (here lower left with indices 2 and 3), the area with not-acceptable risk indices (here upper right with indices 5, 6 and 7), and the area between the before mentioned two (here the diagonal with index 4), where the acceptance depends on further description of the event, for instance means of detection of the failure and the possibility of a manual mode of operation after a failure has occurred. In this area every effort should be made to make the risk as low as reasonably practicable.

No. 138 (cont)

Table 2: Example of Severity Index (SI) table

SI	Description	Definition
3	High	Serious impact on safety, e.g. fatality and/or Serious impact on engine performance e.g. engine stop
2	Medium	Medium impact on safety, e.g. injury and/or Medium impact on engine performance e.g. engine de-rated
1	Low	Negligible to low impact on safety and/or Negligible to low impact on engine performance

Table 3: Example of Frequency Index (FI) table

FI	Description	Definition
4	High	1 or more events per year of engine operation
3	Medium	1 event in 10 to less than 1 event in 1 engines per year of engine operation
2	Low	1 event in 100 to less than 1 event in 10 engines per year of engine operation
1	Very Low	less than 1 event in 100 engines per year of engine operation

Table 4: Example of Risk Index (RI) table

	FI	**1**	**2**	**3**	**4**
SI		**Very Low**	**Low**	**Medium**	**High**
3	**High**	4	5	6	7
2	**Medium**	3	4	5	6
1	**Low**	2	3	4	5

2.3 Identify all potential failure modes and their causes

A failure mode is the specific effect by which a failure is observed. When used in conjunction with functional performance specifications governing the inputs and outputs on the system block diagram, all potential failure modes can be thus identified and described.

Each (sub-) system should be considered in a top-down approach. Starting from the system's functional output a failure should be assumed by one possible cause at a time. Since a failure mode may have more than one cause, all potential independent causes for each failure mode should be identified.

2.3.1 Identify all potential common cause failures: It is not sufficient to consider only random and independent failures. Some common-cause failures (CCF) can occur, that cause system performance degradation or failure through simultaneous deficiency in several system components, due to a single source, environmental stresses, or human error. CCFs are those failures, which defeat the fundamental assumption that the failure modes under consideration in the FMEA are independent. The CCF will cause more than one item to fail simultaneously, or within a sufficiently short period of time as to have the effect of simultaneous failures. Typically, sources of CCF include environmental influences, such as electrical interference, temperature cycling, vibration, as well as human factors like incorrect operating or maintenance actions.

No. 138 (cont)

2.4 Evaluate the effects for each failure mode

The consequence of a failure mode on the operation, function, or status of a component or a system is called a 'failure effect'. The failure effects are to be evaluated regarding safety and availability in two respects locally, i.e. related to the engine, considering effects to the engine safety system as well, if applicable; and globally, i.e. related to the engine application, e.g. single prime mover in a ship or multiple engine installation.

2.5 Identify failure detection methods

A failure detection method can be a visual or audible warning device, automatic sensing devices, sensing instrumentation, manual inspection or other unique indications. These are to be identified for every failure mode and its causes, as appropriate.

2.6 Assess the severity and frequency of occurrence against the safety and performance acceptance criteria

The severity of each failure effect, as well as the frequency of occurrence of each failure mode should be assessed, e.g. using elaborated index tables dependent on the acceptable performance and safety criteria as described in 2.2 above. Local and global effects on safety and availability should be considered when determining the severity index.

2.7 Evaluate the established Risk Index

The risk index for each failure mode is to be evaluated as described in 2.2.3 and the example in Table 4.

2.8 Identify corrective measures for failure modes

The response of any back-up equipment, or any corrective action (manual or automatic) initiated at a given system level to prevent or reduce the effect of the failure mode of a system element or component is to be identified and evaluated.

2.9 Document the analysis

It is helpful to perform FMEA on worksheets with a structure similar to the example below. The worksheet(s) should start with the highest system level and then proceed down through the system hierarchy.

No. 138 (cont)

Example FMEA worksheet

Name of system_____ References_____

Mode of operation_____ System block diagram_____

Sheet No_____ _____

Date_____ _____

FMEA participants_____ Drawings_____

Id. No.	Item description	Function	Failure mode	Failure effects		Severity Index of failure effect	Failure causes	Frequency Index of event	Risk Index	Detection method	Corrective action	Remark / Testing
				local	global							
	Ref to 2.1	Ref to 2.1.4	Ref to 2.3	Ref to 2.4	Ref to 2.4	Ref to 2.6	Ref to 2.3	Ref to 2.6	Ref to 2.7	Ref to 2.5	Ref to 2.8	Ref to 2.10

2.10 Describe input to test programme

A test program should be developed to support the conclusions from the FMEA analysis and to verify any assumptions made.

The FMEA should be an input to the development of test specifications in general and particularly for identification of relevant test to be done during Type Approval Test (TAT) and Factory Acceptance Test (FAT) respectively.

3 FMEA report

The FMEA report should include a description of the diesel engine control system, its subsystems and their functions and the proposed operating and environmental conditions for the failure modes, causes and effects to be understood. The analysis assumptions, system block diagrams, performance acceptance criteria, worksheets (ref. to 2.9), as well as the reference to a test programme and any other test reports should be included. The report should contain a summary of the main conclusions, such as the results of the evaluation against the acceptance criteria.

4 References

HSC Code 2000: International Code of Safety for High Speed Craft
Annex 3 - *Use of probability concept*
Annex 4 - *Procedures for failure mode and effects analysis*
International Maritime Organization, 2000

IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). International Electrotechnical Commission IEC, 2006

IMCA M 166: Guidance on Failure Modes & Effects Analyses (FMEAs). The International Marine Contractors Association (IMCA), 2002

End of Document