Extension to Chapter 3.
FMECA

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- To understand why Failure modes, effects, and criticality analysis (FMECA) is used
- To understand terminology used in an FMECA
- To learn the steps of an FMECA
- To realize the pros and cons of an FMECA

The slides provide additional information to Chapter 3 in **Reliability of Safety-Critical Systems: Theory and Applications**.
DOI:10.1002/9781118776353.

Outline of Presentation

What is FMECA?

☞ Failure modes, effects, and criticality analysis (FMECA): A methodology to identify and analyze:

- All potential failure modes of the various parts of a system
- The effects these failures may have on the system
- How to avoid the failures, and/or mitigate the effects of the failures on the system

FMECA is a technique used to *identify*, *prioritize*, and *eliminate* potential failures from the system, design or process before they reach the customer.

– Omdahl (1988)

FMECA is a technique to "resolve potential problems in a system before they occur."

– SEMATECH (1992)

FMECA – FMEA

Initially, the FMECA was called FMEA (Failure modes and effects analysis). The C in FMECA indicates that the criticality (or severity) of the various failure effects are considered and ranked.

Today, FMEA is often used as a synonym for FMECA. The distinction between the two terms has become blurred.

Background

- FMECA was one of the first systematic techniques for failure analysis
- FMECA was developed by the U.S. Military. The first guideline was Military Procedure MIL-P-1629 “Procedures for performing a failure mode, effects and criticality analysis” dated November 9, 1949
- FMECA is the most widely used reliability analysis technique in the initial stages of product/system development
- FMECA is usually performed during the conceptual and initial design phases of the system in order to assure that all potential failure modes have been considered and the proper provisions have been made to eliminate these failures

What Can FMECA be Used for?

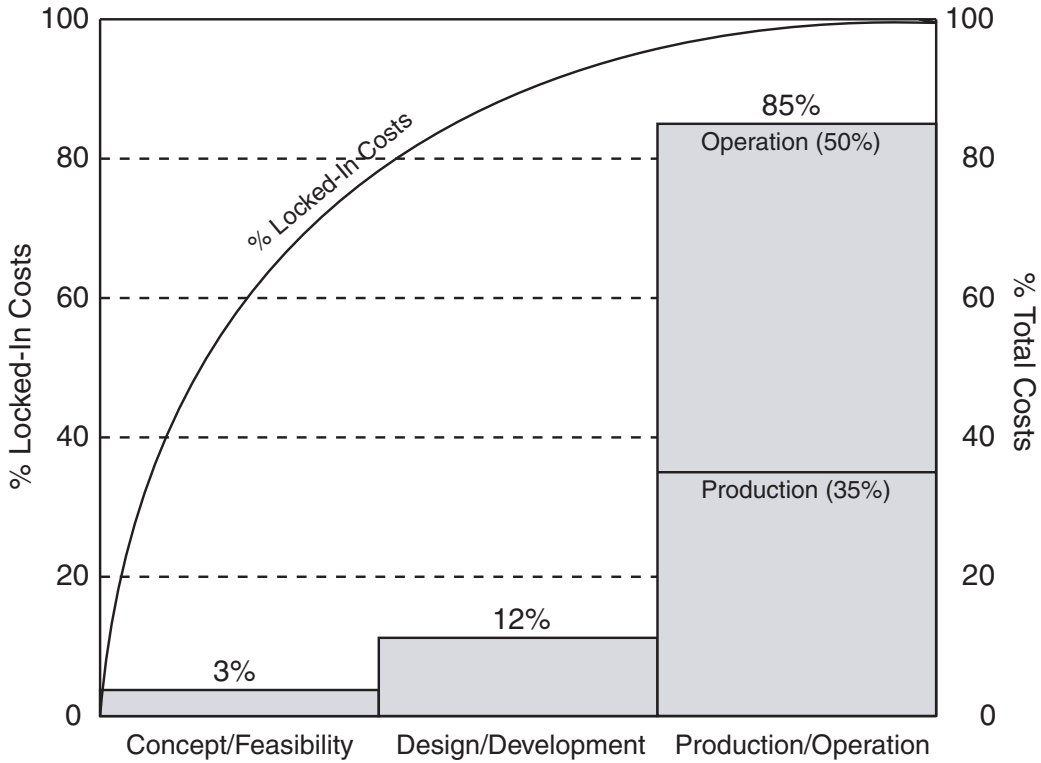
- Assist in selecting design alternatives with high reliability and high safety potential during the early design phases
- Ensure that all conceivable failure modes and their effects on operational success of the system have been considered
- List potential failures and identify the severity of their effects
- Develop early criteria for test planning and requirements for test equipment
- Provide historical documentation for future reference to aid in analysis of field failures and consideration of design changes
- Provide a basis for maintenance planning
- Provide a basis for quantitative reliability and availability analyses.

FMECA Basic Question

1. How can each part conceivably fail?
2. What mechanisms might produce these modes of failure?
3. What could the effects be if the failures did occur?
4. Is the failure in the safe or unsafe direction?
5. How is the failure detected?
6. What inherent provisions are provided in the design to compensate for the failure?

When to Perform an FMECA

The FMECA should be initiated early in the design process, where we are able to have the greatest impact on the equipment reliability. The locked-in cost versus the total cost of a product is illustrated in the figure:



– Source: SEMATECH (1992)

Types of FMECA

- Design FMECA is carried out to eliminate failures during equipment design, taking into account all types of failures during the whole life-span of the equipment
- Process FMECA is focused on problems stemming from how the equipment is manufactured, maintained or operated
- System FMECA looks for potential problems and bottlenecks in larger processes, such as entire production lines

Two Approaches to FMECA

- Bottom-up approach
  - The bottom-up approach is used when a system concept has been decided. Each component on the lowest level of indenture is studied one-by-one. The bottom-up approach is also called *hardware* approach. The analysis is *complete* since all components are considered.

- Top-down approach
  - The top-down approach is mainly used in an early design phase before the whole system structure is decided. The analysis is usually function oriented. The analysis starts with the main system functions - and how these may fail. Functional failures with significant effects are usually prioritized in the analysis. The analysis will not necessarily be complete. The top-down approach may also be used on an existing system to focus on problem areas.

FMECA Standards

- MIL-STD 1629 “Procedures for performing a failure mode and effect analysis”
- IEC 60812 “Procedures for failure mode and effect analysis (FMEA)”
- BS 5760-5 “Guide to failure modes, effects and criticality analysis (FMEA and FMECA)”
- SAE ARP 5580 “Recommended failure modes and effects analysis (FMEA) practices for non-automobile applications”
- SAE J1739 “Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA)”
- SEMATECH (1992) “Failure Modes and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry”

Definition of Failure

☞ Failure: The termination of the ability of an item to perform a required function. [IEV 191-04-01]

A failure is always related to a required function. The function is often specified together with several performance requirements, such as response time, reliability target, behavoir upon fault condition etc.

Shutdown valve

A maximum closing time of a shutdown valve may be set to 15 seconds. A failure of the function occurs when the closing time exceeds 15 seconds.

Failure Attributes

A failure is an event that occurs at a specific point in time.

A failure may:

- Develop gradually
- Occur as a sudden event

The failure may sometimes be revealed:

- On demand (i.e., when the function is needed) (“hidden”)
- During a functional test (also “hidden”)
- By monitoring or diagnostics (“evident”)

Fault

☞ Fault: The state of an item characterized by inability to perform a required function [IEV 191-05-01]

While a failure is an event that occurs at a specific point in time, a fault is a state that will last for a shorter or longer period.

In most cases, an item will have a fault after a hardware failure has occurred – and we say that the item is in a failed state.

Design and installation errors may also prevent the item from performing its required function. The item has a fault that is not preceded by any hardware failure and we call this fault a systematic fault.

Error

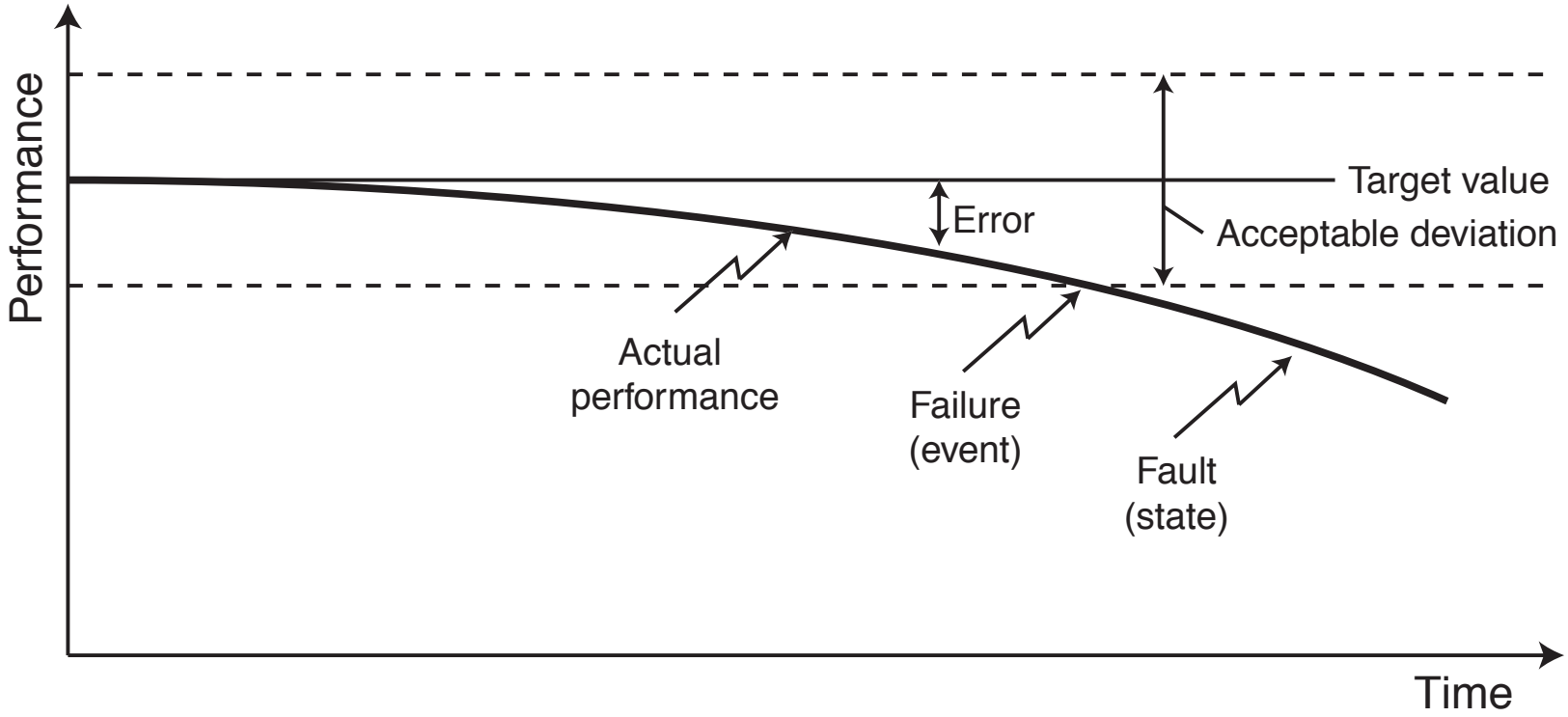
☞ Error: Discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

[IEC 191-05-24].

An error is present when the performance of a function deviates from the target performance (i.e., the theoretically correct performance), but still satisfies the performance requirement. An error will often, but not always, develop into a failure.

Relationship failure, fault and error

A failure may originate from an error. When the failure occurs, the item enters a fault state.



Failure Mode

☞ Failure mode: The way a failure is observed on a failed item. [IEC 191-05-22]

A failure mode is the way in which an item could fail to perform its required function. An item can fail in many different ways – a failure mode is a description of a possible state of the item after it has failed.

Pump

Performance requirement: The pump must provide an output between 100 and 110 liters per minute.
Associated failure modes may be:

- No output
- Too low output
- Too high output
- Too much fluctuation in output

Classification of Failures

Failures may be classified according to their:

- Causes: To avoid future occurrences and make judgments about repair
- Effects: To rank between critical and not so critical failures
- Detectability: To distinguish failures that may be revealed "automatically" (and shortly after their occurrence) and those that may be hidden until special effort is taken, such as functional tests.
- And several other criteria.

Special category:

- Common-cause failures (CCFs)

Example: Failure classification in IEC 61508

IEC 61508 classify failures according to their:

- Causes:
  - Random (hardware) faults
  - Systematic("functional") faults (including software faults)
- Effects:
  - Safe failures (typically: untimely activation of function)
  - Dangerous failures (typically: function prevented)
  - No part/no effect failures (typically: Not associated with the main function)
- Detectability:
  - Detected - revealed by online diagnostics
  - Undetected - revealed by functional tests or upon a real demand for activation

FMECA main steps

1. FMECA prerequisites (what to prepare before start)
2. System structure analysis
3. Failure analysis and preparation of FMECA worksheets
4. Team review
5. Corrective actions

FMECA Prerequisites (1)

1. Define the system to be analyzed
   - System boundaries (which parts should be included and which should not)
   - Main system missions and functions (incl. functional requirements)
   - Operational and environmental conditions to be considered
     Note: Interfaces that cross the design boundary should be included in the analysis

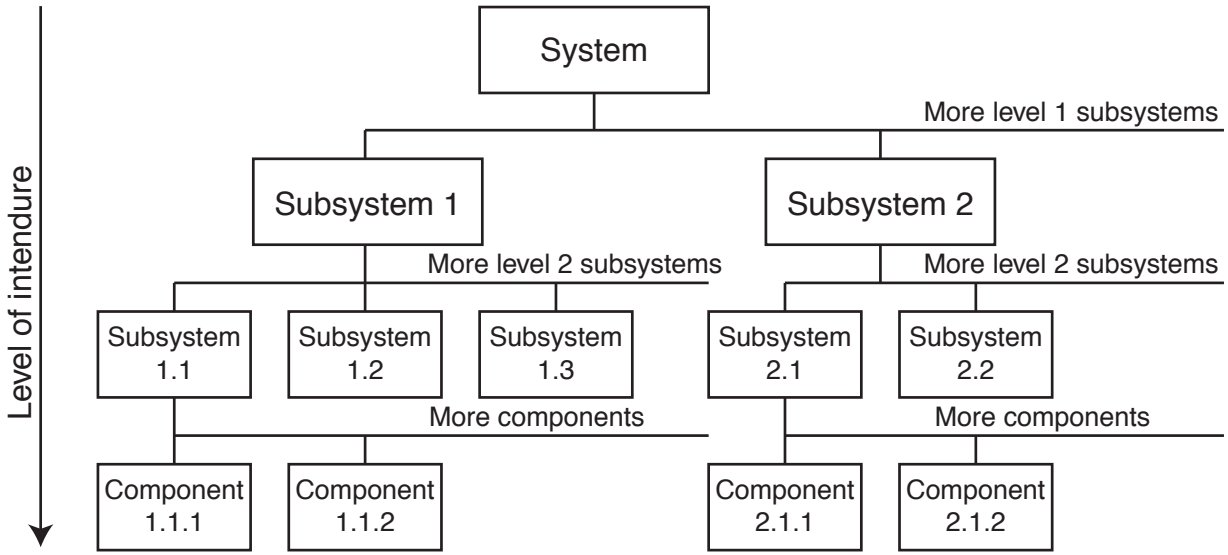
...continued on next slide

FMECA Prerequisites (2)

2. Collect available information that describes the system to be analyzed; including drawings, specifications, schematics, component lists, interface information, functional descriptions, and so on
3. Collect information about previous and similar designs from internal and external sources; including FRACAS data, interviews with design personnel, operations and maintenance personnel, component suppliers, and so on

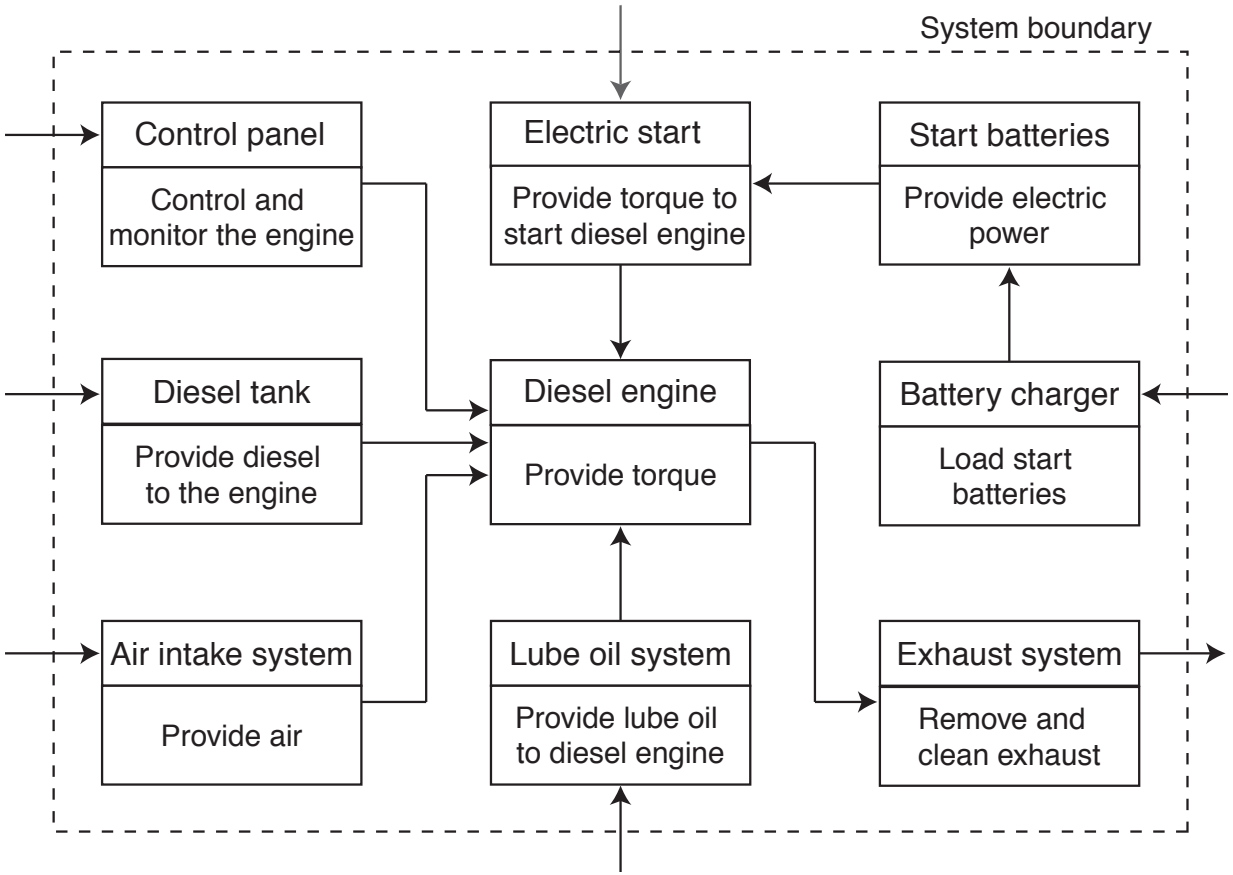
System Structure Analysis (1)

- Divide the system into manageable units - typically functional elements.
- To what level of detail we should break down the system will depend on the objective of the analysis.
- It is often desirable to illustrate the structure by a hierarchical tree diagram:



System Structure Analysis (2)

In some applications it may be beneficial to illustrate the system by a functional block diagram (FBD) as illustrated in the following figure.



System Structure Analysis (3)

Rules of thumb:

- The analysis should be carried out on an as high level in the system hierarchy as possible ("screening of subsystems to study in more detail")
- If unacceptable consequences are discovered on this level of resolution, then the particular element (subsystem, sub-subsystem, or component) should be divided into further detail to identify failure modes and failure causes on a lower level.
- **To start on a too low level will give a complete analysis, but may at the same time be a waste of efforts and money.**

FMECA Worksheet (1)

A suitable FMECA worksheet has to be decided. In many cases the client (customer) will have requirements to the worksheet format – for example to fit into her maintenance management system.

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Operational mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

FMECA Worksheet (2)

For each system element (subsystem, component) the analyst must consider all the functions of the elements in all its operational modes, and ask if any failure of the element may result in any unacceptable system effect. If the answer is no, then no further analysis of that element is necessary. If the answer is yes, then the element must be examined further.

FMECA Worksheet (3)

We will now discuss the various columns in the FMECA worksheet on the previous frame.

1. In the first column a unique reference to an element (subsystem or component) is given. It may be a reference to an id. in a specific drawing, a so-called tag number, or the name of the element.

2. The functions of the element are listed. It is important to list all functions. A checklist may be useful to secure that all functions are covered.

FMECA Worksheet (4)

3. The various operational modes for the element are listed. Example of operational modes are: idle, standby, and running. Operational modes for an airplane include, for example, taxi, take-off, climb, cruise, descent, approach, flare-out, and roll. In applications where it is not relevant to distinguish between operational modes, this column may be omitted.

4. For each function and operational mode of an element the potential failure modes have to be identified and listed. Note that a failure mode should be defined as a nonfulfillment of the functional requirements of the functions specified in column 2.

FMECA Worksheet (5)

5. The failure modes identified in column 4 are studied one-by-one. The failure mechanisms (e.g., corrosion, erosion, fatigue) that may produce or contribute to a failure mode are identified and listed. Other possible causes of the failure mode should also be listed. If may be beneficial to use a checklist to secure that all relevant causes are considered. Other relevant sources include: FMD-97 “Failure Mode/Mechanism Distributions” published by RAC, and OREDA (for offshore equipment)

FMECA Worksheet (6)

6. The various possibilities for detection of the identified failure modes are listed. These may involve diagnostic testing, different alarms, proof testing, human perception, and the like. Some failure modes are evident, other are hidden. The failure mode “fail to start” of a pump with operational mode “standby” is an example of a hidden failure.

FMECA Worksheet (7)

In some applications, an extra column is added to rank the likelihood that the failure will be detected before the system reaches the end-user/customer. The following detection ranking may be used:

Rank	Description
1-2	Very high probability that the defect will be detected. Verification and/or controls will almost certainly detect the existence of a deficiency or defect.
3-4	High probability that the defect will be detected. Verification and/or controls have a good chance of detecting the existence of a deficiency/defect.
5-7	Moderate probability that the defect will be detected. Verification and/or controls are likely to detect the existence of a deficiency or defect.
8-9	Low probability that the defect will be detected. Verification and/or control not likely to detect the existence of a deficiency or defect.
10	Very low (or zero) probability that the defect will be detected. Verification and/or controls will not or cannot detect the existence of a deficiency/defect.

– Source: SEMATECH (1992)

FMECA Worksheet (8)

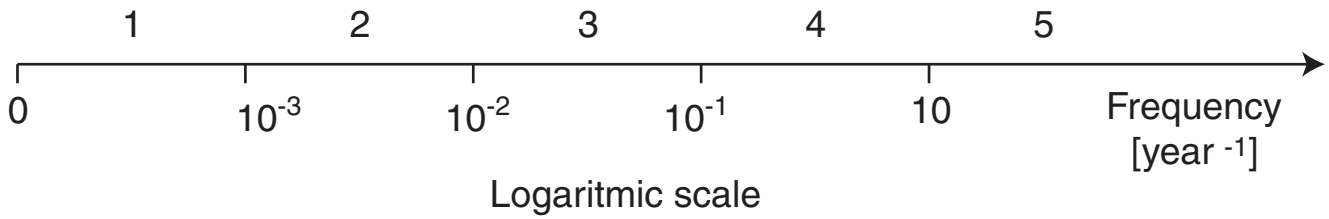
7. The effects each failure mode may have on other components in the same subsystem and on the subsystem as such (local effects) are listed.
8. The effects each failure mode may have on the system (global effects) are listed. The resulting operational status of the system after the failure may also be recorded, that is, whether the system is functioning or not, or is switched over to another operational mode. In some applications it may be beneficial to consider each category of effects separately, like: safety effects, environmental effects, production availability effects, economic effects, and so on.

In some applications it may be relevant to include separate columns in the worksheet for *Effects on safety*, *Effects on availability*, etc.

FMECA Worksheet (9)

9. Failure rates for each failure mode are listed. In many cases it is more suitable to classify the failure rate in rather broad classes. An example of such a classification is:

1	Very unlikely	Once per 1000 years or more seldom
2	Remote	Once per 100 years
3	Occasional	Once per 10 years
4	Probable	Once per year
5	Frequent	Once per month or more often



In some applications it is common to use a scale from 1 to 10, where 10 denotes the highest rate of occurrence.

FMECA Worksheet (10)

10. The severity of a failure mode is the worst potential (but realistic) effect of the failure considered on the system level (the global effects). The following severity classes for health and safety effects are sometimes adopted:

Rank	Severity class	Description
10	Catastrophic	Failure results in major injury or death of personnel.
7-9	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment.
4-6	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system.
1-3	Minor	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment

FMECA Worksheet (11)

In some application the following severity classes are used:

Rank	Description
10	Failure will result in major customer dissatisfaction and cause non-system operation or non-compliance with government regulations.
8-9	Failure will result in high degree of customer dissatisfaction and cause non-functionality of system.
6-7	Failure will result in customer dissatisfaction and annoyance and/or deterioration of part of system performance.
3-5	Failure will result in slight customer annoyance and/or slight deterioration of part of system performance.
1-2	Failure is of such minor nature that the customer (internal or external) will probably not detect the failure.

– Source: SEMATECH (1992)

FMECA Worksheet (12)

11. Possible actions to correct the failure and restore the function or prevent serious consequences are listed. Actions that are likely to reduce the frequency of the failure modes should also be recorded. We come bach to these actions later in the presentation.

12. The last column may be used to record pertinent information not included in the other columns.

Risk Ranking

The risk related to the various failure modes is often presented either by a:

- Risk matrix, or a
- Risk priority number (RPN)

Risk Matrix

The risk associated to failure mode is a function of the frequency of the failure mode and the potential end effects (severity) of the failure mode. The risk may be illustrated in a risk matrix.

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

Acceptable - only ALARP actions considered

Acceptable - use ALARP principle and consider further investigations

Not acceptable - risk reducing measures required

Risk Priority Number RPN)

An alternative to the risk matrix is to use the ranking of:

- O = the rank of the occurrence of the failure mode
- S = the rank of the severity of the failure mode
- D = the rank of the likelihood the the failure will be detected before the system reaches the end-user/customer.

All ranks are given on a scale from 1 to 10. The risk priority number (RPN) is defined as

$$\text{RPN} = \text{S} \times \text{O} \times \text{D}$$

The smaller the RPN the better – and – the larger the worse.

Limitations of RPN

- How the ranks O, S, and D are defined depend on the application and the FMECA standard that is used.
- The O, S, D, and the RPN can have different meanings for each FMECA.
- Sharing numbers between companies and groups is very difficult.

– Based on Kmenta (2002)

Alternative FMECA Worksheet

When using the risk priority number, we sometimes use an alternative worksheet with separate columns for O, S, and D. An example is shown below:

Project: Version: Date:

System: Subsystem: Teamwork leader:

Id.	Comp.	Function	Failure mode	Failure cause	Local effects	Global effects	S	O	D	RPN	Corrective actions

Example FMECA Worksheet

POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

___ System	1 - Automobile		FMEA Number 1234
___ Subsystem	2 - Body Closures		Page 4 of 9
X Component	3 - Front Door L.H.	Design Responsibility: Body Engineering	Prepared By: A. Tate - X6412 - Body Engr
Model Year(s)/Program(s)	199X/Lion 4dr/Wagon	Key Date: 3/3/2003	FMEA Date (Orig.) 2/28/2003 (Rev) 3/3/2003
Core Team	T. Fender - Car Product Dev., C. Childers - Manufacturing, J. Ford - Assy Ops (Dalton, Fraser, Henley Assembly Plants)		

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/Mechanism(s) of Failure	Occur	Current Design Controls	Det	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	Sev	Occ	Det	RPN
3 - Front Door L.H.																
- Ingress to and egress from vehicle. - Occupant protection from weather, noise, and side impact. - Support anchorage for door hardware including mirror, hinges, latch and window regulator. - Provide proper surface for appearance items - paint and soft trim.	Corroded interior lower door panels	Deteriorated life of door leading to: - Unsatisfactory appearance due to rust through paint over time. - Impaired function of interior door hardware.	7		Upper edge of protective wax application specified for inner door panels is too low.	6	Vehicle general durability test veh. T-118 T-109 T-301	7	294	Add laboratory accelerated corrosion testing.	A. Tate Body Engrg - 2/25/2003	Based on test results (Test No. 1481) upper edge spec raised 125 mm.	7	2	2	28
					Insufficient wax thickness specified.	4	Vehicle general durability testing - as above. - Detection	7	196	Add laboratory accelerated corrosion testing.	A. Tate Body Engrg - 3/28/2003	Test results (Test No. 1481) show specified thickness is adequate.	7	2	2	28
										Conduct Design of Experiments (DOE) on wax thickness.	A. Tate Body Engrg - 3/28/2003	DOE shows 25% variation in specified thickness is acceptable.				
					Inappropriate wax formulation specified.	2	Physical and Chem Lab test - Report No. 1265. - Detection	2	28				7	2	2	28
					Entrapped air prevents wax from entering corner/edge access.	5	Design aid investigation with nonfunctioning spray head. - Detection	8	280	Add team evaluation using production spray equipment and specified wax.	Body Engrg & Assy Ops - 3/28/2003	Based on test, addition vent holes will be provided in affected areas.	7	1	3	21
					Wax application plugs door drain holes.	3	Laboratory test using "worst case" wax application and hole size. - Detection	1	21				7	3	1	21
					Insufficient room between panels for spray head access.	4	Drawing evaluation of spray head access. - Detection	4	112	Add team evaluation using design aid buck and spray head.	Body Engrg & Assy Ops - 3/28/2003	Evaluation showed adequate access.	7	1	1	7

– ReliaSoft Xfmea printout, from www.reliasoft.com

FMECA Review team

A design FMECA should be initiated by the design engineer, and the system/process FMECA by the systems engineer. The following personnel may participate in reviewing the FMECA (the participation will depend on type of equipment, application, and available resources):

- Project manager
- Design engineer (hardware/software/systems)
- Test engineer
- Reliability engineer
- Quality engineer
- Maintenance engineer
- Field service engineer
- Manufacturing/process engineer
- Safety engineer

Review Objectives

The review team studies the FMECA worksheets and the risk matrices and/or the risk priority numbers (RPN). The main objectives are:

1. To decide whether or not the system is acceptable
2. To identify feasible improvements of the system to reduce the risk. This may be achieved by:
   - Reducing the likelihood of occurrence of the failure
   - Reducing the effects of the failure
   - Increasing the likelihood that the failure is detected before the system reaches the end-user.

If improvements are decided, the FMECA worksheets have to be revised and the RPN should be updated.

Problem solving tools like brainstorming, flow charts, Pareto charts and nominal group technique may be useful during the review process.

Selection of Actions

The risk may be reduced by introducing:

- Design changes
- Engineered safety features
- Safety devices
- Warning devices
- Procedures/training

Reporting of Actions

The suggested corrective actions are reported, for example, as illustrated in the printout from the Xfmea program.

Xfmea®

RECOMMENDED ACTIONS
(Summary Report)

Date: 3/26/2003
Page 5 of 9

#	Recommended Action(s)	Target Completion Date	Responsibility	Actions Taken	Item	Potential Cause(s)/Mechanism(s) of Failure	Priority
1	Add laboratory accelerated corrosion testing.	2/25/2003	A. Tate Body Engrg	Based on test results (Test No. 1481) upper edge spec raised 125 mm.	Front Door L.H.	Upper edge of protective wax application specified for inner door panels is too low.	
2	Add laboratory accelerated corrosion testing.	3/28/2003	A. Tate Body Engrg	Test results (Test No. 1481) show specified thickness is adequate.	Front Door L.H.	Insufficient wax thickness specified.	
3	Conduct Design of Experiments (DOE) on wax thickness.	3/28/2003	A. Tate Body Engrg	DOE shows 25% variation in specified thickness is acceptable.	Front Door L.H.	Insufficient wax thickness specified.	
4	Add team evaluation using production spray equipment and specified wax.	3/28/2003	Body Engrg & Assy Ops	Based on test, addition vent holes will be provided in affected areas.	Front Door L.H.	Entrapped air prevents wax from entering corner/edge access.	
5	Add team evaluation using design aid buck and spray head.	3/28/2003	Body Engrg & Assy Ops	Evaluation showed adequate access.	Front Door L.H.	Insufficient room between panels for spray head access.	

– ReliaSoft Xfmea printout, from www.reliasoft.com

RPN Reduction

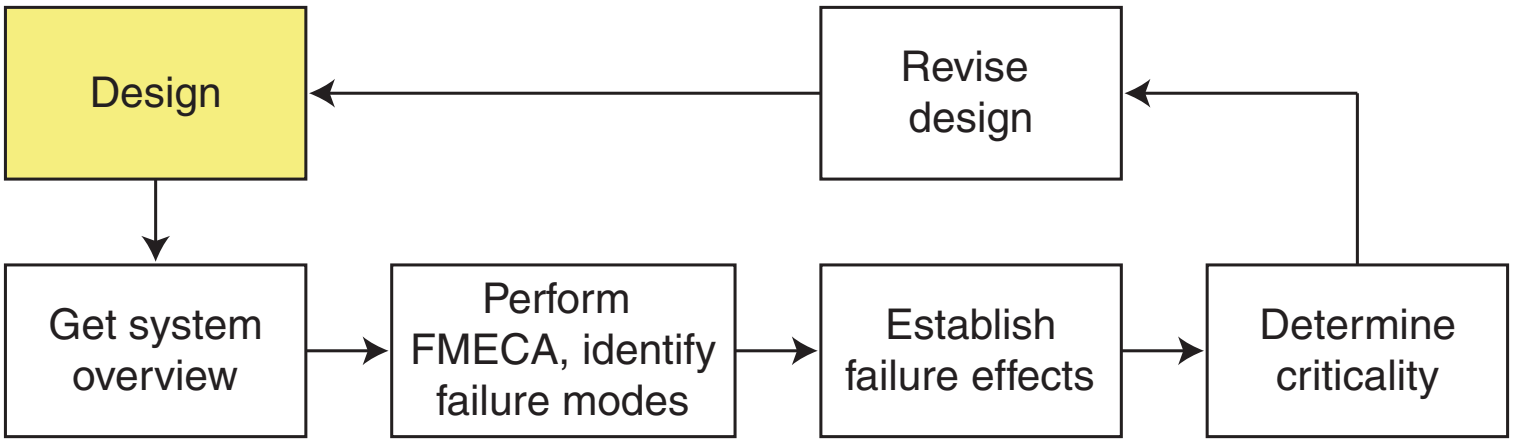
The risk reduction related to a corrective action may be comparing the RPN for the initial and revised concept, respectively. A simple example is given in the following table.

	Occurrence O	Severity S	Detection D	RPN
Initial	7	8	5	280
Revised	5	8	4	160
% Reduction in RPN				43%

Application Areas

- Design engineering. The FMECA worksheets are used to identify and correct potential design related problems.
- Manufacturing. The FMECA worksheets may be used as input to optimize production, acceptance testing, etc.
- Maintenance planning. The FMECA worksheets are used as an important input to maintenance planning – for example, as part of reliability centered maintenance (RCM). Maintenance related problems may be identified and corrected.

FMECA in Design



FMECA Pros and Cons

Pros:

- FMECA is a very structured and reliable method for evaluating hardware and systems
- The concept and application are easy to learn, even by a novice
- The approach makes evaluating even complex systems easy to do

Cons:

- The FMECA process may be tedious, time-consuming (and expensive)
- The approach is not suitable for multiple failures
- It is too easy to forget human errors in the analysis

FMEDA - a Variant of FMECA

An *Failure modes, Effects, and Diagnostic Analysis* (FMEDA) is an extension of an FMECA that is tailured-made for a SIS.

- FMEDA as a method was developed by the company Exida
- Is in principle, very similar to an FMECA, and a FMECA-like table is used
- Focus is placed on (and columns in the table are allocated to) the classification of each failure mode into DU, DD, SU or SD
- Failiure rates can be estimated for each failure category with basis in the classification and the overall failure rate of the item
- Also proof test coverage may be considered
- The approach can supplement manufacturers calculations of failure rates, and specific measures like the safe failure fraction (SFF) and diagnostic coverage factor (DC)

More information is available from the book “Safety instrumented systems verification”, by William M. Goble and Harry Cheddie.

FMEDA Example

Table 1
FMEDA (failure modes, effects and diagnostic analysis) for high diagnostic PLC AC input circuit (failure per billion hours)

1 Name	2 Code	3 Function	4 Mode	5 Cause	6 Effect	7 Criticallty λ	8	9 Remarks	10 Det.	11 Diagnostics	12 Mode	13 SD	14 SU	15 DD	16 DU
R1-10K	4555-10	Input	Short		Threshold shift	Safe	0.125		0		1	0	0.13	0	0
		Threshold	Open	solder open	Open circuit	Safe	0.5		1	Lose input pulse	1	0.5	0	0	0
			Drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			Drift high			Safe	0.01	none until too high	1	Lose input pulse	1	0.01	0	0	0
R2100K	4555-100	Current limit	Short		Short input	Safe	0.125		1		1	0.13	0	0	0
			Open	solder open		Safe	0.5		1	loss input pulse		0	0	0.5	0
			Drift low			Safe	0.01	none until too low	0		1	0	0.01	0	0
			Drift high			Safe	0.01	none until too high	1	Lose input pulse	1	0.01	0	0	0
D1	4200-7	Voltage drop	Short	surge	Over voltage	Safe	2		1	Lose input pulse	1	2	0	0	0
			Open		Open circuit	Safe	5		1	Lose input pulse	1	5	0	0	0
D2	4200-7	Voltage drop	Short	surge	Overvoltage	Safe	2		1	Lose input pulse	1	2	0	0	0
			Open		Open circuit	Safe	5		1	Lose input pulse	1	5	0	0	0
OC1	4805-25	Isolate	led dim	wear	No light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			Tran. Short	internal short	Read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			Tran. Open		Read logic 0	Safe	3		1	Comp. mismatch	1	6	0	0	0
OC2	4805-25	Isolate	led dim	wear	No light	Safe	28		1	Comp. mismatch	1	28	0	0	0
			Tran. Short	internal short	Read logic 1	Dang.	10		1	Comp. mismatch	0	0	0	10	0
			Tran. Open		Read logic 0	Safe	6		1	Comp. mismatch	1	6	0	0	0
OC1/OC2			Cross	channel short	Same signal	Dang.	0.01		0		0	0	0	0	0.01
R3-100K	4555-100	Filter	Short		Lose filter	Safe	0.125			0	1	0	0.13	0	0

W.M. Goble, A.C. Brombacher / Reliability Engineering a

Reference: Goble, W.M. and Brombacher, A. Using a failure modes, effects and diagnosis analysis (FMEDA) to mesure diagnostic coverage in programmable electronic systems. DOI:10.1016/S0951-8320(99)00031-9 (Journal of Reliability Engineering and System Safety)